UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

DIVISIÓN ACADÉMICA DE INFORMÁTICA Y SISTEMAS

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

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

Maestro en Administración de Tecnologías de la Información

Presenta:

Noel Zacarias Morales

Directores de Trabajo Recepcional:

Dr. Julian Javier Francisco León
Dr. Gilberto Murillo González

Jurado Revisor:

Dr. Herman Aguilar Mayo
Dr. Guillermo de los Santos Torres
Dr. Miguel Antonio Wister Ovando

Cuerpos Académicos o Grupos de Investigación de los directores:

Ingenieria de software
Sistemas Inteligentes

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

Administración, diseño e implementación de integración de soluciones de T.I.

Cunduacán, Tabasco. Septiembre, 2019.

UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

"ESTUDIO EN LA DUDA. ACCIÓN EN LA FE"

DAIS
11111000011

Oficio No. 1717/2019/DAIS/D
20 de agosto de 2019

Dr. Julián Javier Francisco León
Profesor-Investigador
Presente

De acuerdo al artículo 46 fracción III del Reglamento General de Estudios de Posgrado Vigente, de la Universidad Juárez Autónoma de Tabasco, me permito informarle a Usted, que ha sido asignado director del trabajo de tesis titulado **"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"**, a realizar por el **C. Noel Zacarias Morales**, para obtener el grado de Maestro en Administración de Tecnologías de la Información.

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

Atentamente

UNIVERSIDAD JUAREZ AUTONOMA DE TABASCO

MTE. Oscar Alberto González González
Director

DIVISION ACADEMICA DE INFORMATICA Y SISTEMAS

C.c.p. MASI. Arturo Corona Ferreira.-Encargado del Despacho de la Coordinación de Posgrado.
Archivo.
Consecutivo.

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

Consorcio de Universidades Mexicanas

UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

"ESTUDIO EN LA DUDA. ACCIÓN EN LA FE"

DAIS
11111000011

Oficio No. 1718/2019/DAIS/D
20 de agosto de 2019

Dr. Gilberto Murillo González
Profesor-Investigador
Presente

De acuerdo al artículo 46 fracción III del Reglamento General de Estudios de Posgrado Vigente, de la Universidad Juárez Autónoma de Tabasco, me permito informarle a Usted, que ha sido asignado director del trabajo de tesis titulado **"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"**, a realizar por el **C. Noel Zacarias Morales**, para obtener el grado de Maestro en Administración de Tecnologías de la Información.

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

Atentamente

UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

MTE. Óscar Alberto González González
Director

DIVISIÓN ACADÉMICA DE INFORMÁTICA Y SISTEMAS

C.c.p. MASI. Arturo Corona Ferreira.-Encargado del Despacho de la Coordinación de Posgrado.
Archivo.
Consecutivo.

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

Consorcio de Universidades Mexicanas

F5: Liberación de Dirección de Tesis 2019

Cunduacán, Tabasco., a 11 de junio de 2019.

Asunto: Liberación de dirección de tesis.

MTE. Óscar Alberto González González
Director de la División Académica de Informática y Sistemas
Universidad Juárez Autónoma de Tabaco

Por medio de la presente nos permitimos comunicarle que después de haber concluido la dirección 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***", elaborada por el ***C. Noel Zacarías Morales***, estudiante de la **Maestría en Administración de Tecnologías de la Información**, consideramos que puede continuar con los trámites para la obtención del grado.

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

UNIVERSIDAD JUAREZ AUTONOMA DE TABASCO
14 JUN. 2019
COORDINACION DE INV. Y POSGRADO

A t e n t a m e n t e

Dr. Julián Javier Francisco León.

Dr. Gilberto Murillo González.

C.c.p. M.A.S.I. Arturo Corona Ferreira. - Encargado del Despacho de la Coordinación de Posgrado.
Directores de Tesis.
Estudiante.

RECIBIDO
14 JUN 2019

F6: Solicitud de Jurado 2019

Cunduacán, Tabasco., a 11 de junio de 2019.

Asunto: Solicitud de Jurado

MTE. Óscar Alberto González González
Director de la División Académica de Informática y Sistemas
Universidad Juárez Autónoma de Tabaco

Por este medio me permito informarle que 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***", ha sido liberada por mis directores: **Dr. Julián Javier Francisco León** y **Dr. Gilberto Murillo González**, por lo que en atención a ello me dirijo a usted con la finalidad de solicitarle tenga a bien nombrar al jurado para que evalúe el citado trabajo.

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

Atentamente

Noel Zacarías Morales.

Matrícula:	172H11002
Domicilio:	Carretera Villahermosa a Reforma Km 6
Localidad:	Centro, Tabasco
Teléfono:	(933)-593-4244
E-mail:	zamn920822@gmail.com

UNIVERSIDAD JUAREZ AUTONOMA DE TABASCO 14 JUN. 2019 COORDINACION DE INV. Y POSGRADO

14 JUN 2019

C.c.p. M.A.S.I. Arturo Corona Ferreira. -Encargado del Despacho de la Coordinación de Posgrado.
Estudiante.

F7: Respuesta de Jurado 2019

Cunduacán, Tabasco., a 01 de julio de 2019.

Asunto: Respuesta de Jurado

MTE. Óscar Alberto González González
Director de la División Académica de Informática y Sistemas
Universidad Juárez Autónoma de Tabaco

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 **"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"**, realizada por el **C. Noel Zacarias Morales**, 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 correspondientes a la obtención del grado.

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

Atentamente integrantes del jurado

Dr. Guillermo de los Santos Torres.

Dr. Miguel Antonio Wister Ovando.

Dr. Herman Aguilar Mayo.

c.c.p. M.A.S.I. Arturo Corona Ferreira. - Encargado del Despacho de la Coordinación de Posgrado.
Integrantes del Jurado.
Estudiante.

UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO 11 JUL. 2019

RECIBIDO 11 JUL 2019

UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

"ESTUDIO EN LA DUDA. ACCIÓN EN LA FE"

DIVISIÓN ACADÉMICA DE INFORMÁTICA Y SISTEMAS

Cunduacán Tabasco 01 Julio 2019

En la Universidad Juárez Autónoma de Tabasco, de acuerdo al Reglamento de Estudios de Posgrado vigente, se revisó el trabajo de investigación titulado **"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"**, realizado por el **C. Noel Zacarias Morales**, para obtener el Grado de Maestro en Administración de Tecnologías de la Información bajo la modalidad de Tesis.

Los integrantes del jurado, después de revisar el trabajo, lo declararon aceptado. Firmando la presente a los 01 del mes julio de 2019.

Dr. Guillermo de los Santos Torres.
Profesor-Investigador

Dr. Miguel Antonio Wister Ovando.
Profesor-Investigador

Dr. Hermán Aguilar Mayo.
Profesor-Investigador

11 JUL. 2019

UNIVERSIDAD JUÁREZ AUTÓNOMA DE TABASCO

"ESTUDIO EN LA DUDA. ACCIÓN EN LA FE"

DAIS
11111000011

Oficio No. 1699/19/DAIS/D
16 de agosto de 2019

C. Noel Zacarias Morales
Matricula 172H11002

En virtud de que cumple satisfactoriamente los requisitos establecidos en el Reglamento General de Estudio de Posgrado vigente en la Universidad, informo a Usted que se autoriza la impresión del trabajo recepcional **"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"**, para presentar examen y obtener el Grado de Maestro en Administración de Tecnologías de la Información bajo la modalidad de Tesis.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente

UNIVERSIDAD JUAREZ AUTONOMA DE TABASCO

20 AGO. 2019

MTE. Oscar Alberto González González
Director

DIVISION ACADEMICA DE INFORMATICA Y SISTEMAS

C.c.p. MASI. Arturo Corona Ferreira - Encargado del Despacho de la Coordinación de Posgrado
Archivo.
Consecutivo.

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

Consorcio de Universidades Mexicanas

F8. Cesión de Derechos 2019

Cunduacán, Tabasco., a 12 de julio de 2019.

Asunto: Cesión de Derechos.

A quien corresponda:

El que suscribe la presente, declara que el trabajo de tesis titulado, **"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"** 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

Autores:

Nombre	Domicilio	Firma autógrafa
Noel Zacarias Morales	Tabasco, México.	
Dr. Julián Javier Francisco León	Veracruz, México.	
Dr. Gilberto Murillo González	Tabasco, México.	

c.c.p. **MTE. Óscar Alberto González González.** - Director de la DAIS.
M.A.S.I. Arturo Corona Ferreira. - Encargado del Despacho de la Coordinación de Posgrado
Directores de Tesis.
Estudiante.

UNIVERSIDAD JUAREZ AUTONOMA DE TABASCO
15 AGO. 2019
COORDINACION DE INV. Y POSGRADO

15 ABR.

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 "**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**", de la cual soy autor y titular de los Derechos de Autor.

La finalidad del uso por parte de la Universidad Juárez Autónoma de Tabasco de la tesis antes mencionada será única y exclusivamente para difusión, educación y sin fines de lucro; autorización que se hace de manera enunciativa más no limitativa para subirla a la Red Abierta de Bibliotecas Digitales (RABIO) y a cualquier otra Red Académica con las que la Universidad tenga relación Institucional.

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

Se firma la presente autorización en la Ciudad de Villahermosa, Tabasco a los 12 días del mes de julio del año 2019.

AUTRIZO

NOEL ZACARIAS MORALES

Dedicatorias

Esta tesis esta especialmente dedicada a todas aquellas personas que, a pesar de las adversidades, no se rinden sin dar batalla.

Agradecimientos

Agradezco a toda aquella persona que dedique un poco de su tiempo en leer esta tesis.

Resumen

En el presente documento se explica la importancia de la seguridad de la información, específicamente para la Coordinación de Desarrollo y Soporte de Sistemas (CDSS) de la Universidad Juárez Autónoma de Tabasco (UJAT), que es la encargada de, entre otras funciones, del desarrollo, mantenimiento y funcionamiento de los sistemas de información institucionales de todos los departamentos que conforman a la UJAT. Dentro de los hallazgos de este estudio se encuentran: los incidentes de seguridad de la información que se han presentado en la Coordinación, los mecanismos de seguridad de la información actualmente implementados, y el grado de cumplimiento de los apartados la norma ISO/IEC 27002:2013 que se consideraron aplicables en la Coordinación (dominios, objetivos de control y controles). Logrando de esta manera el objetivo primordial de este estudio, que es identificar las prácticas de seguridad de la información que permitan mitigar las vulnerabilidades y amenazas existentes en la Coordinación.

Introducción

La seguridad de la información, según la Organización Internacional de Normalización, tiene por objetivo preservar la confidencialidad, integridad y disponibilidad de la información de una organización, independientemente del medio en el que esta se encuentre, pudiendo ser información escrita, impresa, proyectada, digital, entre otros (International Organization for Standardization & International Electrotechnical Commission, 2018).

En las instituciones de educación superior, como es el caso de la Universidad Juárez Autónoma de Tabasco, se concentra información contable, legal, administrativa, entre otros tipos, que es considerada importante, ya que de dicha información depende la correcta operación diaria de todos los departamentos que la conforman, este es motivo principal por el cual se lleva a cabo el presente trabajo y que tiene por objetivo, realizar un estudio sobre la seguridad de la información con un enfoque en la norma ISO/IEC 27002:2013 para la Coordinación de Desarrollo y Soporte de Sistemas de la Dirección de Tecnologías de información e Innovación de la Universidad Juárez Autónoma de Tabasco.

El presente documento está integrado por cinco capítulos en los que se contextualizan las razones por las cuales se decidió llevar a cabo esta investigación, se presenta el estado del arte actual relacionado a la problemática de la seguridad de la información, así como la aplicación de la metodología propuesta para concluir exitosamente la investigación, finalmente, se presentan los resultados, conclusiones y trabajos futuros.

Índice general

Índice de figuras

Índice de tablas

Capítulo 1. Generalidades

En este primer capítulo, se encuentran contenidos los aspectos generales del estudio, como el planteamiento del problema, los objetivos generales y específicos del estudio, su justificación y la metodología plantada para su elaboración.

1.1 Antecedentes

El SysAdmin Audit, Networking and Security Institute (SANS), menciona que la seguridad de la información se refiere a: los procesos y metodologías diseñados e implementados para proteger la información impresa, electrónica o cualquier otra forma de información confidencial, privada o sensible, de acceso no autorizado, uso indebido, divulgación, destrucción o modificación (SysAdmin Audit, Networking and Security Institute, s/f).

En septiembre 2017, el instituto SANS publicó los resultados de una encuesta en la que el 78% de los encuestados encontró que, en sus organizaciones, ocurrieron dos o más amenazas en los 12 meses previos a la fecha de publicación de la encuesta, así también, el 12% de ellos encontró una brecha de seguridad; y de igual manera el 68% reporto que las amenazas ocurrieron en múltiples ocasiones (SysAdmin Audit, Networking and Security Institute, 2017).

El instituto SANS (2017) mencionó que dentro de los datos e información donde se concentran el mayor número de brechas de seguridad, se encuentran los nombres de usuario y contraseñas (conocidos como datos de acceso de usuarios) así como la información personal privilegiada (conocida como información de identificación personal), con lo que es posible apreciar que los datos privilegiados y sensibles son los más codiciados por atacantes. Las conclusiones claves del reporte son que: 48%, de los que se encontraron con una brecha de seguridad, informaron que el incidente terminó con una filtración de datos sensibles; así como que el 31% de los encuestados señalan que su mayor obstáculo para la protección de datos sensibles es la falta de personal y recursos.

En general, los resultados indican que las organizaciones necesitan comprender mejor sus datos confidenciales y cómo la tecnología puede ayudar a reforzar las políticas y procedimientos para proteger esos datos (SysAdmin Audit, Networking and Security Institute, 2017).

Un incidente en el cual se comprometió la seguridad de la información fue el de Facebook con Data Analytics y Cambridge Analytica (compañías privadas dedicadas a la minería y análisis de datos). En este incidente, las compañías recolectaron información de aproximadamente 87 millones de perfiles de usuarios de Facebook sin autorización de los usuarios, esta información fue vinculada a las campañas presidenciales del 2016 en Estados Unidos (Symeonidis et al., 2018).

Otro incidente importante fue el registrado en mayo del 2017, conocido como WannaCry, en el cual un grupo de hackers iniciaron la difusión de un ransomware (programa informático que bloquea todos los archivos en el sistema infectado) alrededor del mundo. De acuerdo con la Oficina Europea de Policía (Europol) más de 200,000 computadoras en 150 países fueron víctimas del ataque de encriptación de archivos. Algunas de las empresas más afectadas fueron: Fedex, Megafon, Telefónica, el Banco Central de Rusia, al igual que hospitales de Inglaterra y Escocia, la figura 1.1 muestra una captura de pantalla se un sistema infectado por el ransomware WannaCry (A. Mattei, 2017).

Figura 1.1. Sistema infectado por el ransomware WannaCry.

Fuente: (Kaspersky Lab, 2017).

En el incidente WannaCry, México fue uno de los países más afectados en América Latina, siendo los sectores con mayor exposición los comercios minoristas, telecomunicaciones y finanzas (Chávez, 2017).

Ahora bien, así como continuamente se desarrollan métodos que permiten violentar la seguridad de la información, también se existen métodos cuyo interés principal es mantener la confidencialidad,

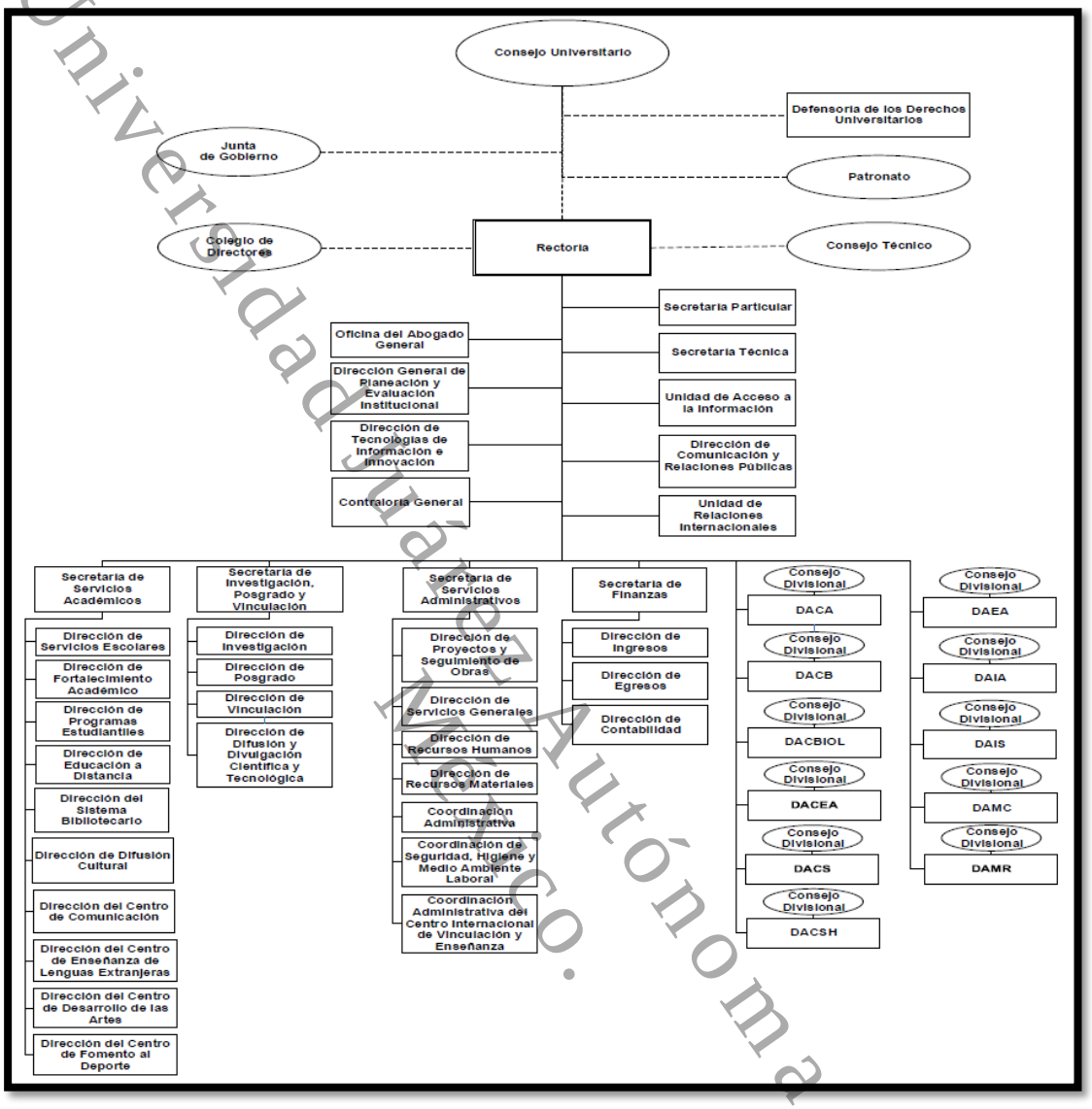
integridad y disponibilidad de esta, pero es evidente que su implementación es responsabilidad de cada organización.

En las instituciones de educación superior se concentra información considerada importante, como: información académica, administrativa, y contable, así como la relacionada con sus empleados y estudiantes, tanto inscritos como egresados, entre otros tipos de información, la cual permite la realización eficiente de las actividades en todas sus áreas.

La Universidad Juárez Autónoma de Tabasco (UJAT) es una universidad pública, cuya unidad central está localizada en el municipio de Centro, en el estado de Tabasco, México. Su misión es contribuir de manera significativa a la transformación de la sociedad y al desarrollo del país, con particular interés en el Estado de Tabasco, a través de la formación sólida e integral de profesionales capaces de adquirir, generar, difundir y aplicar el conocimiento científico, tecnológico y humanístico, con ética y responsabilidad para ser mejores individuos y ciudadanos (Universidad Juárez Autónoma de Tabasco, 2018).

Dentro de las diversas áreas o departamentos que integran a la Universidad Juárez Autónoma de Tabasco se encentra la Dirección de Tecnologías de Información e Innovación (DTII), la cual, por ser la encargada de la administración de la infraestructura tecnológica de la Universidad, mantiene presencia en las demás áreas que se muestran en la figura 1.2.

Figura 1.2. Organigrama de la Universidad Juárez Autónoma de Tabasco.



Fuente: (Universidad Juárez Autónoma de Tabasco, 2014).

Esta Dirección es la encargada de dirigir y evaluar programas institucionales para impulsar, establecer y administrar la aplicación de las tecnologías de información e innovación a los procesos de gestión de la Universidad, con el propósito de contar con los recursos para el diseño e implementación de estrategias organizacionales de administración del cambio y competitividad (Universidad Juárez Autónoma de Tabasco, 2014). Entre sus actividades primarias se encuentran las siguientes:

- Administrar la infraestructura tecnológica de la Universidad utilizada para el apoyo a las funciones sustantivas, adjetivas y programas institucionales.
- Dirigir los servicios de tecnologías de información y comunicación que se brindan en las dependencias universitarias.
- Promover y establecer los sistemas de seguridad informática y mecanismos de protección de las comunicaciones, servicios de cómputo y flujos de información institucional.
- Dirigir y supervisar las actividades de mantenimiento y actualización de los sistemas de información de la Universidad.
- Determinar la creación y actualización del marco normativo universitario en materia de tecnologías de información y comunicación.

A su vez, la Dirección de Tecnologías de Información e Innovación está integrada por las siguientes coordinaciones, que es su conjunto, permiten llevar a cabo todas sus actividades continuamente:

- Coordinación Administrativa.
- Coordinación de Redes y Telecomunicaciones.
- Coordinación de Desarrollo y Soporte de Sistemas.
- Coordinación de Soporte Técnico.
- Coordinación de Cómputo Académico.
- Coordinación de Cómputo Chontalpa.

Para llevar a cabo el presente trabajo, se eligió la Coordinación de Desarrollo y Soporte de Sistemas (CDSS), la cual es la encargada de coordinar e implementar tanto los procesos de desarrollo, como los de soporte a los sistemas de información, al igual que administrar las bases de datos institucionales, con la finalidad de asegurar la disponibilidad y habilitación para el desempeño de las funciones automatizadas de la Universidad (Universidad Juárez Autónoma de Tabasco, 2014). Entre sus principales funciones están:

- Coordinar y supervisar el servicio de atención a las divisiones académicas, secretarías y órganos de apoyo de la rectoría en materia de desarrollo y soporte a sistemas de información.

- Planear y coordinar los procesos de desarrollo y mantenimiento de los sistemas informáticos de la Universidad.
- Coordinar los procesos de documentación de los sistemas informáticos desarrollados por la Universidad.
- Establecer lineamientos y criterios para la realización de videoconferencias, la implementación de sistemas de seguridad informática, así como para el desarrollo y mantenimiento de los sistemas informáticos en la Universidad.
- Coordinar y supervisar la operación y mantenimiento de la infraestructura de las bases de datos de la Universidad.
- Coordinar y supervisar los procesos de respaldo de la información contenida en las bases de datos de la Universidad y los sistemas de información institucionales.

Actualmente, la Coordinación de Desarrollo y Soporte de Sistemas está conformada por 19 empleados, los cuales tienen asignadas diversas actividades y responsabilidades relacionadas con las funciones mencionadas anteriormente (Dirección de Tecnologías de Información e Innovación, 2018). Entre sus diferentes cargos se pueden mencionar los siguientes:

- Coordinador de desarrollo y soporte de sistemas.
- Jefe del departamento de soporte a sistemas de producción.
- Postmaster (Administrador de correo).
- Webmaster (Administrador web).
- Administrador de base de datos
- Desarrollador de sistemas.

En julio del 2018, la Dirección de Tecnologías de Información e Innovación publico los lineamientos generales en el uso de las tecnologías de información y comunicación de la Universidad Juárez Autónoma de Tabasco, en los cuales se brinda el primer marco normativo general para el uso de la infraestructura, servicios y desarrollo de las tecnologías de la información y comunicación que la Universidad requiere y ofrece.

1.2 Planteamiento del problema

1.2.1 Definición del problema

Normalmente se considera que la información es la sangre de las organizaciones, si el flujo de información es continuo, los procesos se llevaran a cabo de una manera óptima, pero por el lado contrario, si dicho flujo es restringido o perturbado, las organizaciones tienden a deteriorarse, lo cual convierte a la seguridad de la información en algo prioritario (Cárdenas-Solano, Martínez-Ardila, & Becerra-Ardila, 2016).

La información administrada por la Coordinación de Desarrollo y Soporte de Sistemas es un elemento clave para el correcto desarrollo, mantenimiento y funcionamiento de los sistemas de información institucionales de todos los departamentos que conforman a la Universidad Juárez Autónoma de Tabasco, sin los cuales la operación de dichos sistemas se vería interrumpida, como lo son los sistemas de consultas de información académica, los servicios de transacciones bancarias, entre otros.

Además del desarrollo y mantenimiento de los sistemas de información, la Coordinación tiene a su cargo la operación y mantenimiento de las bases de datos de toda la Universidad (bases de datos de alumnos, docentes, y de los sistemas de información de la Universidad), así como de la infraestructura que está utiliza (equipo de cómputo, y servidores), convirtiendo a la Coordinación en uno de los eslabones con mayor importancia en la cual la seguridad de la información tiene que ser un tema prioritario.

Como se mencionó anteriormente, la Dirección de Tecnologías de Información e Innovación recientemente publicó los lineamientos generales en el uso de las tecnologías de información y comunicación de la Universidad Juárez Autónoma de Tabasco, los cuales tienen como objeto normar el uso, adquisición, actualización, baja de equipos de cómputo y software; así como el contenido, diseño, desarrollo de los servicios en línea y de la infraestructura en telecomunicación que se oferta a la comunidad universitaria, a fin de coadyuvar al desarrollo de las actividades académicas y administrativas de la Universidad.

Si bien, en dichos lineamientos se contemplan puntos enfocados a la seguridad de la información, como el uso del correo electrónico, las redes de datos y los respaldos, al no ser lineamientos completamente enfocados a la seguridad de la información, existe la posibilidad de pudieran pasar alto medidas de seguridad de la información que puedan dar paso a incidentes que pongan en riesgo la confidencialidad o integridad de su información.

Según la Asociación Nacional de Universidades e Instituciones de Educación Superior, en México, 4 de cada 10 Instituciones de Educación Superior (IES) no tienen políticas de seguridad informática establecidas, lo que se puede traducir en que los responsables de TI de dichas instituciones no dispongan, ni siquiera, de procedimientos establecidos que les permitan actuar de manera rápida y acertada en caso de algún ataque informático (ANUIES, 2016).

Desafortunadamente en la Coordinación de Desarrollo y Soporte de Sistemas, ya se tienen antecedentes de incidentes de seguridad de la información, por lo que resulta necesario e indispensable comenzar a considerar el uso de normativas específicamente desarrolladas para prevenir incidentes de seguridad de la información.

1.2.2 Delimitación de la investigación

1.2.2.1 Alcances

Este documento presenta un estudio sobre la seguridad de la información, con un enfoque en la norma ISO/IEC 27002:2013, únicamente para la Coordinación de Desarrollo y Soporte de Sistemas de la Dirección de Tecnologías de Información e Innovación de la Universidad Juárez Autónoma de Tabasco.

Debido a el número de objetivos de control que componen a la norma ISO/IEC 27002:2013 (constando de 14 dominios y un total de 35 objetivos de control), se buscó efectuar al menos un análisis de un objetivo de control por cada dominio que la norma indica.

1.2.2.2 Limitaciones

Este trabajo estuvo sujeto a las siguientes tres limitaciones:

La primera consistió en que únicamente se tomó en cuenta a la Coordinación de Desarrollo y Soporte de Sistemas para el desarrollo del presente trabajo, y no a los demás departamentos que conforman la Dirección de Tecnologías de Información e Innovación de la Universidad Juárez Autónoma de Tabasco.

La segunda limitación corresponde a que, debido a la importancia de la información con la que se trabajó y al estar relacionada con la seguridad de esta, se consideró el uso de un acuerdo de confidencialidad.

La tercera tuvo que ver con el tiempo de realización de este trabajo, que, por cuestiones académicas debió ser terminado en 9 meces, de noviembre del 2018 a julio del 2019.

1.2.3 Pregunta de investigación

De acuerdo con el planteamiento del problema se plantea la siguiente pregunta de investigación:

- ¿Cómo puede la ISO/IEC 27002:2013 ayudar a la Coordinación de Desarrollo y Soporte de Sistemas a mejorar sus prácticas de seguridad de información?

1.3 Objetivos

Objetivo General

Realizar un estudio sobre la seguridad de la información con un enfoque en la norma ISO/IEC 27002:2013 para la Coordinación de Desarrollo y Soporte de Sistemas de la Dirección de Tecnologías de Información e Innovación de la Universidad Juárez Autónoma de Tabasco, para proponer prácticas de seguridad de la información que permitan mantener la confidencialidad, integridad y disponibilidad de su información.

Objetivos específicos

- Desarrollar un diagnostico situacional del estado actual de seguridad de la información en la Coordinación de Desarrollo y Soporte de Sistemas mediante MAGERIT y la norma ISO/IEC 27002:2013.

- Formular una propuesta de prácticas de seguridad de la información de acuerdo a la norma ISO/IEC 27002:2013 para la Coordinación de Desarrollo y Soporte de Sistemas.

1.4 Justificación

Con la aparición de Internet, el volumen de ataques cibernéticos ha ido creciendo progresivamente, por lo que la seguridad de la información tiene un papel crucial en los sistemas de TI. Las organizaciones

enfrentan decisiones complejas con respecto a la elección de controles de seguridad que permiten proteger sus activos de información. La implementación de estos controles debe garantizar un nivel adecuado de protección. Sin embargo, su selección requiere conocer las vulnerabilidades y amenazas existentes en la organización (Almeida & Respício, 2018).

La información que la Coordinación de Desarrollo y Soporte de Sistemas maneja durante los procesos de desarrollo y mantenimiento de los sistemas de información, al igual que en la operación y mantenimiento de la infraestructura de las bases de datos de la Universidad, es considerada por ellos de carácter altamente confidencial y crítico, por lo tanto, la información debe ser manejada con base en estándares internacionales de seguridad de la información.

La seguridad de la información está en el corazón de los enfoques de muchas organizaciones para reforzar las conductas deseables de seguridad de la información y reforzar las restricciones contra los comportamientos de seguridad indeseables (Marcinkowski & Stanton, 2003). Contar con las mejores prácticas de seguridad para la información y basadas en los controles de la norma ISO/IEC 27002:2013, permitirá mitigar las vulnerabilidades y amenazas de la seguridad de la información de la Coordinación de Desarrollo y Soporte de Sistemas, ya que al tratarse de prácticas diseñadas por organismos internacionales como son la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional, reflejarán la experiencia combinadas de diversas compañías internacionales influyentes sobre las medidas de control relevantes, procedimientos y técnicas, que proporcionan un nivel adecuado o aceptable de seguridad de la información.

Además, el uso de una norma diseñada por los mencionados organismos internacionales proporcionará a la Coordinación de Desarrollo y Soporte de Sistemas, mejoras en sus procesos internos, ya que, en esencia, las normas ISO/IEC buscan que las organizaciones logren la mayor eficacia posible en todo su trabajo.

Por último, es necesario resaltar que los resultados de este estudio brindarán a los 19 empleados la oportunidad de adquirir el conocimiento sobre la norma ISO/IEC para que, en un futuro, se pueda optar a una certificación ISO de la serie de normas 27000.

1.5 Metodología

Este estudio se considera de tipo descriptivo con un enfoque mixto, ya que se hizo uso de la combinación de los enfoques cuantitativo y cualitativo, con el objetivo de profundizar en la investigación de una forma completa, lo que no se hubiera logrado con el uso de un solo enfoque.

Para Arias, la investigación de tipo descriptiva consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento (Arias, 2012). Este estudio se realizó teniendo en cuenta que este tipo de investigación requeriría observar y cuantificar una o más características del fenómeno estudiado (la seguridad de la información).

Blasco y Pérez señalan que, en la investigación cualitativa, se estudia la realidad en su contexto natural, tal y como sucede, sacando e interpretando los fenómenos de acuerdo con las personas implicadas (Blasco & Pérez, 2007). Por otro lado, Hueso y Cascant mencionan que en la investigación cuantitativa se basa en el uso de técnicas estadísticas (técnicas de recolección cuantitativas como las encuestas, y técnicas de análisis cuantitativo como la estadística descriptiva e inferencial) para conocer ciertos aspectos de interés sobre la población que se está estudiando (Hueso & Cascant, 2012).

El uso del enfoque cuantitativo se aplicó debido a que parte de las evaluaciones consistieron en el análisis numérico y estadístico de presencia o ausencia de los controles de la norma ISO/IEC 27002, y que, de igual manera, permitió medir la cantidad y el nivel de implementación de cada uno de los controles de seguridad aplicables en la Coordinación de Desarrollo y Soporte de Sistemas, y en base a este resultado, proponer las medidas que protejan los activos. Por otra parte, con el enfoque cualitativo se pudo analizar e interpretar los datos generados mediante la observación del entorno y entrevistas hechas al personal de la Coordinación de Desarrollo y Soporte de Sistemas.

Según Hamui-Sutton los métodos de investigación mixtos tienen como característica principal la combinación de la perspectiva cuantitativa y cualitativa en un mismo estudio, ya que la combinación de los métodos permite darle profundidad al análisis (Hamui-Sutton, 2013).

Valencia y Mauricio, en su trabajo “Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000”, plantean una metodología de 5 fases para poder comprender los pasos a desarrollar para llevar a cabo una implementación de un sistema de gestión de seguridad de la información en una organización (Valencia-Duque & Orozco-Alzate, 2017).

Si bien el objetivo del presente trabajo no es lograr una implementación de un sistema de gestión de seguridad de la información, la metodología utilizada en este estudio, incorpora consideraciones de las fases 3 y 4 propuestas por Valencia y Mauricio, las cuales están relacionadas con la identificación de los activos de información y la identificación de las vulnerabilidades y amenazas de los activos de información, para lo cual, y como es recomendado por los mismos, se utilizó MAGERIT (Valencia-Duque & Orozco-Alzate, 2017).

La metodología para este estudio estuvo conformada por 4 fases, las cuales se muestran a continuación:

- **Fase 1: Análisis de la Coordinación de Desarrollo y Soporte de Sistemas (análisis del área de trabajo)**

Se llevaron a cabo las reuniones en las que se recopilo información de la Coordinación relacionada a las características de las áreas de trabajo de los empleados, así como información relacionada a la seguridad de la información actualmente implantada.

- **Fase 2: Evaluación de seguridad**

Se elaboraron los instrumentos para la identificar tanto a los activos de información, como sus vulnerabilidades y amenazas, así como los mecanismos actualmente implementados para la seguridad de la información con base en la norma ISO/IEC 27002:2013, y posteriormente se aplicaron en la Coordinación de Desarrollo y Soporte de Sistemas.

- **Fase 3: Elaboración del informe**

Se integraron los resultados de la evaluación y se detallaron los hallazgos encontrados durante la fase de evaluación de seguridad de la información.

- **Fase 4: Propuesta de prácticas de seguridad de la información para la Coordinación de Desarrollo y Soporte de Sistemas**

Por último, y tomando como base la información del informe elaborado y la norma ISO/IEC 27002, se propusieron a la Coordinación de Desarrollo y Soporte de Sistemas, prácticas de seguridad de la información consideraras importantes.

Capítulo 2. Estado del arte

La información es el instrumento fundamental para el funcionamiento de las empresas y la operación de los negocios, esto hace que deba protegerse como el activo más importante de la organización (Velásquez, 2003). El presente capitulo se encuentra dividido en dos apartados, en el primero se mencionan los trabajos considerados relevantes para este estudio, y en el segundo, los conceptos con los que el lector debe estar familiarizado para comprender el resto del contenido de este estudio.

2.1 Marco referencial

La seguridad de la información es un campo de estudio con diferentes enfoques (Altamirano & Bayona, 2017), por lo que se han publicado trabajos de investigación, que han dado paso a la creación de modelos, normas y estándares de seguridad. Diversas investigaciones alrededor del mundo han profundizado en la importancia que debe darse a la seguridad de la información, estas han aportado conclusiones y avances en diferentes enfoques. Este estudio considera relevantes los siguientes trabajos:

El trabajo de investigación realizado por Cárdenas, Martínez y Becerra, en el cual se realizó una revisión bibliografía sistemática acerca las tendencias de investigación sobre la seguridad de la información, en el periodo entre enero del 2001 y octubre del 2015, y que obtuvieron como resultado un amplio marco de trabajo multi-dimensional en el que se relaciona gestión del conocimiento, gestión de riesgos, incidentes de seguridad, sistemas de información y redes, recursos humanos, aspectos económicos, gobernanza, políticas, y buenas prácticas (Cárdenas-Solano et al., 2016).

La creación de un modelo basado en múltiples teorías de seguridad, que explica la adherencia de los empleados a las políticas de seguridad, para este modelo se combinaron elementos de la Teoría de la Motivación de la Protección, la Teoría de la Acción Razonada y la Teoría de la Evaluación Cognitiva (Siponen, Mahmood, & Pahnila, 2014).

Los resultados de esta investigación mostraron la gravedad percibida de las posibles amenazas a la seguridad de la información, la creencia de los empleados sobre si pueden aplicar y adherirse a las políticas de seguridad de la información, la vulnerabilidad a posibles amenazas de seguridad y la actitud de los empleados hacia el cumplimiento las normas para cumplir con estas políticas. La investigación enfatiza la importancia de que los empleados reciban educación y capacitación práctica sobre seguridad.

Otra investigación analizó las teorías de seguridad de la información, y mediante de la revisión sistemática de la literatura, identifico que las teorías más relevantes que los autores están empleando en sus investigaciones relacionadas al cumplimiento de las políticas de seguridad, están enfocadas a comprender el comportamiento humano a través de teorías psicológicas o sociales (Altamirano & Bayona, 2017).

Esto conduce a tener un enfoque interdisciplinario que permita una visión global, que en su conjunto conlleve a un enfoque real del problema, y no solo desde la perspectiva tecnológica como comúnmente se hace.

La investigación: "Modelo de cumplimiento de la política de seguridad de la información en las organizaciones", concluye que la falta de conciencia de la seguridad de la información, la ignorancia, la negligencia, la apatía y la resistencia son la raíz de los errores de los usuarios, y que terminan por comprometer la seguridad de la información. Además, muestra cómo el cumplimiento de las políticas de seguridad de la información organizacional moldea y mitiga el riesgo del comportamiento de los empleados. Los resultados del análisis de datos revelaron que el intercambio de conocimientos de seguridad de la información, la colaboración, la intervención y la experiencia, tienen un efecto significativo en la actitud de los empleados hacia el cumplimiento de las políticas de seguridad de la información organizacional (Sohrabi, Von, & Furnell, 2016).

El desarrollo de mecanismos de seguridad de la información implica más que la mera formulación e implementación de políticas. Aquellas organizaciones que no reconozcan los pasos requeridos en el desarrollo de medidas de seguridad corren el riesgo de desarrollar, por ejemplo, políticas mal pensadas, incompletas, redundantes e irrelevantes, y que no serán totalmente respaldadas por los usuarios.

También resulta interesante mencionar el trabajo de investigación: "Cómo gestionar la seguridad de la información (según ISO 27001: 2013) en una PyME del sector de las tecnologías de la información y la comunicación"; el objetivo de este trabajo fue crear una guía para ayudar a pequeñas y medianas empresas (PyME) a adquirir el conocimiento suficiente sobre la norma ISO/IEC 27001:2013 para poder optar a la certificación ISO de la misma (Abad, 2015).

Por su parte, Díaz y Reyes, de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México (UNAM), contribuyen a esta interesante área de estudio de la seguridad, con el trabajo: "Buenas prácticas de seguridad alineadas al ISO/IEC 27002 para el aseguramiento de equipos Linux-Debian pertenecientes a un CERT", y cuyo objetivo fue realizar una matriz de controles y recomendaciones de buenas prácticas para el aseguramiento de equipos de cómputo asignados a estaciones de trabajo

pertenecientes a un equipo de respuesta a incidentes en cómputo (CERT por sus siglas en inglés) (Díaz & Reyes, 2015).

Otro trabajo similar es el propuesto por Vergel y Sepúlveda, titulado “Diseño de un manual de políticas de seguridad informática aplicando la norma ISO 27002 para la alcaldía del municipio de la Playa de Belén, norte de Santander”, el cual tuvo por objetivo establecer políticas de seguridad informática que contribuyeran a gestionar las brechas de seguridad presentes en una alcaldía municipal de Colombia (Vergel & Sepúlveda, 2015).

Adicionalmente, Chen y Li, de la Universidad de Tecnología de Dalian, mencionan que el comportamiento de seguridad de la información de los empleados es fundamental para garantizar la seguridad de los activos de información de una organización, por lo que su trabajo *“Understanding Organization Employee's Information Security Omission Behavior: an Integrated Model of Social norm and Deterrence”*, proponen un modelo que integra la teoría de disuasión y de normas sociales para asegurar que el factor humano acepte y cumpla con las normas de seguridad de la información (Chen & Li, 2014).

La investigación apoya la idea de que el comportamiento de omisión de los empleados de una organización, hacia el cumplimiento de la seguridad de la información, depende de la interacción de lo que ellos definen como control formal (amonestaciones, multas, o suspensiones, entre otros) e informal (políticas, lineamientos o normas).

Fazlida & Said, en su investigación *“Information Security: Risk, Governance and Implementation Setback”*, concluyen, después de analizar las características y diferencia entre la gobernanza de TI y la gobernanza de la seguridad de la información, que las normas ISO (en específico la ISO 27001) se identifican como marco principal para la seguridad de la información (Fazlida & Said, 2015).

Por su parte, Márquez, de la Universidad Juárez Autónoma de Tabasco, analiza la necesidad de contar con políticas de seguridad especialmente en el uso de las redes de datos de la Universidad Juárez Autónoma de Tabasco, ya que se mejoraría la operación, funcionamiento e integridad de sus sistemas informáticos e infraestructura de telecomunicaciones, adicionalmente, ofrece una comparación de las características sobre la implementación de seguridad en instituciones de educación superior de la región sur-sureste del país (Márquez, 2006).

Actualmente la seguridad de la información es un área sujeta a estudio e investigación constante alrededor del mundo, principalmente impulsada por los acontecimientos mencionados al inicio de esta investigación, y los trabajos mencionados anteriormente pretenden mostrar los diversos enfoques que se pueden encontrar.

2.2 Marco conceptual

2.2.1 Datos e información

Un dato puede ser definido como un conjunto de hechos objetivos y discretos sobre los eventos, y en un contexto organizacional, los datos se describen más útilmente como registros estructurados de transacciones (Davenport & Prusak, 1998), es decir, son la unidad mínima de información.

Se denomina información a un conjunto de datos relacionados entre sí, es decir, una estructura de datos. Sin embargo, no cualquier estructura de datos constituye información: la información está siempre referida a objetos concretos o ideales, pero siempre bien especificados y contextualizados. No hay información si no hay posibilidad de interpretación, que es lo que hace a la información comunicable de una persona a otra (Enciclopedia de ciencias y tecnologías en Argentina, 2017).

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración (ISO27000.es, 2005).

2.2.2 Sistemas de información

Es posible plantear la definición técnica de un sistema de información como un conjunto de componentes interrelacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar los procesos de toma de decisiones y de control en una organización. Además de apoyar la toma de decisiones, la coordinación y el control, los sistemas de información también pueden ayudar a los gerentes y trabajadores del conocimiento a analizar problemas, visualizar temas complejos y crear nuevos productos (Laudon & Laudon, 2012).

Kendall & Kendall mencionan que dentro de los principales sistemas de información se encuentran los administrativos, que son sistemas de información computarizados que funcionan debido a la decidida interacción entre las personas y las computadoras. Al requerir que las personas, el software y el hardware funcionen en concierto, los sistemas de información administrativos brindan soporte a los usuarios para realizar un espectro más amplio de tareas organizacionales, incluyendo los procesos de análisis y toma de

decisiones. Para acceder a la información, los usuarios del sistema de información administrativa comparten una base de datos común; ésta almacena tanto los datos como los modelos que permiten al usuario interactuar con ellos, interpretarlos y aplicarlos. Los sistemas de información administrativa producen información que se utiliza en el proceso de toma de decisiones. También pueden ayudar a integrar algunas de las funciones de información computarizadas de una empresa (Kendall & Kendall, 2011).

2.2.3 Tipos de seguridad

Con el propósito de ampliar el panorama en cuanto a la seguridad se refiere, Muñoz ofrece las siguientes definiciones importantes (Muñoz, 2002):

Seguridad física.

Se refiere a todos los aspectos correspondientes con la seguridad y salvaguarda de los bienes tangible de los sistemas computacionales de las empresas, tales como el hardware central, los equipos periféricos y equipos asociados, las instalaciones eléctricas, las instalaciones de comunicación y de datos, las construcciones, el mobiliario y equipo de oficina, así como la protección a los accesos al centro de comando o sistematización. Por consiguiente, es todo lo referido con la conservación de equipos, la prevención de riesgo y protección de los recursos físicos informáticos de la empresa.

Seguridad lógica.

Es lo relativo con la seguridad de los bienes intangibles de los centros informáticos, tales como software (programas, aplicaciones, sistemas operativos y lenguajes), así como lo concerniente con las metodologías y procedimientos de operación, los niveles de acceso a los sistemas y programas institucionales, el uso de las contraseñas, los privilegios y restricciones de los usuarios, la protección de los archivos e información de la empresa y las medidas y programas para prevenir y erradicar cualquier virus informático. En sí, todo lo concerniente con las medidas de seguridad, protección y tipos de accesos a los datos e información del sistema.

Seguridad de las bases de datos.

Es la protección específica de la información que se maneja, resguarda y protege en las áreas de sistemas de la empresa, ya sea a través de las medidas de seguridad y control que limiten

el acceso y uso de esa información, o mediante sus respaldos periódicos con el fin de mantener su confidencialidad y prevenir las alteraciones, descuido, robos y otros actos delictivos que afecten su consistencia.

Seguridad en la operación.

Se refiere a la seguridad en la operación de los sistemas computacionales en cuanto a su acceso y aprovechamiento por parte del personal informático y de los usuarios, al acceso a la información y los programas institucionales, a la forma de proteger la operación de los equipos, los archivos y programas, así como las instalaciones, mobiliario, etcétera.

Seguridad del personal de informática.

Se refiere a la seguridad y protección de los operadores, analistas, programadores y demás personal que está en contacto directo con el sistema, así como a la seguridad de los beneficiarios de la información.

Seguridad de las telecomunicaciones.

Es todo lo relacionado con la seguridad y protección de los niveles de acceso, privilegios, recepción y envío de información por medio del sistema de cómputo, protocolos, software, equipos e instalaciones que permiten la comunicación y transmisión de la información en la empresa, etcétera.

Seguridad en las redes.

Es todo lo relacionado con la seguridad y control de contingencias para la protección adecuada de los sistemas de redes de cómputo, en cuanto a las salvaguardas de información y datos de las redes, la seguridad en el acceso a los sistemas computacionales, a la información y a los programas del sistema, así como la protección de accesos físicos, del mobiliario, del equipo y de los usuarios de los sistemas, incluyendo el respaldo de la información y los privilegios de accesos a sistemas, información y programas.

2.2.4 Seguridad de la información

Según la ISO/IEC 27000 la seguridad de la información tiene por objetivo preservar las siguientes propiedades de la información (International Organization for Standardization & International Electrotechnical Commission, 2018):

- Confidencialidad (no está disponible o divulgada a personas, entidades o procesos no autorizados).
- Integridad (precisas y sin cambios).
- Disponibilidad (es accesible y utilizable a pedido de una entidad autorizada).

Política de Seguridad de la información

Según la ISO/IEC 27000, una política expresa una intención y dirección de una organización, y esta expresada formalmente por su alta dirección (International Organization for Standardization & International Electrotechnical Commission, 2018).

La política de seguridad puede ser definida como un conjunto de documentos o directivas que se encuentran sistematizadas y que indican las normas y actuaciones que se deben cumplir, y que son la base en la que se centra el diseño del sistema de seguridad de la organización (International Organization for Standardization & International Electrotechnical Commission, 2013a). Cabe destacar que no son elementos inmóviles, sino que se trata de directivas que se encuentran en constante evolución.

En la literatura es posible encontrar muchas definiciones para una política de seguridad de la información, la cual debe expresar el compromiso formal de la administración para la implementación y mejora de su sistema de gestión de la seguridad de la información y debe incluir objetivos de seguridad de la información o facilitar su desarrollo.

Chen y Li, afirman que la gerencia utiliza una política de seguridad de la información para diferenciar entre los comportamientos de los empleados que están permitidos o prohibidos, así como las sanciones consiguientes si se producen los comportamientos prohibidos (Chen & Li, 2014).

La ISO/IEC 270001 menciona que la política de seguridad de la información debe estar disponible como información documentada, comunicada dentro de la organización y estar disponible a las partes interesadas según sea apropiado (International Organization for Standardization & International Electrotechnical Commission, 2013a).

Por otro lado, la ISO/IEC 27002 establece que el objetivo de una política de seguridad de la información es proporcionar a la administración, dirección y soporte de acuerdo con los requisitos y regulaciones del negocio cuando se trata de la seguridad de la información (International Organization for Standardization & International Electrotechnical Commission, 2013b).

2.2.5 Normas ISO/IEC de seguridad de la información

Las normas establecen la necesidad de sistematizar y formalizar, en una serie de procedimientos, toda una serie de procesos empresariales relativos a los diferentes ámbitos de la gestión empresarial (Heras & Casadesús, 2006). La estandarización o normalización se podría definir, de forma genérica, como la actividad encaminada a poner orden en aplicaciones repetitivas que se desarrollan en el ámbito de la industria, la tecnología, la ciencia y la economía (Escalera & Pascual, 2004).

La Organización Internacional de Normalización (ISO por sus siglas en inglés) es una organización no gubernamental formada por las organizaciones de estandarización de varios países, incluido México. Se le considera el mayor desarrollador mundial de estándares internacionales, que facilita el comercio mundial proporcionando estándares comunes entre países (ISOTools, 2017).

La Comisión Electrotécnica Internacional (IEC por sus siglas en inglés) es una organización de normalización en los campos: eléctrico, electrónico y tecnologías relacionadas, sin fines de lucro y fundada en 1906. Los miembros de IEC son Comités Nacionales, y nombran expertos y delegados provenientes de la industria, organismos gubernamentales, asociaciones e instituciones académicas para participar en el trabajo técnico y de evaluación de conformidad de IEC (International Electrotechnical Commission, 2019).

ISO/IEC 27000

Esta norma proporciona una visión general de todas las normas que componen la serie 27000 e indican el alcance y propósito de cada una de ellas, y de la misma manera recolecta todas las definiciones relacionadas con la serie de normas 27000, además de mencionar una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI) (International Organization for Standardization & International Electrotechnical Commission, 2018).

ISO/IEC 27001

La norma ISO/IEC 27001 es la principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información, adema que enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO/IEC 27002, para que sean seleccionados por las organizaciones en el desarrollo de sus sistemas de gestión de la seguridad de la información (International Organization for Standardization & International Electrotechnical Commission, 2013a).

ISO/IEC 27002

La norma ISO/IEC 27002 es una guía de buenas prácticas, está estructurada en 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. En total, el documento recomienda un total de 114 controles que se pueden considerar para su aplicación (aunque no es obligatorio cumplirlos todos) (International Organization for Standardization & International Electrotechnical Commission, 2013b).

El primer dominio es el de “Políticas de seguridad de la información”, el cual hace énfasis en la importancia de contar con una política de seguridad adecuada, aprobada por la dirección de la organización y comunicada al personal, también menciona la importancia de revisarla y actualizarla periódicamente.

El segundo dominio es “Organización de la seguridad de la información”, cuyos controles establecen un marco de gestión para el control de la implementación de la seguridad de la información dentro de la organización, contemplando de igual manera la seguridad en el teletrabajo y los dispositivos móviles.

El tercer dominio es “Seguridad relativa a los recursos humanos”, el cual se enfoca en las responsabilidades y obligaciones del recurso humano antes, durante y al final la relación laboral con la organización.

El cuarto es “Gestión de activos”, y centra la atención en reconocer la información como un activo y en las medidas adecuadas para protegerlos ante posibles incidentes que puedan comprometerlos.

El quinto dominio es el “Control de acceso”, y abarca los temas relacionados con la administración de los accesos mediante roles y procedimientos definidos, también incluye controles relacionados con las responsabilidades de los usuarios respecto a su información de autenticación.

El sexto dominio es “Criptografía”, el cual es aplicable especialmente en los casos donde se trate con información considerada sensible o critica para la organización, sus controles se enfocan en el uso de algoritmos criptográficos para proteger la información, así como en la gestión de claves.

El séptimo dominio, “Seguridad física y del entorno” concentra los controles enfocados a prevenir el acceso físico no autorizado a las áreas donde se encuentre información y recursos de importancia para la organización, así como los relacionados con evitar la pérdida, daño o robo de los activos.

El octavo, “Seguridad de las operaciones”, prioriza el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información, y de igual manera la protección contra el software malicioso y la perdida de datos, además, propone el registro de eventos de las actividades de los usuarios sin olvidar la protección de la privacidad.

El noveno dominio abarca la “Seguridad de las comunicaciones”, y parte de la base de que se debe proteger adecuadamente los medios de transmisión de los datos, sobre todo si se toma en cuenta las diversas tecnologías que interactúan en, por ejemplo, las redes de datos.

El décimo es el de “Adquisiciones, desarrollo y mantenimiento de los sistemas de información”, en el cual se busca garantizar que la seguridad de la información sea parte integral de los sistemas de información utilizados tanto por la organización como los que proporcionan los servicios a través de redes públicas.

El undécimo dominio abarca la “Relación con proveedores”, y busca asegurar la protección de los activos de la organización que sean accesibles a los proveedores, además de mantener un nivel acordado de seguridad entre ambas partes.

El duodécimo es la “Gestión de incidentes de seguridad de la información”, el cual cuenta con los controles para la gestión de incidentes de seguridad de la información, como la recopilación de evidencias y aprendizaje de los incidentes que se puedan presentar.

El décimo tercer dominio engloba los “Aspectos de seguridad de la información para la gestión de la continuidad del negocio”, y se centra en la verificación, revisión y evaluación de la continuidad de la seguridad de la información.

Por último, el décimo cuarto dominio es el “Cumplimiento”, y que busca evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad, como, por ejemplo, los derechos de propiedad intelectual o la protección y privacidad de la información de carácter personal.

A pesar de no ser obligatoria la implementación de absolutamente todos los controles enumerados en la norma, cada organización que se disponga a implementarla deberá argumentar las razones por las cuales se seleccionaron, o no, los controles.

2.2.6 Análisis de riesgos (MAGERIT)

La evaluación de riesgos o análisis de riesgos es el proceso de identificar los riesgos de seguridad para un sistema, así como determinar su probabilidad de ocurrencia, su impacto y las medidas salvaguardas que mitigarían ese impacto. La evaluación de riesgos es uno de los pasos en el proceso de gestión de riesgos. El principal problema en la evaluación de riesgos es, cómo evaluar todos los riesgos en un sistema u organización para que, al utilizar el resultado de la evaluación de riesgos, estas organizaciones puedan definir controles apropiados para reducir o eliminar esos riesgos (Syalim, Hori, & Sakurai, 2009).

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) fue elaborada por el Consejo Superior de Administración Electrónica (CSAE) del gobierno Español, como respuesta a la percepción de que la Administración Pública (y en general toda la sociedad) depende de forma creciente de los sistemas de información para alcanzar sus objetivos (Ministerio de Hacienda y Administraciones Públicas de España, 2012a).

Según el portal de administración electrónica de España, MAGERIT permite estudiar los riesgos que soporta un sistema de información y el entorno asociado a él, además, MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados. Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios (Consejo Superior de Administración Electrónica, 2010).

MAGERIT persigue los siguientes objetivos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).

- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

2.2.7 Otros conceptos

Incidente

La norma ISO/IEC 27035 menciona que un Incidente, de Seguridad de la Información, es indicado por un único o una serie de eventos seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información (International Organization for Standardization & International Electrotechnical Commission, 2016).

Riesgo

El riesgo puede ser definido como la posibilidad de que algo que ocurra impacte negativamente sobre la información o sobre los recursos para gestionarla, la probabilidad de ocurrencia es el producto del análisis sobre datos históricos respecto a cuántas veces sucedió un hecho similar en un periodo de tiempo que se tomará como unidad. Se entiende por consecuencias, el impacto, es decir, los hechos o acontecimientos que resultan de uno o varios eventos evaluados para esa organización (Prandini & Pallero, 2013).

Amenaza

El concepto hace referencia a una situación potencial que supone un daño para un activo o para un control implementado en una organización, con cierta probabilidad de ocurrencia. También es factible definir a una amenaza como una violación potencial a la seguridad y, en ese sentido, para el contexto informático debe interpretarse para la seguridad de la información (Prandini & Pallero, 2013).

En la ISO/IEC 27000 se comprende como amenaza, a la causa potencial de un incidente no deseado, que puede ocasionar daños a un sistema u organización, y que surge a partir de la existencia de vulnerabilidades que pudieran ser aprovechadas (International Organization for Standardization & International Electrotechnical Commission, 2018).

Vulnerabilidad

Una vulnerabilidad es una debilidad de un bien o de un control, que puede ser aprovechada por una amenaza. Se trata de una característica negativa del bien, también conocido como activo o recurso de

información, o de un control que se implementó sobre él, que lo hace vulnerable. En efecto esa vulnerabilidad es susceptible de ser aprovechada y varía de acuerdo con los cambios en las condiciones que dieron origen a su existencia o a las acciones que se tomen con el fin de evitar su explotación o aprovechamiento (Prandini & Pallero, 2013).

Capítulo 3. Análisis y desarrollo de instrumentos

Una investigación es científicamente válida al estar sustentada en información verificable, y para ello, es imprescindible realizar un proceso de recolección de datos en forma planificada y teniendo claros objetivos sobre el nivel y profundidad de la información a recolectar (Torres, Paz, & Salazar, 2006). En este tercer capítulo se describe el análisis situacional inicial de la Coordinación de Desarrollo y Soporte de Sistemas, así como el diseño de tres instrumentos de recolección de información, dos de ellos basados en la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, y uno basado en la norma ISO/IEC 27002:2013.

3.1 Análisis de la Coordinación de Desarrollo y Soporte de Sistemas

La reunión inicial se llevó a cabo en las instalaciones de la Coordinación de Desarrollo y Soporte de Sistemas, el día 17 de octubre del 2018, estando presente el Coordinador de la Coordinación de Desarrollo y Soporte de Sistemas y el autor del presente documento, en dicha reunión se explicaron los objetivos y alcances del proyecto, así como los beneficios de este para la Coordinación de Desarrollo y Soporte de Sistemas.

Posteriormente, se llevaron a cabo 5 reuniones en las que se discutieron las características de su entorno de trabajo (distribución del personal, marco normativo de la Dirección de Tecnologías de Información e Innovación, entre otros), así como las funciones del personal que labora en la Coordinación de Desarrollo y Soporte de Sistemas, y las problemáticas de seguridad de la información que se han presentado en la Coordinación, entre otros temas.

Las reuniones se realizaron con el personal encargado de las 5 funciones principales en la Coordinación de Desarrollo y Soporte de Sistemas, estas son: el desarrollo de software, la administración de las bases de datos, la administración del correo electrónico institucional, la administración de la página web y la creación de la documentación de los sistemas de información.

Mediante las reuniones en la Coordinación de Desarrollo y Soporte de Sistemas fue posible identificar que los empleados han sufrido incidentes relacionados con la seguridad de su información, como

lo son la perdida de información derivado del extravío de dispositivos de almacenamiento (memorias tipo USB), perdida de información por la omisión en la creación de respaldos, e inclusive el robo de equipos de cómputo (laptops). La tabla 1 enlista los incidentes comunes de seguridad de la información encontrados en las áreas de la Coordinación de Desarrollo y Soporte de Sistemas (CDSS):

Tabla 1. *Incidentes de seguridad de la información en la CDSS.*

Funciones de la Coordinación de Desarrollo y Soporte de Sistemas		**Incidentes para la seguridad de la información**
1	Desarrollo de software	Perdida de datos debido a errores humanos
2	Administración de bases de datos	Fallas de hardware, acceso no autorizado y fallas eléctricas en el centro de datos, obsolescencia del almacenamiento.
3	Administración del correo electrónico	Perdida de datos debido a errores humanos (bajas a equipos que contenían información en uso).
4	Administración de página web	Fallas de equipos de cómputo.
5	Documentación	Fallas de equipos de cómputo y errores humanos (información eliminada sin respaldo previo).

3.2 Diseño de los instrumentos de recolección de información

Para el presente trabajo, se optó por utilizar 3 diferentes instrumentos recolección de información, el primer instrumento para identificar los activos críticos de información de la Coordinación de Desarrollo y Soporte de Sistemas, el segundo para identificar las vulnerabilidades y amenazas de dichos activos de información (ambos instrumentos están compuestos por las características planteadas en la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información versión 3), y el tercero para evaluar el grado de cumplimiento de los controles de la norma ISO/IEC 27002:2013.

Instrumento 1: Identificación de activos de información

El primer instrumento tuvo por objetivo identificar cada uno de los activos de información que se encuentran presentes en las instalaciones de la Coordinación de Desarrollo y Soporte de Sistemas, los cuales fueron identificados según los criterios de la metodología MAGERIT. El formato para la identificación de activos de información puede ser visualizado a continuación en la figura 3.1:

Figura 3.1. Formato para la identificación de activos de información.

Identificación de Activos de Información										
Institución:										
Departamento:										
Resp. del departamento:										
Persona que elabora:										
Fecha:										
ID	Nombre	Descripción	Tipo	Unidad Responsable		Persona Responsable		Ubicación	Cantidad	Critico (si/no)
				Mantiene	Explota	Responsable	Operador			
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

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

Instrumento 2: Identificación de amenazas y vulnerabilidades de los activos de información

Posteriormente, el segundo instrumento se diseñó para identificar las vulnerabilidades y amenazas para cada activo de información de la Coordinación de Desarrollo y Soporte de Sistemas, una vez más, utilizando los criterios de MAGERIT. El formato para la identificación de vulnerabilidades y amenazas puede ser visualizado a continuación en la figura 3.2:

Figura 3.2. Formato para la identificación de vulnerabilidades y amenazas.

Identificación de Vulnerabilidades y Amenazas			
Institución:			
Departamento:			
Resp. del departamento:			
Persona que elabora:			
Fecha:			
ID	Activo	Vulnerabilidad	Amenaza
1			
2			
3			
4			
5			

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

Instrumento 3: Grado de cumplimiento de controles de la norma ISO/IEC 27002:2013

El tercer instrumento tuvo por objetivo evaluar el grado de cumplimiento de seguridad de información de la Coordinación de Desarrollo y Soporte de Sistemas en cuanto a los controles de la norma ISO/IEC 27002:2013, para lo cual se adaptó la herramienta propuesta por Tovar y Salguero, la cual consiste en una lista de cotejo (*checklist*) de los controles de la norma, estableciendo un nivel de madurez de los controles según los niveles de madurez de procesos establecidos en la norma ISO/IEC 21827, dicho instrumento pude ser visualizado en la figura 3.3 (Tovar & Salguero, 2018).

Figura 3.3. Herramienta para la evaluación de controles de ISO/IEC 27002:2013.

ISO/IEC 27002:2013 Herramienta de Evaluacion de Controles		CRITERIOS DE EVALUACIÓN	
		No realizado	0%
		Realizado informalmente	20%
		Planificado	40%
		Bien definido	60%
		Cuantitativamente controlado	80%
		Mejora continua	100%
Norma	**Seccion**		
5	**Políticas de seguridad de la información**	**0%**	
5.1	**Directrices de gestión de la seguridad de la información**	**0%**	
5.1.1	Políticas para la seguridad de la información	**No realizado**	0%
5.1.2	Revisión de las políticas para la seguridad de la información	**No realizado**	0%
8	**Gestión de activos**	**0%**	
8.1	**Responsabilidad sobre los activos**	**0%**	
8.1.1	Inventario de activos	**No realizado**	0%
8.1.2	Propiedad de los activos	**No realizado**	0%
8.1.3	Uso aceptable de los activos	**No realizado**	0%
8.1.4	Devolución de activos	**No realizado**	0%
8.2	**Clasificación de la información**	**0%**	
8.2.1	Clasificación de la información	**No realizado**	0%
8.2.2	Etiquetado de la información	**No realizado**	0%
8.2.3	Manipulado de la información	**No realizado**	0%
8.3	**Manipulación de los soportes**	**0%**	
8.3.1	Gestión de soportes extraíbles	**No realizado**	0%
8.3.2	Eliminación de soportes	**No realizado**	0%
8.3.3	Soportes físicos en tránsito	**No realizado**	0%
9	**Control de acceso**	**0%**	
9.1	**Requisitos de negocio para el control de acceso**	**0%**	
9.1.1	Política de control de acceso	**No realizado**	0%

Fuente: Elaboración propia, basada en la propuesta de (Tovar & Salguero, 2018).

El nivel de madurez de los controles propuesto por Tovar y Salguero, y utilizado para este trabajo, se describe detalladamente en la tabla 2:

Tabla 2. *Descripción de los niveles de madurez*.

Niveles De Madurez		
Porcentaje	**Criterio**	**Descripción**
0%	No realizado	No hay controles de seguridad de la información establecidos.
20%	Realizado informalmente	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.
40%	Planificado	Los controles de seguridad de la información establecidos son planificados, implementados y repetibles.
60%	Bien definido	Los controles de seguridad de la información además de planificados son documentados, aprobados e implementados en toda la organización.
80%	Cuantitativamente controlado	Los controles de seguridad de la información están sujetos a verificación para establecer su nivel de efectividad.
100%	Mejora continua	Los controles de seguridad de la información definidos son periódicamente revisados y actualizados. Estos reflejan una mejora al momento de evaluar el impacto.

Fuente: (Tovar & Salguero, 2018)**.**

3.3 Descripción del instrumento para la evaluación de controles

El instrumento para evaluar el grado de cumplimiento propuesto por Tovar y Salguero y adaptado para este estudio, que como se mencionó anteriormente, consiste en una lista de cotejo (*checklist*) de los controles de la norma, evalúa cada control seleccionado de manera individual, es decir, establece un nivel de madurez (en porcentaje) según los niveles de madurez de la tabla 2.

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 en los que el objetivo de control solo contenga un único control, su valor será el de ese control.

De manera similar, el porcentaje de cumplimiento para cada dominio es calculado mediante el promedio de los valores de los objetivos de control que lo conforman, con el promedio de los valores de los objetivos de control en los casos en los que sean 2 o más, y con el mismo valor en los casos que solo cuenten con un único objetivo de control.

La tabla 3 muestra el procedimiento de cálculo para los valores de los dominios y objetivo de control que sean seleccionados como aplicables en la herramienta:

Tabla 3. *Calculo de valores del instrumento de evaluación de controles*.

Sección	Calculo 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_2)	**= $(C_1 + C_2) / 2$**
Control	C_1 %
Control	C_2 %
Objetivo de Control (OC_x)	**= $(C_1 + C_2 + \ldots + C_n) / n$**
Control	C_1 %
Control	C_2 %
Control	C_n %

donde:

- C_1 + C_2 y C_n, representan los valores del nivel de madurez de cada control individual.
- OC_1 + OC_2 y OC_x, representan los valores de cada objetivo de control.

Es necesario aclarar que la finalidad de la herramienta no es emitir una calificación aprobatoria o reprobatoria, sino identificar el nivel de madurez (o cumplimiento) de los mecanismos de seguridad de la

información actualmente implementados en la Coordinación de Desarrollo y Soporte de Sistemas respecto a la norma ISO/IEC 27002:2013, y de esta manera, identificar las prácticas de seguridad de la información que permitan mitigar vulnerabilidades y amenazas.

Selección de los controles para el instrumento de evaluación del grado de cumplimiento

La selección de los controles que integraron el instrumento de evaluación del grado de cumplimiento de la norma ISO/IEC 27002:2013 y que fueron aplicables a la Coordinación de Desarrollo y Soporte de Sistemas (CDSS) se llevó a cabo tomando como base la información obtenida mediante las entrevistas en la Coordinación, obteniendo de esta manera los dominios, objetivos de control y controles, como se muestra en la taba 4.

Tabla 4. *Apartados de la ISO/IEC 27002:2013 aplicables a la CDSS*.

Apartado	**ISO/IEC 27002:2013**	**Aplicable a la Coordinación de Desarrollo y Soporte de Sistemas**
Dominios	14	9
Objetivos de control	35	23
Controles	114	70

Para una mejor comprensión, la tabla 5 muestra los dominios considerados como aplicables y no aplicables para la Coordinación de Desarrollo y Soporte de Sistemas (CDSS):

Tabla 5. *Dominios aplicables para la CDSS*.

Norma	Dominio	Aplicable	No aplicable
5	Políticas de seguridad de la información	X	
6	Organización de la seguridad de la información		X
7	Seguridad relativa a 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 mantenimiento de los sistemas de información	X	
15	Relación con proveedores	X	
16	Gestión de incidentes de seguridad de la información	X	
17	Aspectos de seguridad de la información para la gestión de la continuidad del negocio		X
18	Cumplimiento		X

De los 14 dominios se consideraron aplicables 9, estando integrados estos por un total de 23 objetivos de control y 70 controles, de igual manera, se consideraron no aplicables 5 dominios, 12 objetivos de control y 34 controles, los cuales no se incluyeron en el instrumento de la evaluación del grado de cumplimiento de la norma.

En lo que respecta a los dominios que se consideraron como no aplicables, en la tabla 6 se muestran las razones por las cuales se consideraron de dicha manera:

Tabla 6. *Detalles de los dominios no aplicables para la CDSS*.

Norma	Dominio	Razones
6	Organización de la seguridad de la información	Este dominio busca instaurar un marco de referencia para definir el proceso para la implantación y control de la seguridad de la información dentro de organización, es decir, es aplicable durante el proceso de la implementación de un sistema de gestión de seguridad de la información, y para este estudio no es el caso.
7	Seguridad relativa a los recursos humanos	Este dominio se enfoca en las responsabilidades y obligaciones del recurso humano antes, durante y al final la relación laboral, pero para el caso de este estudio, no se consideró al recurso humano como un activo de información, ya que se consideró únicamente a los activos tecnológicos de la Coordinación de Desarrollo y Soporte de Sistemas.
10	Criptografía	Este dominio es aplicable en los casos donde se utilicen algoritmos criptográficos para proteger la información, así como en la gestión de claves, y en el caso de la Coordinación de Desarrollo y Soporte de Sistemas no se utilizan métodos criptográficos actualmente.
17	Aspectos de seguridad de la información para la gestión de la continuidad del negocio	Este dominio se centra en la continuidad de la seguridad durante un evento de interrupción (crisis o desastre), y estas actividades no son responsabilidad de la Coordinación de Desarrollo y Soporte de Sistemas sino de otro departamento de la Dirección de Tecnologías de Información e Innovación, tal como es descrito en el manual general de organización de la Universidad Juárez Autónoma de Tabasco.
18	Cumplimiento	Este dominio busca evitar incumplimientos de las obligaciones legales o reglamentarias relativas a la seguridad de la información, y no se consideró aplicable ya que, como se mencionó, los controles se limitaron a la seguridad de los activos de información tecnológicos de la Coordinación de Desarrollo y Soporte de Sistemas

En el apéndice A se encuentra la herramienta completa utilizada para la evaluación de controles utilizada en la Coordinación de Desarrollo y Soporte de Sistemas.

Capítulo 4. Resultados

En la práctica, la ciencia que transmite mejor sus resultados es la más útil, por ello es prioritario comunicar los resultados (Cáceres, 2014). En este capítulo se detallan los resultados obtenidos a través de los tres instrumentos de recolección de información descritos en el capítulo tercero, y que, a su vez, permiten lograr el objetivo de este estudio, el cual es elaborar una propuesta de prácticas de seguridad de la información para la Coordinación de Desarrollo y Soporte de Sistemas, incluida en este mismo capítulo.

4.1 Activos de información

Identificación de activos de información de la Coordinación de Desarrollo y Soporte de Sistemas

Con la aplicación del primer instrumento de evaluación, fue posible identificar 13 tipos de activos de información en la Coordinación de Desarrollo y Soporte de Sistemas (CDSS), los cuales están ubicados en 2 áreas (oficina de la Coordinación y el centro de datos), como se muestra en la tabla 7.

Tabla 7**.** *Identificación de activos de información de la CDSS.*

Tipo	Activo
Equipamiento informático (hardware)	PC Servidores físicos Servidores virtuales Impresoras Escáner Switch Teléfonos IP
Claves de cifrado	Claves de autenticación
Soportes de información	S.A.N. Memorias USB Discos duros externos
Instalaciones	Centro de datos Oficina de la Coordinación

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

Identificación de amenazas y vulnerabilidades de los activos de información

Posteriormente, y mediante las reuniones que se realizaron con el personal, se identificaron vulnerabilidades y amenazas para los activos de información de la Coordinación de Desarrollo y Soporte de Sistemas identificados, como se muestra en la tabla 8.

Tabla 8**.** *Identificación de amenazas y vulnerabilidades.*

Tipo	Activo	Vulnerabilidad	Amenaza
Equipamiento informático (hardware)	PC	Errores de los usuarios	Perdida de información por respaldos no periódicos
	Servidores físicos	Agotamiento de recursos	Caída del sistema y denegación de servicio
	Servidores virtuales		
	Impresoras	Obsolescencia del hardware	Averías de origen físico o lógico no reparables
	Escáner		
	Switch		
	Teléfonos IP		
Claves de cifrado	Claves de autenticación	Robo de credenciales de acceso	Suplantación de la identidad del usuario y acceso no autorizado
Soportes de información	S.A.N.	Degradación de los soportes de almacenamiento	Perdida de información
	Memorias USB		
	Discos duros externos		
Instalaciones	Centro de datos	Desastres naturales	Inundación o incendio en las instalaciones
	Oficina de la Coordinación		

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

4.2 Grado de cumplimiento de controles

Una vez aplicado el instrumento que permitió conocer el grado de cumplimiento de la norma ISO/IEC 27002:2013 se obtuvieron los siguientes resultados:

En la tabla 9 se encuentran los porcentajes de cumplimiento para cada uno de los 9 dominios seleccionados, en donde se aprecia un promedio de cumplimiento general de los dominios del 32%, siendo el apartado 12 de la norma (Seguridad de las operaciones) el que mayor grado de cumplimiento presentó, así como el 5 (políticas de seguridad de la información) el que menor grado de cumplimiento obtuvo (0%).

Tabla 9**.** *Cumplimiento por dominio en la CDSS.*

Norma	Dominio	Porcentaje de cumplimiento
5	Políticas de seguridad de la información	0%
8	Gestión de activos	29%
9	Control de acceso	37%
11	Seguridad física y del entorno	41%
12	Seguridad de las operaciones	51%
13	Seguridad de las comunicaciones	35%
14	Adquisición, desarrollo y mantenimiento de los sistemas de información	45%
15	Relación con proveedores	40%
16	Gestión de incidentes de seguridad de la información	6%
Promedio de cumplimiento general		32%

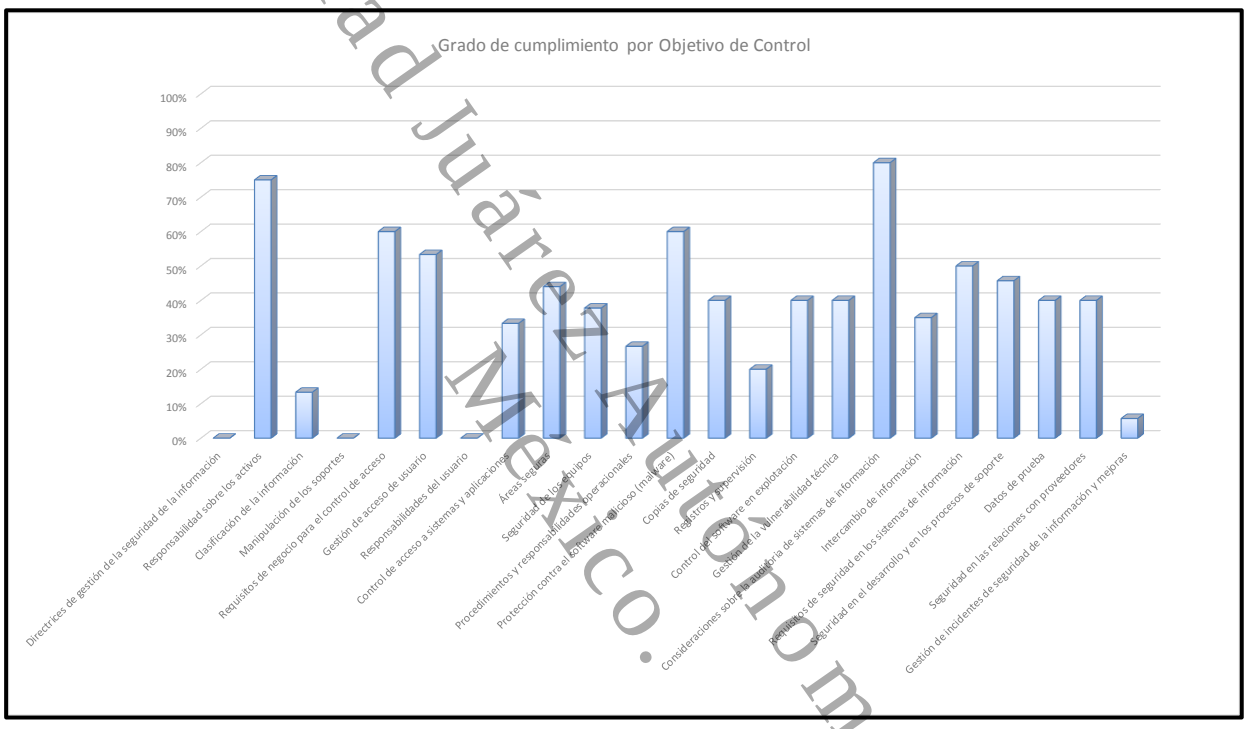
En lo que respecta a los objetivos de control, la tabla 10 muestra el porcentaje de cumplimiento para cada uno de los 23 seleccionados, en donde se aprecia un promedio de cumplimiento general de los objetivos de control del 37%.

Tabla 10. *Cumplimiento por objetivos de control en la CDSS*.

Norma	Objetivos de Control	Porcentaje de cumplimiento
5.1	Directrices de gestión de la seguridad de la información	0%
8.1	Responsabilidad sobre los activos	75%
8.2	Clasificación de la información	13%
8.3	Manipulación de los soportes	0%
9.1	Requisitos de negocio para el control de acceso	60%
9.2	Gestión de acceso de usuario	53%
9.3	Responsabilidades del usuario	0%
9.4	Control de acceso a sistemas y aplicaciones	33%
11.1	Áreas seguras	44%
11.2	Seguridad de los equipos	38%
12.1	Procedimientos y responsabilidades operacionales	27%
12.2	Protección contra el software malicioso	60%
12.3	Copias de seguridad	40%
12.4	Registros y supervisión	20%
12.5	Control del software en explotación	40%
12.6	Gestión de la vulnerabilidad técnica	40%
12.7	Consideraciones sobre la auditoria de sistemas de información	80%
13.2	Intercambio de información	35%
14.1	Requisitos de seguridad en los sistemas de información	50%
14.2	Seguridad en el desarrollo y en los procesos de soporte	46%
14.3	Datos de prueba	40%
15.1	Seguridad en las relaciones con proveedores	40%
16.1	Gestión de incidentes de seguridad de la información y mejoras	6%
Promedio de cumplimiento general		37%

Solo los apartados 5.1, 8.3 y 9.3 de la norma presentaron un grado de cumplimiento de 0%, debido tanto a la falta de una política de seguridad de la información, como de procedimientos definidos para dichos apartados. Por otra parte, el objetivo de control 12.7 de la norma (consideraciones sobre la auditoria de sistemas de información), fue el que presento mayor grado de cumplimiento (80%), ya que la Coordinación de Desarrollo y Soporte de Sistemas planea y se ejecuta auditorías para los sistemas de información. En la figura 4.1 se aprecia la representación gráfica de la tabla anterior para una mejor comprensión.

Figura 4.1. Cumplimiento por objetivos de control en la CDSS.



Con relación al cumplimiento individual de cada uno de los 70 controles, se mencionarán únicamente los que integran la sección 14 de la norma en la tabla 11, con la finalidad de mantener la confidencialidad de la información de la Coordinación de Desarrollo y Soporte de Sistemas (CDSS).

Tabla 11. *Cumplimiento de la sección 14 de la norma en la CDSS*.

Norma	Sección	Cumplimiento	
14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**	**45%**	
14.1	**Requisitos de seguridad en los sistemas de información**	**50%**	
14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	**Bien definido**	60%
14.1.3	Protección de las transacciones de servicios de aplicaciones	**Planificado**	40%
14.2	**Seguridad en el desarrollo y en los procesos de soporte**	**46%**	
14.2.1	Política de desarrollo seguro	**Bien definido**	60%
14.2.2	Procedimiento de control de cambios en sistemas	**Bien definido**	60%
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en SO	**Bien definido**	60%
14.2.4	Restricciones a los cambios en los paquetes de software	**Planificado**	40%
14.2.6	Entorno de desarrollo seguro	**Planificado**	40%
14.2.7	Externalización del desarrollo de software	**No realizado**	0%
14.2.8	Pruebas funcionales de seguridad de sistemas	**Bien definido**	60%
14.3	**Datos de prueba**	**40%**	
14.3.1	Protección de los datos de prueba	**Planificado**	40%

Por último, respecto a los 70 controles aplicables de la norma ISO/IEC 27002:2013 en la Coordinación de Desarrollo y Soporte de Sistemas, la evaluación de los controles se resume en la tabla 12, donde se visualiza la cantidad de controles por grado de cumplimiento y su equivalencia en porcentaje.

Tabla 12. *Cumplimiento de controles por nivel*.

Grado de cumplimiento	Controles en la Coordinación de Desarrollo y Soporte de Sistemas
No realizado	24
Realizado informalmente	2
Planificado	20
Bien definido	17
Cuantitativamente controlado	4
Mejora continua	3
Total	**70**

4.3 Análisis de los resultados

Como resultado de la evaluación de los 9 dominios de la norma ISO/IEC 27000:2013, fue posible identificar los mecanismos actualmente implementados en la Coordinación de Desarrollo y Soporte de Sistemas para la seguridad de la información, así como las oportunidades de mejora que pueden preparar a la Coordinación para optar por la certificación a futuro de la norma ISO/IEC 27001. Resulta necesario mencionar que, para poder realizar el presente estudio fue necesaria la revisión de las normas ISO/IEC 27000:2018 y 27001:2013, ya que dichas normas proveen información complementaria para la correcta interpretación de la norma utilizada (ISO/IEC 27000:2013).

Análisis por dominio

Durante el proceso de evaluación fue posible identificar que la Coordinación de Desarrollo y Soporte de Sistemas, si bien cuenta con procedimientos enfocados a la seguridad de su información, los procedimientos de seguridad correspondientes al 29% de los controles (20 controles) no llegan a estar documentados, sino que son implementados de manera informal y a conciencia de los empleados, lo cual reduce en cierta manera su efectividad. A continuación, se mencionan detalles de los resultados de la evaluación por dominio:

- El dominio “Políticas de seguridad de la información”, que hace énfasis en la importancia de contar con una política de seguridad adecuada, está integrado por 1 objetivo de control y 2 controles respectivamente, presento el menor grado de cumplimiento de todos los dominios, un porcentaje de cumplimiento del 0%, esto debido a que la Coordinación de Desarrollo y Soporte de Sistemas actualmente no dispone de una política de seguridad de la información.

- El dominio “Gestión de activos”, integrado por 3 objetivos de control y 10 controles respectivamente, presento un grado de cumplimiento del 29%, ya que la Coordinación de Desarrollo y Soporte de Sistemas cuenta con procedimientos definidos en los inventarios de sus activos, pero no dispone de procedimientos establecidos para el correcto manejo de medios extraíbles, así como la clasificación y etiquetado de su información a nivel operacional o técnico.

- El dominio “Control de acceso”, que abarca los temas relacionados con la administración de los accesos mediante roles y procedimientos definidos, está integrado por 4 objetivos de control y 11 controles respectivamente, presento un grado de cumplimiento del 37%, ya que en la Coordinación de Desarrollo y Soporte de Sistemas existen procedimientos para la gestión de los privilegios de accesos establecidos e implementados, de acuerdo los criterios de evaluación utilizados, aun se requieren mejoras.

- El dominio “Seguridad física y del entorno”, que se concentra los controles enfocados a prevenir el acceso físico no autorizado a las áreas donde se encuentre información, se integra por 2 objetivos de control y 14 controles respectivamente, presento un grado de cumplimiento del 41%, dado que la Coordinación de Desarrollo y Soporte de Sistemas dispone de procedimientos para el acceso físico a sus activos de información, desafortunadamente, los controles relacionados con las áreas de trabajo individuales de los usuarios obtuvieron resultados más bajos, lo que representa una oportunidad de mejora para la Coordinación.

- El dominio “Seguridad de las operaciones”, que prioriza el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información, y de igual manera la protección contra el software malicioso y la perdida de datos, está integrado por 7 objetivos de control y 10 controles respectivamente, presento el mayor grado de cumplimiento de todos los dominios, un grado de cumplimiento del 51%, a causa de que la Coordinación de Desarrollo y Soporte de Sistemas implementa medidas de seguridad como la protección contra software malicioso y copias de seguridad, así como auditorías.

- El dominio “Seguridad de las comunicaciones”, parte de la base de que se debe proteger adecuadamente los medios de transmisión de los datos, está integrado por 1 objetivo de control y

4 controles respectivamente, presento un grado de cumplimiento del 35%, en vista que en la Coordinación de Desarrollo y Soporte de Sistemas se cuenta con seguridad en las redes de datos dentro de la universidad, pero existen oportunidades de mejora en los controles relacionados con la transferencia de información a terceras partes (redes externas).

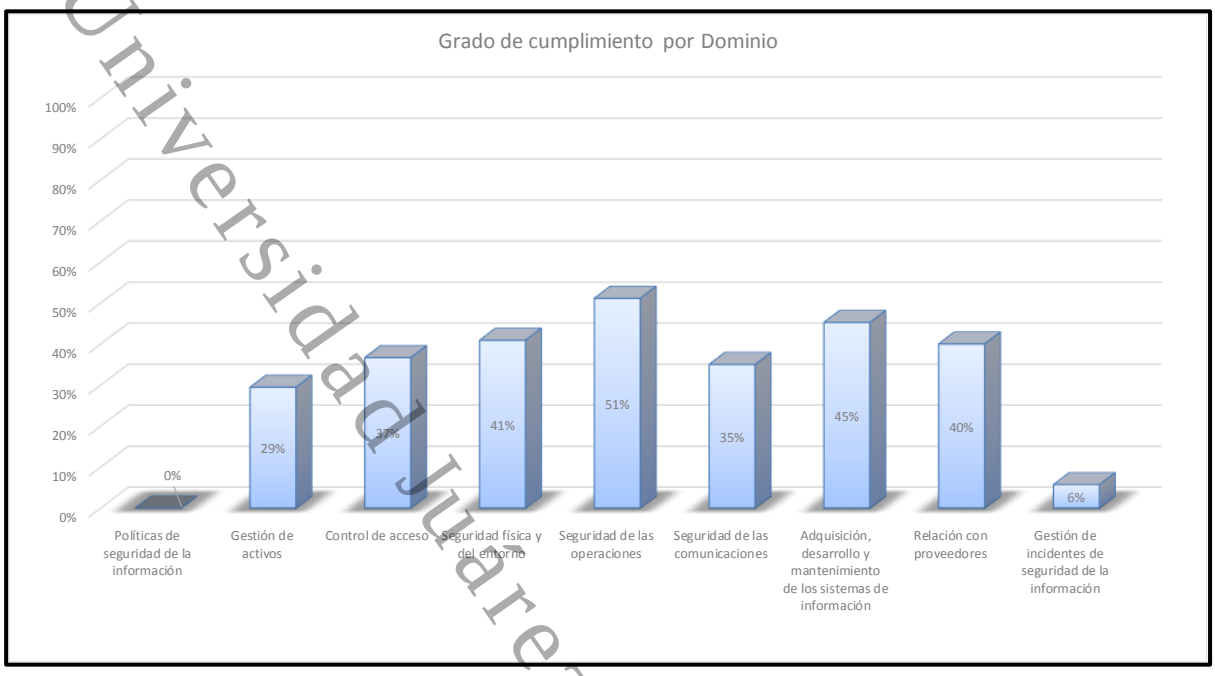
- El dominio "Adquisición, desarrollo y mantenimiento de los sistemas de información", el cual busca garantizar que la seguridad de la información sea parte integral de los sistemas de información utilizados por la organización, está integrado por 3 objetivos de control y 10 controles respectivamente, presento el segundo mayor grado de cumplimiento de todos los dominios, un grado de cumplimiento del 45%, dado que se identificaron buenos mecanismos de seguridad en los procesos de desarrollo de software.

- El dominio "Relación con proveedores", busca asegurar la protección de los activos de la organización manteniendo un nivel acordado de seguridad entre ambas partes, está integrado por 1 objetivo de control y 2 controles respectivamente, presento un grado de cumplimiento del 40%, ya que ambos controles obtuvieron el mismo resultado en la evaluación.

- El dominio "Gestión de incidentes de seguridad de la información", el cual cuenta con los controles para la gestión de incidentes de seguridad de la información, así como la recopilación de evidencias y aprendizaje de los incidentes, está integrado por 1 objetivo de control y 7 controles respectivamente, presento el segundo menor grado de cumplimiento de todos los dominios, un grado de cumplimiento del 6%, ya que, si bien, en la Coordinación de Desarrollo y Soporte de Sistemas los incidentes son gestionados adecuadamente, los controles relacionados con la recopilación de evidencias y el aprendizaje de los incidentes, presentaron un resultado nulo.

Con base en los resultados de la evaluación por dominio, resulta importante señalar que la Coordinación de Desarrollo y Soporte de Sistemas tiene grandes oportunidades de mejora, inicialmente con el establecimiento de su política de seguridad de la información, que será la base para establecer los procedimientos necesarios para asegurar la confidencialidad, integridad y disponibilidad de la información, y en un mediano plazo, poder optar por una certificación en la serie de normas ISO/IEC 27000. En la figura 4.2 se aprecia la representación gráfica de los resultados de los dominios para una mejor comprensión.

Figura 4.2. Cumplimiento por dominio en la CDSS.



Análisis por controles

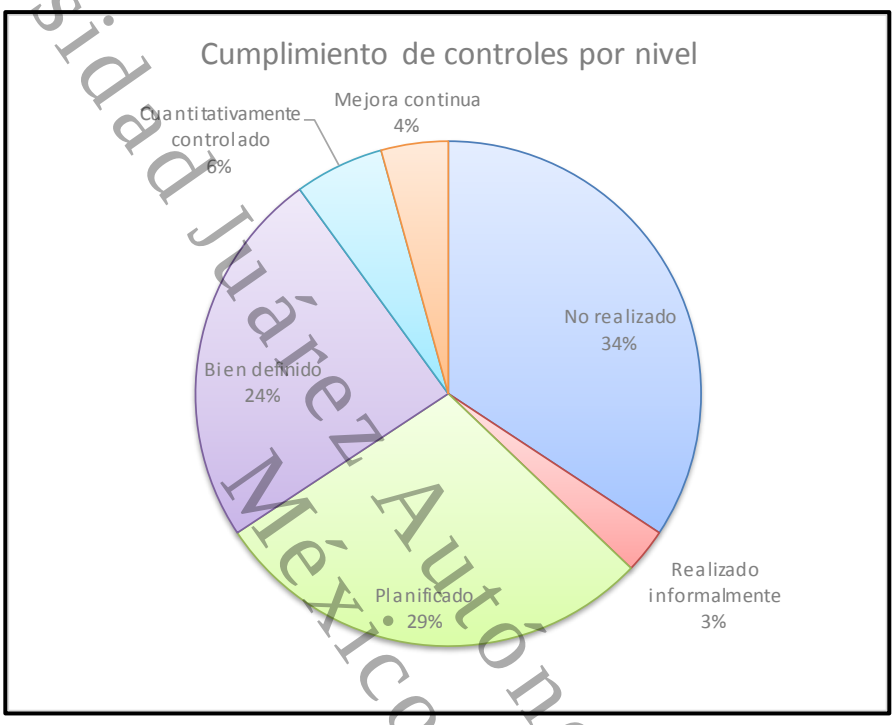
Ahora bien, respecto a la evaluación individual de los 70 controles, se pudo identificar lo siguiente:

- Para el 34% (24 controles), no se encontraron procedimientos establecidos en la Coordinación de Desarrollo y Soporte de Sistemas.
- Para el 3% (2 controles), se encontraron procedimientos, pero que desafortunadamente no fueron adoptados formalmente.
- Para el 29% (20 controles), se encontraron procedimientos implementados en la Coordinación de Desarrollo y Soporte de Sistemas.
- Para el 24% (17 controles), se encontraron procedimientos, además de que se encuentran documentados en lineamientos o manuales existentes.
- Para el 6% (4 controles), se identificó que además de estar documentados, se verifican para conocer su efectividad.

- Para el 4% (3 controles), adicionalmente a su verificación, se actualizan periódicamente para su mejora.

En la figura 4.3 se aprecia la representación gráfica de los resultados de la evaluación individual de los 70 controles por nivel.

Figura 4.3. Cumplimiento de controles por nivel.



Los resultados de la evaluación a nivel individual de los controles, muestran la necesidad de la Coordinación de Desarrollo y Soporte de Sistemas por establecer, no solamente los procedimientos de seguridad de la información para los 24 controles que se identificaron como “No realizado”, sino de establecerlos en lineamientos formales junto a los procedimientos de los 2 controles identificados como “Realizado informalmente” y los 20 identificados como “Planificados”, ya que de esta forma se formaliza y generaliza su adopción por parte de los empleados de la Coordinación.

Esto, lo que generaría sería una cultura homogénea de seguridad de la información, claro está, que el establecimiento de los procedimientos debe estar acompañado de una difusión correcta por parte de la Coordinación de Desarrollo y Soporte de Sistemas a los empleados.

Para los procedimientos o requerimientos correspondientes a los 17 controles identificados como “Bien definidos”, y los 4 identificados como “Cuantitativamente controlados”, resta decir que requieren verificaciones y revisiones periódicas para mantenerlos actualizados, con la finalidad que reflejen mejoras en la forma que son implementados en la Coordinación de Desarrollo y Soporte de Sistemas, y de esta manera mejorar la eficiencia en la seguridad de la información.

En lo que respecta a los resultados del presente estudio, es importante reiterar que el objetivo es identificar las prácticas de seguridad de la información que permitan mantener la confidencialidad, integridad y disponibilidad de la información, y la evaluación del grado de cumplimiento de los controles de la norma ISO/IEC 27002:2013 no buscó emitir una calificación, sino identificar el grado actual de cumplimiento de seguridad de información con respecto a la norma.

4.4 Propuesta de prácticas de seguridad de la información

A partir de la información obtenida durante el análisis, así como de los resultados de los instrumentos recolección de información, se proponen las siguientes prácticas de seguridad para la información basadas en la norma ISO/IEC 27002:2013, las cuales buscan ayudar a la Coordinación de Desarrollo y Soporte de Sistemas a identificar las prácticas de seguridad de la información que le permitan mantener la confidencialidad, integridad y disponibilidad de su información.

Establecimiento de una “Política de Seguridad de la Información”

Se recomienda establecer una política de seguridad de la información para gestionar los objetivos de seguridad de la información de la organización, y que contengan los principios de la seguridad de la información, así como la asignación de responsabilidades generales y específicas en materia de gestión de la seguridad de la información. Se recomienda que dicha política contemple los siguientes apartados:

- Políticas para el control de acceso.
- Políticas para el manejo y clasificación de la información.
- Políticas de seguridad física y ambiental.
- Políticas de puesto de trabajo despejado.
- Políticas de respaldos.
- Políticas de transferencia de información.

- Políticas de desarrollo seguro.
- Políticas de relaciones con proveedores.

Procedimientos para la gestión de activos

Se recomienda establecer procedimientos para la gestión de los soportes extraíbles (discos duros portátiles y memorias tipo USB), que contemplen directrices como:

- Eliminación definitiva de los contenidos de cualquier soporte extraíble que vaya a ser reutilizado o desechado.
- Almacenamiento de los soportes extraíbles en un entorno seguro y protegido.
- Implementación de técnicas criptográficas para proteger datos en soportes extraíbles.
- Implementación de múltiples copias de datos valiosos en soportes separados para reducir aún más el riesgo de daño o pérdida de los datos.

Procedimientos para la gestión de puestos de trabajos

Se recomienda establecer procedimientos de seguridad para proteger los equipos de los usuarios cuando ellos no se encuentren presentes en sus puestos de trabajo, dichos procedimientos deben asesorar a los usuarios para:

- Terminar las sesiones activas cuando deban retirarse de su área de trabajo.
- Asegurar los ordenadores personales frente a accesos no autorizados a través de un bloqueo con clave o un control equivalente.
- Prevenir el uso de fotocopias y otros dispositivos de reproducción (escáneres, cámaras digitales, o similares) por usuarios no autorizados.
- La información sensible o crítica (en papel o en soportes de almacenamiento electrónico) debe estar guardada cuando no se necesite.

Los procedimientos para mantener los puestos de trabajos despejados reducen los riesgos de accesos no autorizados, pérdida o daño de la información tanto durante las horas normales de trabajo como fuera de ellas.

Procedimientos para la gestión de capacidades

Se recomienda establecer procedimientos para supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido de los sistemas de información de la universidad. Se recomienda aplicar sistemas de control y de ajuste para asegurar, donde sea necesario, la mejora de la disponibilidad y de la eficiencia de los sistemas.

Procedimientos para el intercambio de información

Se recomienda establecer procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación considerando los siguientes aspectos:

- Procedimientos para proteger información electrónica sensible que tiene la forma de adjuntos.
- El uso de técnicas criptográficas.
- Asesorar al personal para que tome las precauciones necesarias de no revelar información confidencial.
- Acuerdos para el intercambio seguro de información entre la Coordinación y terceros.

Procedimientos para la adquisición de los sistemas de información

Se recomienda establecer procedimientos de supervisión en los casos en los que el desarrollo de software sea externalizado, es decir, cuando se subcontrata el desarrollo de un sistema, considerando los siguientes puntos:

- Pruebas de aceptación de calidad y seguridad.
- Presentación de pruebas de que se han realizado suficientes pruebas para proteger contra la presencia en los entregables de contenido malicioso, tanto intencionado como no intencionado.

- Presentación de pruebas de que se han realizado suficientes pruebas para proteger contra la presencia de vulnerabilidades conocidas.

Procedimientos para la gestión de incidentes de seguridad de la información

Se recomienda establecer procedimientos que aseguren eficazmente la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades identificadas, considerando lo siguiente:

- Procedimientos para monitorear, detectar, analizar y comunicar eventos e incidentes de seguridad de la información.
- Procedimientos para registrar las actividades de gestión de incidentes.
- Procedimientos para evaluar y tomar decisiones sobre eventos de seguridad y evaluar puntos débiles de la seguridad de la información.
- Procedimientos de respuesta a partir de un incidente, y comunicación a personas internas o externas.

También se recomienda que los incidentes de seguridad de la información sean notificados por los canales de gestión adecuados lo antes posible, todos los empleados deben conocer su responsabilidad de comunicar cualquier incidente o punto débil de seguridad de la información lo antes posible. Los incidentes de seguridad de la información deben ser respondidos de acuerdo con procedimientos documentados, incluyendo lo siguiente:

- Evidencias tan pronto como sea posible tras la ocurrencia del incidente.
- Realización de un análisis forense de la seguridad de la información (si así se requiere).
- Escalado del incidente (si así se requiere).
- Comunicación de la existencia del incidente de seguridad de la información para personas internas o externas o terceras entidades que deban tener conocimiento de este.
- Tratamiento de la debilidad o debilidades de seguridad de la información encontradas y que pudieran causar o contribuir al incidente.

- Una vez que el incidente ha sido satisfactoriamente tratado, el cierre y registro formales del mismo

El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de información debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.

Creación de programa de capacitación de seguridad de la información

Se recomienda la creación e implementación de un programa para la capacitación y educación del personal con respecto a las medidas de seguridad de la información implementadas en la Coordinación de Desarrollo y Soporte de Sistemas, en el cual se les proporcione información sobre las políticas, procedimientos e información relevante en función de sus actividades y responsabilidades.

Se recomienda que la Coordinación desarrolle el programa de capacitación y formación con el fin de llevar a cabo una capacitación y formación eficaz. El programa debe estar en consonancia con las políticas y los procedimientos relevantes de seguridad de la información de la Coordinación, teniendo en cuenta la información que ha de protegerse y los controles que se han implantado para proteger dicha información. El programa debe tener en cuenta las diferentes formas de capacitación y formación como, por ejemplo, conferencias, lecciones, seminarios o autoaprendizaje. El programa debe cubrir temas como los siguientes:

- La necesidad de conocer y cumplir con las normas y obligaciones aplicables en seguridad de la información, según se define en las políticas, normas, leyes, reglamentos, contratos y acuerdos.
- La responsabilidad personal por las propias acciones y omisiones, y las responsabilidades generales relativas a asegurar o proteger la información que pertenece a la Coordinación de Desarrollo y Soporte de Sistemas.
- Los procedimientos básicos de seguridad de la información (tales como la notificación de incidentes de seguridad de la información) y los controles básicos (tales como la seguridad de las contraseñas, los controles de software malicioso y los puestos de trabajo despejados).
- Los puntos de contacto y los recursos de información y consejos adicionales sobre cuestiones de seguridad de la información, que incluyan materiales adicionales para profundizar en la capacitación y formación en seguridad de la información.

Al elaborar el programa de capacitación resulta importante no sólo centrarse en el "qué" y "cómo", sino también en el "por qué". Es importante que los empleados entiendan el propósito de la seguridad de la información y el impacto potencial, positivo y negativo, sobre la Coordinación de Desarrollo y Soporte de Sistemas que tiene su propio comportamiento. Se recomienda también, realizar una evaluación del grado de comprensión alcanzado por los empleados al final de una actividad de concienciación, capacitación y formación para determinar el nivel de asimilación de los conocimientos transferidos.

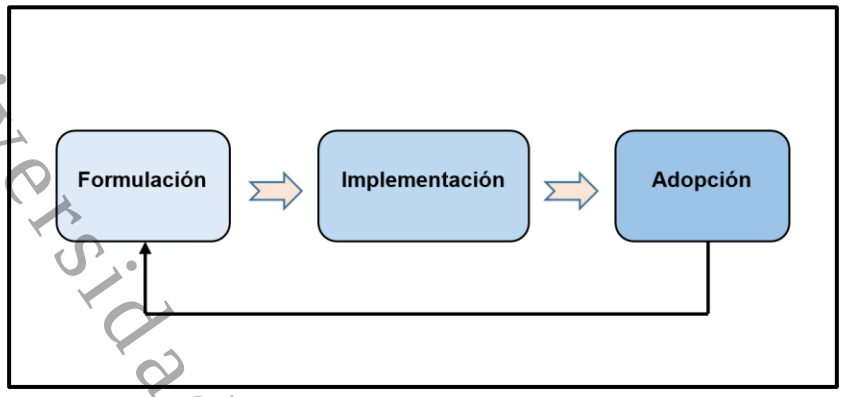
4.5 Discusión de los resultados

Durante la etapa del análisis de la Coordinación de Desarrollo y Soporte de Sistemas fue posible apreciar que, en 3 de las 5 funciones principales en la Coordinación, se han presentado incidentes relacionados con errores humanos, los cuales normalmente son causados por la falta de conciencia de la seguridad de la información, la ignorancia e inclusive negligencia, lo cual concuerda con lo mencionado por (Sohrabi Safa, Von Solms, & Furnell, 2016), quienes también mencionan la importancia del intercambio de conocimientos de seguridad de la información en los empleados.

Por otro lado, y durante la evaluación del grado de cumplimiento de los controles de la norma ISO/IEC 27002:2013, se identificó que la Coordinación de Desarrollo y Soporte de Sistemas actualmente no dispone de una política de seguridad de la información implementada que determine las prácticas de seguridad de la información en la Coordinación, lo cual, como menciona (David, 2002), ocasiona que la seguridad de la información sea arbitraria y esté sujeta a las consideraciones personales de los empleados.

Para la formulación de la política de seguridad de la información es necesario contar con la participación de los colaboradores y miembros de la Coordinación de Desarrollo y Soporte de Sistemas, involucrando sus actividades y su entorno de trabajo. (Karyda, Kiountouzis, & Kokolakis, 2005) mencionan los tres procesos involucrados en la adopción de una política de seguridad, que son: formulación, implementación y adopción. El proceso se puede visualizar en la figura 4.4:

Figura 4.4. Proceso de aplicación de una política de seguridad.



Fuente: (Karyda et al., 2005).

Por último, y en relación a la propuesta de las prácticas de seguridad de la información, es importante mencionar que al estar basadas en la serie de normas ISO/IEC 27000, reflejan la experiencia combinada de muchas compañías internacionales influyentes sobre las medidas de control relevantes, procedimientos y técnicas, que proporcionan un nivel adecuado o aceptable de seguridad de la información, tal y como lo menciona (Von-Solms, 2000), además que dichas normas están alineadas con la norma ISO 9001 e ISO 14001 con el fin de apoyar la aplicación coherente e integrada (Mesquida & Mas, 2015).

Capítulo 5. Conclusiones, recomendaciones y trabajos futuros

En este último quinto capítulo, se encuentran las conclusiones del presente estudio, las cuales adicionalmente se complementan con un apartado de recomendaciones y otro de trabajos futuros.

5.1 Conclusiones

Con base a los resultados de estudio, los cuales son mostrados en el cuarto capítulo del presente documento, se concluye que la metodología propuesta en el primer capítulo permitió cumplir exitosamente con 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 su información.

De la misma forma, se considera que los dos objetivos específicos descritos en el primer capítulo de este documento, y que se refieren al desarrollo de un diagnostico situacional del estado actual de seguridad de la información y a la formulación de una propuesta de prácticas de seguridad de la información de acuerdo a la norma ISO/IEC 27002:2013, fueron alcanzados exitosamente como se puede apreciar en el cuarto capítulo, cumpliendo de esta forma, el objetivo general del estudio.

El análisis llevado a cabo en la Coordinación de Desarrollo y Soporte de Sistemas logró identificar acertadamente, tanto los incidentes de seguridad de la información que se presentaron en el pasado, así como que, los mecanismos de seguridad de la información implementados dependen de las consideraciones personales de los empleados de cada área que integran la Coordinación.

Con respecto al uso de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), es necesario recordar que para el presente estudio sólo fueron utilizados los apartados relacionados con la identificación y clasificación de los activos de información de la Coordinación de Desarrollo y Soporte de Sistemas, así como de sus vulnerabilidades y amenazas, pero en su totalidad, esta metodología presenta un conjunto de técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos, ofreciendo elementos estandarizados que ayudan a las

organizaciones a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control, su uso se recomienda ampliamente para el proceso de valoración y planificación del tratamiento de riesgos, cuando no se dispone de la norma ISO/IEC 27005, que es la diseñada como soporte para aplicar de forma satisfactoria un Sistema de Gestión de Seguridad de la Información (SGSI) basado en el enfoque de gestión de riesgo.

Para los fines de este estudio, la adaptación de la lista de cotejo (c*hecklist*) de los controles de la norma propuesto por (Tovar & Salguero, 2018), permitió evaluar satisfactoriamente el grado de cumplimiento de seguridad de información de la Coordinación de Desarrollo y Soporte de Sistemas en cuanto a los controles de la norma ISO/IEC 27002:2013, su aplicación generó la información adicional necesaria para la construcción de la propuesta de prácticas de seguridad de la información, lo cual se considera el objetivo primordial de este trabajo. Aun así, es necesario indicar que su uso requiere conocimiento sólido y comprensión de por lo menos las normas ISO/IEC 27000, 27001 y 27002.

Mediante la aplicación instrumentos de recolección de información fue posible identificar de manera concisa la información necesaria para la formulación de la propuesta de prácticas de seguridad de la información, dentro de los hallazgos más relevantes están que: se encontraron aplicables 9 de los 14 dominios que integran la norma ISO/IEC 27002:2013, siendo el promedio general de cumplimiento de estos del 32%; se encontraron procedimientos de seguridad de información en la Coordinación para 44 de los 70 controles evaluados, es decir, para el 63% de los controles (aunque en distintos grados de cumplimiento); solamente para 26 controles no se encontraron procedimientos de seguridad de información.

En relación al grado de cumplimiento de los apartados que integran la norma ISO/IEC 27002:2013 en la Coordinación de Desarrollo y Soporte de Sistemas, resulta de importancia reiterar la importancia de contar con una política de seguridad de la información debidamente establecida y difundida en la Coordinación, ya que como se mencionó en el capítulo cuarto, el único dominio que presentó un cumplimiento nulo fue el relacionado con la presencia de una política de seguridad de la información.

La propuesta de prácticas de seguridad de la información planteada en el capítulo cuarto fue construida utilizando el conjunto de información generada por los tres diferentes instrumentos recolección de información, así como la información obtenida durante el análisis, y se encuentra integrada de manera que la Coordinación de Desarrollo y Soporte de Sistemas pueda identificar claramente las prácticas de seguridad de la información que le puedan permitir mantener la confidencialidad, integridad y disponibilidad de su información.

Adicionalmente, se considera que la Coordinación de Desarrollo y Soporte de Sistemas debe poner especial atención en la difusión de los procedimientos de seguridad de la información a los empleados, ya

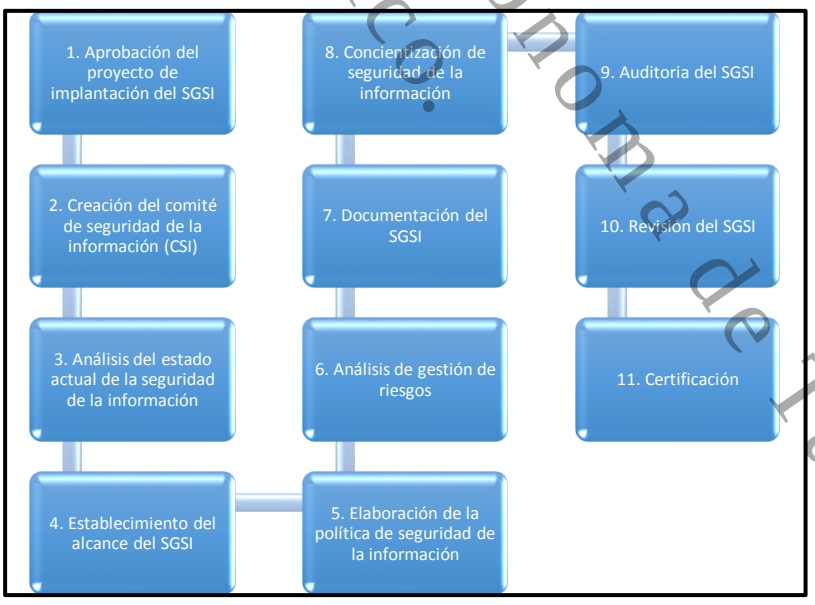
que esto puede llegar a convertirse en el factor decisivo para la mejor implementación de seguridad de información en la Coordinación.

Es comprensible que para un departamento como la Coordinación de Desarrollo y Soporte de Sistemas, en un inicio pueda parecer una labor titánica cumplir con una normatividad tan completa como lo es la ISO/IEC 27002:2013, la aportación de este documento se centra en que la Coordinación cuente con un punto de partida para que a mediano o largo plazo, los mecanismos y procedimientos relacionados con la seguridad de la información sean lo suficientemente sólidos para que la Coordinación de Desarrollo y Soporte de Sistemas o incluso la Dirección de Tecnologías de Información e Innovación opte por una certificación en la serie de normas ISO/IEC 27000.

5.2 Recomendaciones

Considerando las oportunidades de mejora para la Coordinación de Desarrollo y Soporte de Sistemas, así como para la Dirección de Tecnologías de Información e Innovación, se recomienda considerar la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI), para lo cual se propone considerar los pasos mostrados en la figura 5.1:

Figura 5.1. Método para la implantación de un SGSI.



La recomendación de implantación de un Sistema de Gestión de Seguridad de la Información se basa, de igual manera, en el caso de éxito de la certificación en la norma ISO/IEC 27001 por parte de la Universidad de Guadalajara (UdeG) en febrero de 2019 (Universidad de Guadalajara, 2019).

Adicionalmente, en la tabla 13, se menciona la documentación requerida por el ISO/IEC 27001 en el proceso de implementación de un Sistema de Gestión de Seguridad de la Información:

Tabla 13. *Documentación requerida por la ISO/IEC 27001:2013*.

Apartado de la ISO/IEC 27001	**Requisito**
4.3	Alcance del SGSI
5.2	Política de seguridad de la información
6.1.2	Metodología para la evaluación y gestión de riesgos
6.1.3 d	Declaración de aplicabilidad
6.1.3 e	Plan de tratamiento de riesgo
8.2	Informe sobre evaluación de riesgos
A.7.1.2	Definición de roles y responsabilidades de seguridad
A.8.1.1	Inventario de activos
A.8.1.3	Uso aceptable de los activos
A.9.1.1	Política de control de acceso
A.12.1.1	Procedimientos de operación para gestión de TI
A.14.2.5	Principios de ingeniería de sistemas seguros
A.15.1.1	Política de seguridad para proveedores
A.16.1.5	Procedimiento para gestión de incidentes
A.17.1.2	Procedimientos de Continuidad de negocio
A.18.1.1	Requerimientos legales, regulatorios y contractuales

5.3 Trabajos futuros

Por último, y para quienes tengan el interés de continuar con la línea de investigación del presente estudio, se proponen 4 trabajos futuros que permitirían darle continuidad:

- Implementación de un Sistema de Gestión de Seguridad de la Información en la Dirección de Tecnologías de Información e Innovación.
- Diseño e implementación de un programa de educación y capacitación de seguridad de la información para los empleados de la Dirección de Tecnologías de Información e Innovación.
- Diseño de una herramienta de software que facilite el proceso de implementación y auditoria de los controles de la norma ISO/IEC 27002 en la Dirección de Tecnologías de Información e Innovación.
- Proceso de certificación de ISO/IEC 27001 en la Dirección de Tecnologías de Información e Innovación.

Referencias

A. Mattei, T. (2017). *Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack*. *104*, 972–974. https://doi.org/10.1016/j.wneu.2017.06.104

Abad, M. (2015). *Cómo gestionar la seguridad de la información (según ISO 27001: 2013) en una PYME del sector de las tecnologías de la información y la comunicación* (Universidad de Valladolid). Recuperado de https://uvadoc.uva.es/bitstream/10324/16838/1/TFG-I-360.pdf

Almeida, L., & Respício, A. (2018). Decision support for selecting information security controls. *Journal of Decision Systems*, *27*(sup1), 173–180. https://doi.org/10.1080/12460125.2018.1468177

Altamirano, J. R., & Bayona, S. (2017). *Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento*. (25), 112–134. https://doi.org/10.17013/risti.25.112–134

ANUIES. (2016). *Estado actual de las tecnologías de la información y las comunicaciones en las instituciones de educación superior en México* (1ra ed.). Recuperado de http://anuies-tic.anuies.mx/web/encuentro2016/wp-content/uploads/pdf/EstadoActualTIC_en_las_IES.pdf

Arias, F. G. (2012). *El proyecto de investigación. Introducción a la metodología científica. 6ta*. Fidias G. Arias Odón.

Blasco, J., & Pérez, J. (2007). *Metodologías de investigación en las ciencias de la actividad física y el deporte: ampliando horizontes*. España: Club Universitario.

Cáceres, G. (2014). La importancia de publicar los resultados de Investigación. *Revista Facultad de Ingeniería*, *23*, 7–8.

Cárdenas-Solano, L.-J., Martínez-Ardila, H., & Becerra-Ardila, L.-E. (2016). Gestión de seguridad de la información: revisión bibliográfica. *El profesional de la informacion*, *25*(6). https://doi.org/10.3145/epi.2016.nov.10

Chávez, G. (2017). México es el país más afectado por Wannacry en América Latina [Revista Digital]. Recuperado de Tec Review website: http://tecreview.itesm.mx/mexico-es-el-pais-mas-afectado-por-wannacry-en-america-latina/

Chen, H., & Li, W. (2014). *Understanding Organization Employee's Information Security Omission Behavior: an Integrated Model of Social norm and Deterrence.* 1–10.

Consejo Superior de Administración Electrónica. (2010, marzo 9). PAe - CTT - General - MAGERIT versión 3. Recuperado el 12 de marzo de 2019, de https://administracionelectronica.gob.es/ctt/magerit#.XIhMraB7mUk

Davenport, T., & Prusak, L. (1998). *Working Knowledge: How Organizations Manage What They Know* (Vol. 1). https://doi.org/10.1145/348772.348775

David, J. (2002). Policy enforcement in the workplace. *Computers & Security*, *21*(6), 506–513. https://doi.org/10.1016/S0167-4048(02)01006-4

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

Dirección de Tecnologías de Información e Innovación. (2018). *Directorio de la Coordinación de Desarrollo y Soporte de Sistemas*. Recuperado de http://www.archivos.ujat.mx/2016/computo/directorio_desarrollo2.pdf

Enciclopedia de ciencias y tecnologías en Argentina. (2017). Información - ECyT-ar [Enciclopedia]. Recuperado de ECyT-ar website: https://cyt-ar.com.ar/cyt-ar/index.php/Información.

Escalera, G., & Pascual, M. (2004). La normalización y certificación como ventaja competitiva para la empresa española. *Boletín Económico de ICE*, (2820).

Fazlida, M. R., & Said, J. (2015). Information Security: Risk, Governance and Implementation Setback. *7th INTERNATIONAL CONFERENCE ON FINANCIAL CRIMINOLOGY 2015, 7th ICFC 2015, 13-14 April 2015,Wadham College, Oxford University, United Kingdom*, *28*, 243–248. https://doi.org/10.1016/S2212-5671(15)01106-5

Hamui-Sutton, A. (2013). Un acercamiento a los métodos mixtos de investigación en educación médica. *Investigación en Educación Médica*, *2*(8), 211–216. https://doi.org/10.1016/S2007-5057(13)72714-5

Heras, I., & Casadesús, M. (2006). Los estándares internacionales de sistemas de gestión: pasado, presente y futuro. © *Boletín económico de ICE, 2006, núm. 2876, p. 45-61*.

Hueso, A., & Cascant, J. (2012). *Metodología y Técnicas Cuantitativas de Investigación* (Primera, Vol. 1). Recuperado de https://riunet.upv.es/bitstream/handle/10251/17004/Metodolog%C3%ADa%20y%20t%C3%A9cnicas%20cuantitativas%20de%20investigaci%C3%B3n_6060.pdf?sequence

International Electrotechnical Commission. (2019). About the IEC. Recuperado el 26 de enero de 2019, de Who we are website: https://www.iec.ch/about/profile/?ref=menu

International Organization for Standardization, & International Electrotechnical Commission. (2013a). *ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements*. ISO/IEC.

International Organization for Standardization, & International Electrotechnical Commission. (2013b). *ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls*. ISO/IEC.

International Organization for Standardization, & International Electrotechnical Commission. (2018). *ISO/IEC 27000: Information technology - Security techniques - Information security management systems - Overview and vocabulary*. ISO/IEC.

ISO27000.es. (2005). Sistema de Gestión de la Seguridad de la Información [Blog]. Recuperado de ISO27000.es website: http://www.iso27000.es/sgsi.html

ISOTools. (2017). Comité Mexicano para atender a las normas ISO [Blog corporativo]. Recuperado el 26 de enero de 2019, de ISOTools website: https://www.isotools.com.mx/comite-mexicano-atender-las-normas-iso/

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers & Security*, *24*(3), 246–260. https://doi.org/10.1016/j.cose.2004.08.011

Kaspersky Lab. (2017). WannaCry ransomware used in widespread attacks all over the world [Blog]. Recuperado el 25 de febrero de 2019, de https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/

Kendall, K., & Kendall, J. (2011). *Análisis y diseño de sistemas* (Octava). México: Pearson Education.

Laudon, K., & Laudon, J. (2012). *Sistemas de información gerencial*. México: Pearson Educación.

Marcinkowski, S. J., & Stanton, J. M. (2003). *Motivational aspects of information security policies*. *3*, 2527–2532. IEEE.

Márquez, J. (2006). *Implementación de políticas de seguridad en cómputo en la UJAT* (Universidad Juárez Autónoma de Tabasco). Recuperado de http://www.rabid.ujat.mx/FilesRabidPDF/TB3036.pdf

Mesquida, A. L., & Mas, A. (2015). Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 Security Extension. *Computers & Security*, *48*, 19–34. https://doi.org/10.1016/j.cose.2014.09.003

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

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

Muñoz, C. (2002). *Auditoría en sistemas computacionales* (1ra ed.). México: Pearson Educación.

Siponen, M., Mahmood, A., & Pahnila, S. (2014). *Employees' adherence to information security policies: An exploratory field study*. *51*, 217–224.

Sohrabi, N., Von, R., & Furnell, S. (2016). *Information security policy compliance model in organizations*. (56), 70–82. http://dx.doi.org/10.1016/j.cose.2015.10.006

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

Syalim, A., Hori, Y., & Sakurai, K. (2009). *Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide*. 726–731. IEEE.

Symeonidis, I., Biczók, G., Shirazi, F., Pérez-Solá, C., Schroers, J., & Preneel, B. (2018). *Collateral damage of Facebook third-party applications: a comprehensive study*. *77*, 179–208. https://doi.org/10.1016/j.cose.2018.03.015

SysAdmin Audit, Networking and Security Institute. (2017). *Sensitive Data at Risk: The SANS 2017 Data Protection Survey. InfoSec Reading Room*. Recuperado de SysAdmin Audit, Networking and Security Institute website: https://www.sans.org/reading-room/whitepapers/threats/paper/37950

SysAdmin Audit, Networking and Security Institute. (s/f). SANS Institute: Information Security Resources. Recuperado el 26 de enero de 2019, de Information Security Resources website: https://www.sans.org/information-security/

Torres, M., Paz, K., & Salazar, F. (2006). Métodos de recolección de datos para una investigación. *Rev. Electrónica Ingeniería Boletín*, *3*, 12–20.

Tovar, N., & Salguero, A. (2018). *Auditoria interna a los activos físicos del área de TI en la Universidad Cooperativa de Colombia sede Ibagué, aplicando el estándar ISO/IEC 27002:2013*. Universidad Cooperativa de Colombia, Colombia.

Universidad de Guadalajara. (2019). Recibe UdeG certificación ISO en materia de protección de información digitalizada. Recuperado el 6 de abril de 2019, de http://www.udg.mx/es/noticia/recibe-udeg-certificacion-iso-materia-proteccion-informacion-digitalizada

Universidad Juárez Autónoma de Tabasco. *Manual General de Organización*. , (2014).

Universidad Juárez Autónoma de Tabasco. (2018). Misión Institucional de la Universidad Juárez Autónoma de Tabasco [Página oficial de la UJAT]. Recuperado de Misión Institucional website: http://www.ujat.mx/45/348

Valencia-Duque, F. J., & 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 e Tecnologias de Informação*, 73–88.

Velásquez, L. (2003). *Estudio del alcance de la implantación de tecnologías de información, como apoyo al mejoramiento de los procesos, en las pequeñas y medianas empresas del sector manufacturero en Bogotá.*

Vergel, M. M., & Sepúlveda, A. D. (2015). *Diseño de un manual de políticas de seguridad informática aplicando la norma ISO 27002 para la alcaldía del municipio de la Playa de Belén, norte de Santander*. Universidad Francisco de Paula Santander Ocaña, Colombia.

Von-Solms, B. (2000). Information security-The third wave? *Computers & Security*, *19*(7), 615–615.

Glosario

C

CDSS: Coordinación de Desarrollo y Soporte de Sistemas.

CSI: Comité de Seguridad de Información.

D

DTII: Dirección de Tecnologías de Información e Innovación.

I

IEC: International Electrotechnical Commission.

ISO: International Organization for Standardization.

M

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

S

SANS: SysAdmin Audit, Networking and Security.

SGSI: Sistema de Gestión de Seguridad de la Información.

U

UJAT: Universidad Juárez Autónoma de Tabasco.

A P É N D I C E S

Apéndice A. Instrumento para la evaluación de controles de ISO/IEC 27002:2013

Figura A.1. Herramienta para la evaluación de controles en la CDSS.

ISO/IEC 27002:2013 Herramienta de Evaluacion de Controles		CRITERIOS DE EVALUACIÓN	
		No realizado	0%
		Realizado informalmente	20%
		Planificado	40%
		Bien definido	60%
		Cuantitativamente controlado	80%
		Mejora continua	100%
Norma	**Seccion**		
5	**Políticas de seguridad de la información**	**0%**	
5.1	**Directrices de gestión de la seguridad de la información**	**0%**	
5.1.1	Políticas para la seguridad de la información	**No realizado**	0%
5.1.2	Revisión de las políticas para la seguridad de la información	**No realizado**	0%
8	**Gestión de activos**	**0%**	
8.1	**Responsabilidad sobre los activos**	**0%**	
8.1.1	Inventario de activos	**No realizado**	0%
8.1.2	Propiedad de los activos	**No realizado**	0%
8.1.3	Uso aceptable de los activos	**No realizado**	0%
8.1.4	Devolución de activos	**No realizado**	0%
8.2	**Clasificación de la información**	**0%**	
8.2.1	Clasificación de la información	**No realizado**	0%
8.2.2	Etiquetado de la información	**No realizado**	0%
8.2.3	Manipulado de la información	**No realizado**	0%
8.3	**Manipulación de los soportes**	**0%**	
8.3.1	Gestión de soportes extraíbles	**No realizado**	0%
8.3.2	Eliminación de soportes	**No realizado**	0%
8.3.3	Soportes físicos en tránsito	**No realizado**	0%
9	**Control de acceso**	**0%**	
9.1	**Requisitos de negocio para el control de acceso**	**0%**	
9.1.1	Política de control de acceso	**No realizado**	0%
9.2	**Gestión de acceso de usuario**	**0%**	
9.2.1	Registro y baja de usuario	**No realizado**	0%
9.2.2	Provisión de acceso de usuario	**No realizado**	0%
9.2.3	Gestión de privilegios de acceso	**No realizado**	0%
9.2.4	Gestión de la información secreta de autenticación de los usuario	**No realizado**	0%
9.2.5	Revisión de los derechos de acceso de usuario	**No realizado**	0%
9.2.6	Retirada o reasignación de los derechos de acceso	**No realizado**	0%
9.3	**Responsabilidades del usuario**	**0%**	
9.3.1	Uso de la información secreta de autenticación	**No realizado**	0%
9.4	**Control de acceso a sistemas y aplicaciones**	**0%**	
9.4.2	Procedimientos seguros de inicio de sesión	**No realizado**	0%
9.4.4	Uso de utilidades con privilegios del sistema	**No realizado**	0%
9.4.5	Control de acceso al código fuente de los programas	**No realizado**	0%
11	**Seguridad física y del entorno**	**0%**	
11.1	**Áreas seguras**	**0%**	
11.1.1	Perímetro de seguridad física	**No realizado**	0%
11.1.2	Controles físicos de entrada	**No realizado**	0%
11.1.3	Seguridad de oficinas, despachos y recursos	**No realizado**	0%
11.1.4	Protección contra las amenazas externas y ambientales	**No realizado**	0%
11.1.5	El trabajo en áreas seguras	**No realizado**	0%
11.2	**Seguridad de los equipos**	**0%**	
11.2.1	Emplazamiento y protección de equipos	**No realizado**	0%
11.2.2	Instalaciones de suministro	**No realizado**	0%
11.2.3	Seguridad del cableado	**No realizado**	0%
11.2.4	Mantenimiento de los equipos	**No realizado**	0%
11.2.5	Retirada de materiales propiedad de la empresa	**No realizado**	0%
11.2.6	Seguridad de los equipos fuera de las instalaciones	**No realizado**	0%
11.2.7	Reutilización o eliminación segura de equipos	**No realizado**	0%
11.2.8	Equipo de usuario desatendido	**No realizado**	0%
11.2.9	Política de puesto de trabajo despejado y pantalla limpia	**No realizado**	0%

Fuente: Elaboración propia, basado en la propuesta de (Tovar & Salguero, 2018).

Figura A.2. Herramienta para la evaluación de controles en la CDSS (continuación).

ISO/IEC 27002:2013 Herramienta de Evaluacion de Controles		CRITERIOS DE EVALUACIÓN	
		No realizado	0%
		Realizado informalmente	20%
		Planificado	40%
		Bien definido	60%
		Cuantitativamente controlado	80%
		Mejora continua	100%
Norma	**Seccion**		
12	**Seguridad de las operaciones**	**0%**	
12.1	**Procedimientos y responsabilidades operacionales**	**0%**	
12.1.1	Documentación de procedimientos operacionales	**No realizado**	0%
12.1.3	Gestión de capacidades	**No realizado**	0%
12.1.4	Separación de los recursos de desarrollo, prueba y operación	**No realizado**	0%
12.2	**Protección contra el software malicioso (malware)**	**0%**	
12.2.1	Controles contra el código malicioso	**No realizado**	0%
12.3	**Copias de seguridad**	**0%**	
12.3.1	Copias de seguridad de la información	**No realizado**	0%
12.4	**Registros y supervisión**	**0%**	
12.4.1	Registro de eventos	**No realizado**	0%
12.4.3	Registros de administración y operación	**No realizado**	0%
12.5	**Control del software en explotación**	**0%**	
12.5.1	Instalación del software en explotación	**No realizado**	0%
12.6	**Gestión de la vulnerabilidad técnica**	**0%**	
12.6.2	Restricción en la instalación de software	**No realizado**	0%
12.7	**Consideraciones sobre la auditoria de sistemas de información**	**0%**	
12.7.1	Controles de auditoría de sistemas de información	**No realizado**	0%
13	**Seguridad de las comunicaciones**	**0%**	
13.2	**Intercambio de información**	**0%**	
13.2.1	Políticas y procedimientos de intercambio de información	**No realizado**	0%
13.2.2	Acuerdos de intercambio de información	**No realizado**	0%
13.2.3	Mensajería electrónica	**No realizado**	0%
13.2.4	Acuerdos de confidencialidad o no revelación	**No realizado**	0%
14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**	**0%**	
14.1	**Requisitos de seguridad en los sistemas de información**	**0%**	
14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	**No realizado**	0%
14.1.3	Protección de las transacciones de servicios de aplicaciones	**No realizado**	0%
14.2	**Seguridad en el desarrollo y en los procesos de soporte**	**0%**	
14.2.1	Política de desarrollo seguro	**No realizado**	0%
14.2.2	Procedimiento de control de cambios en sistemas	**No realizado**	0%
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el	**No realizado**	0%
14.2.4	Restricciones a los cambios en los paquetes de software	**No realizado**	0%
14.2.6	Entorno de desarrollo seguro	**No realizado**	0%
14.2.7	Externalización del desarrollo de software	**No realizado**	0%
14.2.8	Pruebas funcionales de seguridad de sistemas	**No realizado**	0%
14.3	**Datos de prueba**	**0%**	
14.3.1	Protección de los datos de prueba	**No realizado**	0%
15	**Relación con proveedores**	**0%**	
15.1	**Seguridad en las relaciones con proveedores**	**0%**	
15.1.1	Política de seguridad de la información en las relaciones con los	**No realizado**	0%
15.1.2	Requisitos de seguridad en contratos con terceros	**No realizado**	0%
16	**Gestión de incidentes de seguridad de la información**	**0%**	
16.1	**Gestión de incidentes de seguridad de la información y mejoras**	**0%**	
16.1.1	Responsabilidades y procedimientos	**No realizado**	0%
16.1.2	Notificación de los eventos de seguridad de la información	**No realizado**	0%
16.1.3	Notificación de puntos débiles de la seguridad	**No realizado**	0%
16.1.4	Evaluación y decisión sobre los eventos de seguridad de informaci	**No realizado**	0%
16.1.5	Respuesta a incidentes de seguridad de la información	**No realizado**	0%
16.1.6	Aprendizaje de los incidentes de seguridad de la información	**No realizado**	0%
16.1.7	Recopilación de evidencias	**No realizado**	0%

Fuente: Elaboración propia, basado en la propuesta de (Tovar & Salguero, 2018).