UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

MODELO DE GESTIÓN DE OPERACIONES Y SERVICIOS DE SEGURIDAD PARA TECNOLOGÍAS DE INFORMACIÓN INTEGRANDO COBIT 5, ITILV3:2011 E ISO 27001:2005

VEGA CARRILLO PAOLA ALEXANDRA

MACHALA
2016

UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

MODELO DE GESTIÓN DE OPERACIONES Y SERVICIOS DE SEGURIDAD PARA TECNOLOGÍAS DE INFORMACIÓN INTEGRANDO COBIT 5, ITILV3:2011 E ISO 27001:2005

VEGA CARRILLO PAOLA ALEXANDRA

MACHALA
2016

UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

TRABAJO DE TITULACIÓN
PROPUESTAS TECNOLÓGICAS

MODELO DE GESTIÓN DE OPERACIONES Y SERVICIOS DE SEGURIDAD PARA TECNOLOGÍAS DE INFORMACIÓN INTEGRANDO COBIT 5, ITILV3:2011 E ISO 27001:2005

VEGA CARRILLO PAOLA ALEXANDRA
INGENIERA DE SISTEMAS

LOJA MORA NANCY MAGALY

Machala, 18 de octubre de 2016

MACHALA
2016

Nota de aceptación:

Quienes suscriben LOJA MORA NANCY MAGALY, LOAIZA LOAYZA MONICA CECIBEL, LOJÁN CUEVA EDISON LUIS y VALAREZO PARDO MILTON RAFAEL, en nuestra condición de evaluadores del trabajo de titulación denominado MODELO DE GESTIÓN DE OPERACIONES Y SERVICIOS DE SEGURIDAD PARA TECNOLOGÍAS DE INFORMACIÓN INTEGRANDO COBIT 5, ITILV3:2011 E ISO 27001:2005, hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

LOJA MORA NANCY MAGALY
0703410027
TUTOR

LOAIZA LOAYZA MONICA CECIBEL
0704069293
ESPECIALISTA 1

LOJÁN CUEVA EDISON LUIS
0703249698
ESPECIALISTA 2

VALAREZO PARDO MILTON RAFAEL
0704518893
ESPECIALISTA 3

Machala, 18 de octubre de 2016

Urkund Analysis Result

Analysed Document: VEGA CARRILLO PAOLA ALEXANDRA_FINAL.docx (D21685075)
Submitted: 2016-09-09 18:52:00
Submitted By: paolavegac18@gmail.com
Significance: 1 %

Sources included in the report:

TESIS_RODRIGUEZ_VIZUETE_DARIO222222222.doc (D18261475)
Tesis_Diana_Tola.docx (D13932415)
VÉLEZ RODRÍGUEZ DANIEL ISAAC.docx (D21636724)
http://itilv3.osiatis.es/diseno_servicios_TI/gestion_continuidad_servicios_ti/supervision.php

Instances where selected sources appear:

17

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

El que suscribe, VEGA CARRILLO PAOLA ALEXANDRA, en calidad de autor del siguiente trabajo escrito titulado MODELO DE GESTIÓN DE OPERACIONES Y SERVICIOS DE SEGURIDAD PARA TECNOLOGÍAS DE INFORMACIÓN INTEGRANDO COBIT 5, ITILV3:2011 E ISO 27001:2005, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

El autor declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

El autor como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que él asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 18 de octubre de 2016

VEGA CARRILLO PAOLA ALEXANDRA
0704653294

DEDICATORIA

Dedico ente trabajo a Dios, a mis padres, hermanos y a mi novio por estar siempre presentes acompañándome para poderme realizar y me alentaron continuar cuando parecía que me iba a rendir.

Vega Carrillo Paola Alexandra

AGRADECIMIENTO

Agradezco a Dios por ser la guía en mi camino, la fuerza y voluntad para poder prosperar en la vida. A mis padres Tulio Vega Betancourt por ser mi modelo a seguir y por su apoyo incondicional, mi madre Jacinta Carrillo Landín por sus sabios consejos que han formado mi personalidad. Y a todas las personas que colaboraron en la realización de este proyecto y especialmente a mi tutora Ing. Nancy Loja Mora por su invaluable ayuda.

Vega Carrillo Paola Alexandra

RESUMEN

La gestión de las tecnologías de información es una actividad empresarial que concentra decisiones y procesos para el manejo de operaciones y resguardo de seguridad, llevada a cabo mediante buenas prácticas de gestión y gobierno o estándares de protección de las TI; puesto que, debido al constante riesgo que presentan las empresas al no considerar la implementación de buenas prácticas, al momento de tomar decisiones o establecer procesos de implementación de tecnologías, generan problemas en su seguridad y en sus actividades diarias.

Un modelo de gestión de operaciones y servicios de seguridad para las TI, basado en procesos de COBIT 5; servirá como opción para prevenir delitos informáticos, mejorando el desempeño de las operaciones de las empresas, con el propósito de optimizar la atención al cliente, teniendo en cuenta la economía, la comunicación de servicios y recursos de los que disponen las empresas; por ello el presente trabajo se enfoca en proponer un Modelo de Gestión de Operaciones y Servicios de Seguridad para las Tecnologías de Información, orientado al robustecimiento a los procesos que entran en el espectro de estudio pertenecientes a COBIT 5; definiendo a este modelo como la representación conceptual para la identificación y solución de problemas de las empresas, mediante procesos que permiten coordinar, ejecutar, supervisar y mantener procedimientos operativos, funciones de seguridad y derechos de acceso con el propósito de proteger las tecnologías que gestionan la información, además de garantizar y facilitar el control de operaciones diarias, las cuales se encuentran en función directa con la implementación de buenas prácticas que minimicen perturbaciones e incidentes de seguridad, reduciendo niveles de riesgo, costos, y optimizando recursos, para mantener la integridad y privacidad de la información que posee cada empresa.

Los requerimientos del modelo propuesto se establecieron previamente a su desarrollo, para mejorar la perspectiva del objetivo a alcanzar, por medio de la adaptación de la metodología ágil de ingeniería de requerimientos para empresas emergentes de desarrollo de software; luego se realizó una búsqueda de modelos, marcos de gestión de TI y de estándares que entren en el contexto de estudio; seleccionando así a ITIL V3:2011 e ISO 27001:2005 por su enfoque de gestión; posteriormente se realizó un mapeo para identificar aquellas actividades y objetivos de control, que refuercen los procesos de Gestión de Operaciones y Gestión de Servicios de Seguridad

pertenecientes a COBIT 5; para finalmente efectuar la correspondiente evaluación del trabajo realizado, considerando las opiniones de expertos; recolectadas por medio de una encuesta y aplicando la escala de Licker para establecer sus niveles de aceptación con respecto a los cambios a realizar a COBIT 5; tomando en cuenta el método de muestreo seleccionado es establece como población a las empresas, que cuenten con estructuras organizacionales, implementación de políticas, normas, estándares de seguridad, marcos de gobierno o gestión de las TI y constituidas legalmente ubicadas en ciudades pertenecientes a la Provincia del Oro, siendo estas, Machala, Santa Rosa y Pasaje, por su facilidad de acceso y conocimiento de actividades por parte del investigador; cuyos datos obtenidos fueron analizados e interpretados en tablas y graficas estadísticas, que arrojaron resultados positivos para del modelo propuesto.

Palabras Clave: Tecnologías de Información, Gestión, operaciones, servicios de seguridad, COBIT 5, ITIL V3:2011, ISO 27001:2005.

ABSTRACT

The management of information technology is a business that focuses decisions and processes for managing security and protection operations, conducted through good management and governance practices or standards of protection of IT; since, due to the constant risk presented by companies failing to consider the implementation of good practice, when making decisions or establish processes of implementation of technologies, create problems in safety and in their daily activities.

A model of operations management and security services for IT-based processes COBIT 5; will serve as an option to prevent computer crimes, improving the performance of business operations, in order to optimize the customer, taking into account the economy, communication services and resources available to companies; This paper therefore focuses on proposing a model Operations Management and Security Services for Information Technology, aimed at strengthening the processes involved in the spectrum of study belonging to COBIT 5; defining this model as the conceptual representation for identifying and solving business problems through processes that allow coordinate, implement, monitor and maintain operational procedures, security functions and access rights in order to protect the technologies that manage information, and ensure and facilitate control of daily operations, which are in direct function with the implementation of good practices that minimize disturbances and security incidents, reducing risk levels, costs, and optimizing resources to maintain the integrity and privacy of information held by each company.

The requirements of the proposed development model previously established, to improve the outlook of the objective to be achieved through adaptation of agile requirements engineering methodology for emerging software development companies; then a search for models, IT management frameworks and standards that fall within the context of study was conducted; thus selecting ITIL V3: 2011 and ISO 27001: 2005 for its management approach; then a mapping was performed to identify those activities and control objectives, to strengthen processes Operations Management and Security Management Service belonging to COBIT 5; to finally make the corresponding evaluation of the work done, considering the opinions of experts; collected through a survey and applying Licker scale to establish their levels of acceptance regarding the changes to be made to COBIT 5; taking into account the method selected sampling is set to population businesses that have organizational structures, implementation of policies, standards,

safety standards, governance frameworks or IT management and legally constituted located in cities belonging to the Province Gold, being these, Machala, Santa Rosa and Pasaje, ease of access and knowledge of activities by the investigator; whose data were analyzed and interpreted in tables and graphs statistics that tested positive for the proposed model.

Keywords: Information Technology, Management, operations, security services, COBIT 5, ITIL V3: 2011, ISO 27001: 2005.

ÍNDICE GENERAL **Pág.**

LISTA DE FIGURAS

LISTA DE CUADROS

LISTA DE TABLAS

LISTA DE GRÁFICOS

LISTA DE ANEXOS

INTRODUCCIÓN

La gestión de las tecnologías de información (TI) es una actividad que condensa decisiones y procesos suscitados en las empresas, para el manejo de sus operaciones y resguardo de su seguridad; llevada a cabo mediante buenas prácticas encontradas en marcos de gestión y gobierno de TI o estándares de seguridad.

El presente trabajo está enfocado al robustecimiento de un modelo de gestión de Tecnologías de Información, que se concentre en la gestión de operaciones y servicios de seguridad de las empresas, con el propósito de garantizar y facilitar el control de sus operaciones diarias, las cuales están en función directa con la aplicación de buenas prácticas que minimicen las perturbaciones del servicio e incidentes de seguridad.

La importancia de este trabajo radica en el constante riesgo que presentan las empresas al no considerar la implementación de buenas prácticas, al momento de tomar decisiones o establecer procesos de implementación de tecnologías generando problemas de seguridad y en sus actividades diarias [1],[2],[3]; por ello se toma en consideración el marco de Gestión de TI COBIT 5 que permite una organización globalizada, cubriendo todas las áreas funcionales que compromete la responsabilidad de las tecnologías de información de la empresa [4]; además contiene procesos encargados de la Gestión de las Operaciones y Servicios de seguridad, por esto, el modelo propuesto se fundamenta de ellos tratando de mejorar su enfoque reforzando sus actividades y prácticas, añadiendo actividades del marco de trabajo ITIL V3:2011 cuyos objetivos son exclusivamente enfocados en aspectos de gestión de TI [5] y el estándar de seguridad ISO 27001:2005 en donde se encuentran las mejores acciones de seguridad de la información (objetivos de control y los controles) [6], por esto se emplea un mapeo para identificar las actividades y objetivos de control que permitan reforzar los procesos de COBIT 5 analizados en el contexto de estudio, siendo necesaria la evaluación del modelo propuesto mediante la validación de expertos de empresas ubicadas en las ciudades de Machala, Santa Rosa y Pasaje, pertenecientes a la Provincia de El Oro.

1. DIAGNÓSTICO DE NECESIDADES Y REQUERIMIENTOS

1.1 Ámbito de Aplicación: descripción del contexto y hechos de interés

De acuerdo a un análisis realizado en 22 países alrededor del mundo a pequeñas, medianas y grandes empresas, arrojó resultados desfavorecedores para América Latina; revelando que el 68% de las empresas ha sido víctima de virus, gusanos, spyware y otros programas maliciosos en el año 2012 [1].

En el año 2015 “se firmaron acuerdos sobre la seguridad cibernética entre Rusia y China, China y Estados Unidos, y entre China y el Reino Unido” [2] con el propósito de que ambas partes tratarán de prevenir ataques uno contra el otro, por la dificultad que presenta capturar a los infractores de las seguridades de la información de las empresas.

Encuestas realizadas por ESET a más de 3000 profesionales de distintas organizaciones; revelaron que en el 2015 tuvieron problemas con malware, phishing o vulnerabilidades de software y sistemas. Los países más afectados por códigos maliciosos son Nicaragua, que ocupa el primer lugar con el 58.3%, seguido de Guatemala con el 55.8% y Ecuador con 51.9%. Asimismo, Argentina (29.7%), Chile (29.2%) y Venezuela (24.1%) [3].

Para mitigar este tipo de inconvenientes, varios marcos de gestión han sido creados para apoyar el despliegue de la gestión de TI, como COBIT que se centra en los procesos de la organización para evaluar y monitorear su rendimiento o ITIL; útil en la gestión y prestación de servicios [7].

ITIL es un conjunto de mejores prácticas auditables para la gestión de servicios de TI con el fin de mejorar la calidad del servicio y reducir el costo a largo plazo de las TI en la prestación de servicios. Estas mejores prácticas son aplicables a todas las organizaciones de TI, sin importar su tamaño o la tecnología que aplican [8],[9], mientras que COBIT ofrece objetivos de control para la gestión de servicio a terceros y adquisición de TI, considerando a la información como su principal recurso; este estándar es genérico y útil para todo tipo de empresas [10],[11].

Un ejemplo del uso de estos marcos de gestión, es una de las empresas de acero ubicada en Beijing, que usa el marco ITIL para la gestión de servicios de TI (ITSM) implementado en 5 fases: Estrategia del Servicio, Diseño del servicio, transición del servicio, Operación del servicio y Mejora continua, cuyos objetivos de negocio son el resultado de un balance entre COBIT e ITIL usando como referencia los campos de

control de Planificación y Organización, Adquisición e implementación, Entrega y Apoyos [9].

Implementar marcos de gestión de TI en las empresas influye en su desarrollo tecnológico haciéndolas competitivas además de mejorar su reputación y estatus en el mercado, resultando más atractiva a posibles clientes. Una buena gestión de TI permite que las operaciones dentro y fuera de la empresa se realicen más rápido, con mejores resultados, menor costo y menor número de trabajadores, permitiendo que se realicen inversiones que mejoren gradualmente los sistemas actuales [12].

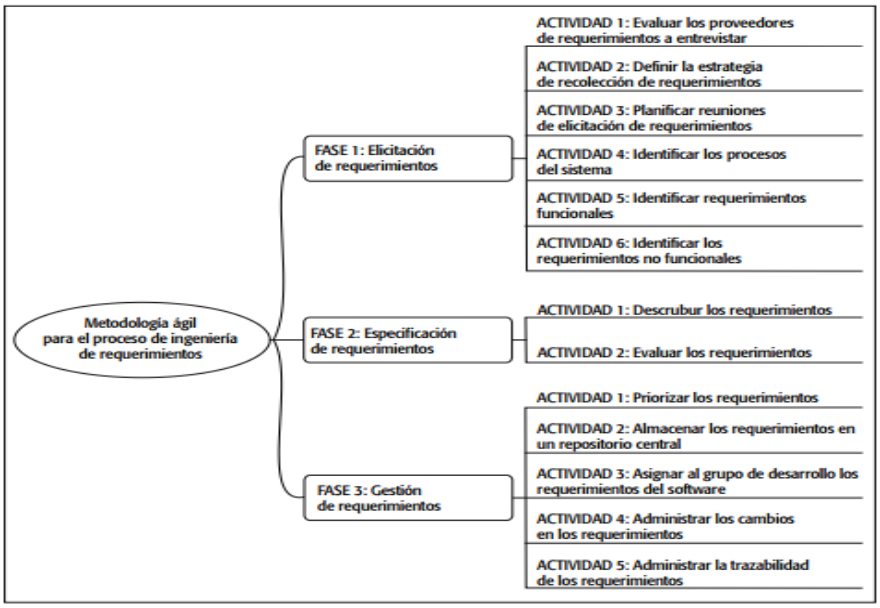
Para todas las empresas independientemente de su tamaño, es fundamental saber que recursos necesitan ser protegidos para mejorar el control de sus operaciones diarias, el acceso al sistema y los derechos de los usuarios del sistema de información.

1.2 Establecimiento de requerimientos

Establecer requerimientos previo al desarrollo de cualquier tipo de proyecto, proporciona una mejor perspectiva de lo que se pretende obtener, puesto que los requerimientos muestran los elementos y funciones necesarias para un proyecto. Sin embargo para garantizar veracidad en la obtención de los requerimientos es necesario el uso de metodologías que permitan la segmentación de tareas con el propósito de analizar la situación del problema a resolver, de forma que no se escape ningún detalle al momento de determinar los requerimientos de solución.

Para la obtención de los requisitos se pretende usar una metodología ágil de ingeniería de requerimientos para empresas emergentes de desarrollo de software, basada en el modelo de madurez de capacidades integrado e ISO/IEC 12207, cuyo análisis comparativo presentó como resultados los proceso de Elicitación, Especificación y Gestión [13].

Figura 1. Estructura de la metodología ágil para el proceso de Ingeniería de Requerimientos



Fuente: L. Merchán, A. Urrea, and R. Rebollar, [13]

Tomando con referencia la primera fase de esta metodología se estableció lo siguiente:

1.2.1 Elicitación de requerimientos

La evolución de las tecnologías de información en la actualidad, cada día es más frecuente, permitiendo a empresas agilizar sus procesos de forma eficiente, sin embargo la mala gestión de las tecnologías en el ambiente operacional de las empresas pueden generar brechas en su seguridad, perjudicando la integridad, confidencialidad y disponibilidad de la información.

En la actualidad existen modelos de gestión certificados y aplicables a cualquier tipo de empresas, por tanto, su aplicación es considerada como una ventaja competitiva, sin embargo no existen modelos robustos enfocados a la gestión de operaciones y servicios de seguridad. Por lo mencionado con anterioridad surge la siguiente interrogante ¿Será posible robustecer un marco de gestión de TI y enfocarlo a la gestión de operaciones y servicios de seguridad?

1.2.2 Especificación de requerimientos

No existe un marco de gestión de TI enfocado a la gestión de operaciones y servicios de seguridad, pero existen normas que pueden ayudar a robustecer la gestión de operaciones y servicios de seguridad. Por tanto, se plantea la posibilidad de robustecer un modelo de gestión de TI, en el cual se tomen actividades de otras normas con el

propósito de mejorar el modelo ya existente y enfocarlo a la gestión de operaciones y servicios de seguridad.

Especificación de requerimientos específicos

Cuadro 1. Requisitos Específicos

Id	**Descripción**
RE-1	Identificar aportes para la gestión de Operaciones y Servicios de Seguridad
RE-2	Integrar actividades para robustecer un modelo de TI para la gestión de Operaciones y Servicios de seguridad
Fuente: Elaboración Propia	

Especificación de requerimientos funcionales

Cuadro 2. Gestión Financiera

Id	**Descripción**
RF-1	Presupuesto
RF-2	Contabilidad
RF-3	Aprobación financiera
Fuente: ITIL V3:2011 [5]	

Cuadro 3. *Relación con los proveedores*

Id	**Descripción**
RF-4	Los procesos de evaluación y selección de proveedores
RF-5	La clasificación y documentación de la relación con los proveedores
RF-6	Renovación o terminación
Fuente: ITIL V3:2011 [5]	

Cuadro 4. Gestión del Conocimiento

Id	**Descripción**
RF-7	Puntualizar una estrategia de Gestión del Conocimiento y divulgarla a toda la empresa [5].
RF-8	Mejora la transmisión de conocimiento entre personas, equipos y departamentos [5].
RF-9	Uso del Sistema de Gestión del Conocimiento del Servicio (SKMS) [5]
Fuente: ITIL V3:2011 [5]	

Cuadro 5. Seguridad y Políticas

Id	Descripción
RF-10	Constituya política de seguridad que oriente a la empresa [5].
RF-11	Realizar un Plan de Seguridad que integre los límites de seguridad adecuados descritos en los acuerdos de servicio firmados con proveedores internos y externo [5].
RF-12	Computación móvil y comunicaciones [14]
RF-13	Tele-trabajo [14]
Fuente: ITIL V3:2011 [5] e ISO 27001:2005 [14]	

1.3 Justificación del requerimiento a satisfacer

El presente trabajo es de suma importancia para mejorar la gestión de las operaciones y servicios de seguridad en las empresas, puesto que se mantienen en un constante riesgo, al no considerar aspectos de seguridad, al momento de tomar decisiones de implementación de tecnologías de información, con el propósito de agilizar sus operaciones diarias y mejorar su estatus en el mercado.

Un modelo de gestión de Operaciones y servicios de seguridad para las tecnologías de información, cuya base parte de los procesos de COBIT 5, servirá como una opción de prevención para evitar los delitos informáticos y mejorar el desempeño de las operaciones de las empresas con el propósito de mejorar la atención de sus clientes; considerando el nivel económico de las mismas y abarcando la comunicación para los servicios, recursos o personal externalizado.

2 DESARROLLO DEL PROTOTIPO

2.1 Definición del prototipo tecnológico

Modelo conceptual es una representación de los conceptos y la relación entre ellos en la solución de los problemas identificados de un proceso de negocio específico [15]; además permite capturar la comprensión actual acerca de la estructura y el funcionamiento de un sistema [16].

Gestión de Operaciones es un proceso que consiste en la coordinación y ejecución de actividades y procedimientos operativos requeridos para dar servicios de TI internos y subcontratados, integrando procedimientos operativos estándar predefinidos y las actividades de supervisión requeridas [17].

Gestión de Servicios de seguridad Los Servicios de seguridad protegen la información de la empresa para mantener el nivel de riesgo acorde con los parámetros de seguridad de las empresas de acuerdo con sus políticas de seguridad. Establecer y mantener las funciones de seguridad de información y los privilegios de acceso y llevar a cabo la supervisión de seguridad [34].

Tecnologías de Información Son innovaciones que consienten el procesamiento y acumulación de enormes cantidades de información [18] siendo necesarias para la gestión y transformación de la información, [19] permitiendo editar, producir, almacenar, intercambiar, transmitir [20], proteger y recuperar esa datos [19] entre diferentes sistemas de información, facilitando el acceso al conocimiento [20].

La definición del modelo propuesto de acuerdo a la información prescrita anteriormente se establece de la siguiente manera:

El **Modelo de Gestión de Operaciones y Servicios de Seguridad para las Tecnologías de Información** se define como la representación conceptual para la identificación y solución de problemas de las empresas, mediante procesos que permiten coordinar, ejecutar, supervisar y mantener procedimientos operativos, funciones de seguridad y derechos de acceso con el propósito de proteger las tecnologías que gestionan la información.

2.2 Fundamentación teórica del Prototipo

2.2.1 Modelo. Un modelo de un sistema se considera generalmente como una representación del sistema. Los modelos también son abstracciones que suprimen detalles que no son de interés. Los modelos están en el corazón de la ciencia y la ingeniería [21].

La real academia de la lengua española define a un modelo como [22]:

- Arquetipo o punto de referencia para imitarlo o reproducirlo.
- Esquema teórico, generalmente en forma matemática, de un sistema o de una realidad compleja, como la evolución económica de un país, que se elabora para facilitar su comprensión y el estudio de su comportamiento.

Otro autor definen a un modelo como:

Los modelos empleados para el desarrollo de software y sistemas las tecnologías de uso de la ingeniería incluyen lenguajes de modelado gráfico, tales como el Lenguaje de Modelado de Sistemas, que el apoyo el diseño del sistema y el análisis a través de modelos de lectura mecánica [21].

Un modelo es una representación abstracta que explica parcialmente la realidad, enfocándose en un fenómeno o proceso especifico facilitando su comprensión y estudio. La aplicación de un modelo a procesos y sistemas, permite probar hipótesis o teorías que pretendan mejorar su situación actual, evitando posibles imprevistos por errores de diseño.

Función de modelo. Las funciones de los modelos son: representar, explicar, guiar, motivar, predecir, evaluar y genera realidades. La función principal de los modelos es la de comprender y explicar la realidad a fin de poder hacer predicciones [23].

Por deducción propia puedo definir que la función de un modelo es generar realidades mediante representaciones que las expliquen y facilite la predicción de un sistema o proceso.

2.2.2 Clasificación de Modelos

Modelo matemático. Los modelos matemáticos intentan interpretar una realidad por medio de ecuaciones para la predicción de un sistema o un proceso. Los datos obtenidos permitirán establecer estadísticas en base a experiencias anteriores, con el propósito obtener resultados cercanos a ambientes reales, ya que este tipo de modelos sufren de un margen de error cuando son comparados con la realidad.

Estos son los razonamientos de varios autores con respecto a los modelos matemáticos:

- Un modelo matemático es un conjunto de ecuaciones que representan las leyes físicas detrás del considerado sistema; en el que necesita definir un conjunto de parámetros considerados durante una construcción del modelo matemático abstracto [24].
- En la ciencia los modelos matemáticos se puede utilizar para predecir las propiedades y los comportamientos de los sistemas. Un modelo debe ser simple, matemáticamente correcto, y experimentalmente verificable. Sin embargo, como con el sistema de la geometría, lo que debería esperarse que no puede haber múltiples interpretaciones de una dada la especificación, algunos de los cuales pueden no ser válidas [21].
- Un modelo matemático de un sistema dinámico se define como conjunto de ecuaciones que representan la dinámica del sistema con precisión o, al menos, bastante bien. Téngase presente que un modelo matemático no es único para un sistema determinado, un sistema puede representarse de muchas formas diferentes, por lo que puede tener muchos números matemáticos, dependiendo de cada perspectiva [25].
- Un sistema donde todos los comportamientos u opciones se pueden simular por medio de ecuaciones matemáticas cuyas variables están previamente establecidas de acuerdo a lo que se quiere contemplar. Permiten obtener resultados en base a experiencias anteriores o a estadística. Se utiliza en pronósticos (de demanda, ventas, en control de inventarios, de calidad, muestre). Hay que rescatar que todo modelo matemático sufre de error cuando se compara con la realidad, pues siempre será un cálculo y factores externos que no permitan la exactitud [26].
- El modelo matemático permite establecer relaciones considerando elementos gráficos, numéricos y simbólicos, empleando datos reales, que estudian parámetros de crecimiento, ya sea poblacional o de una cualidad de un organismo especifico; que facilitan la interpretación correcta del análisis de situaciones. El modelo matemático asocia argumentos que ayudan al aprendizaje de conocimientos, con una práctica real que represente un proceso o idea [27].
- En base de datos se trabaja con estructuras relacionales que consisten en una colección de relaciones matemáticas para la interpretación de oraciones que tienen un significado lógico matemático. Estas representaciones expresan una relación de orden con sistemas numéricos; en donde cada par (m,n) es una relación [21].

*2.2.2.1 Modelo físico***.** Los modelos físicos sirven en general como intermediarios entre el diseño y la construcción. Esta técnica es cientos de años de antigüedad; muchos grandes arquitectos, como Miguel Angel ya han utilizado modelos físicos para explicar la construcción técnicas, estructuras de edificios y sala de ambiente interior para clientes y trabajadores [28]. Un modelo físico, puede ser dividido en dos ramas: (I) las pruebas de muestra. Este tipo de modelos físicos se utiliza para obtener parámetros de entrada, al igual que las propiedades del material, para modelos matemáticos. (II) La vigilancia o experimento. Este tipo de modelos físicos no sirve para la identificación de los parámetros del modelo, pero para verificación y validaciones de modelos matemáticos [24].

El modelo físico parte de la capacidad de hacer cosas utilizando condiciones complejas y en ocasiones inciertas, para ello se debe considerar diferentes perspectivas, que nos generen alternativas de su uso y desarrollo. Entonces el modelo físico trata sobre la capacidad de transformar algo con base en la creatividad para alcanzar nuestro objetivo; de esta manera se presentan continuamente y de forma dinámica situaciones que se deben enfrentar. Para su elaboración es importante contar con la información de su estructura (diseño), comportamiento (parámetros de medición) y función (respuestas a los objetivos de origen) [29].

2.2.2.2 Modelos gráficos. Los modelos gráficos en general representan las entidades de un sistema como nodos en un gráfico y relaciones como arcos. La sintaxis y la semántica proporcionadas por los modelos gráficos ayuda a capturar el significado de frases en lenguaje natural. Sin embargo, para capturar el significado completo de las frases requiere interpretación de los modelos gráficos a un lenguaje legible por máquina tal como XML / XMI. Tres lenguajes gráficos son revisados: 1) entityrelationship diagramas (E-R); 2) el lenguaje de modelado unificado (UML); y 3) el lenguaje de modelado de sistemas (SysML) [21].

2.2.2.3 Modelo conceptual. Un modelo conceptual consiste en expresar relaciones entre conceptos para capturar el funcionamiento de un sistema; además permite integrar nuevas ideas para mejorar su comprensión y estado actual.

Estas son las opiniones de autores sobre el modelo conceptual:

- Modelado conceptual se utiliza en muchos campos, con un grado variable de formalidad. En las aplicaciones ambientales, modelos conceptuales se utilizan para expresar relaciones, explorar y probar ideas, comprobar la inferencia y la causalidad, determinar los conocimientos y lagunas en los datos, sincronizar modelos mentales y construir consenso, y para poner de relieve los procesos clave o dominantes [16].

- En informática, un modelo conceptual es una representación de los conceptos y la relación entre ellos en la solución de los problemas identificados de un proceso de negocio específico [15] para el desarrollo de software un modelo conceptual consiste en la información lógica, información física y mapas de relaciones entre ellos. La información lógica se utiliza para expresar los conceptos relacionados y funciones lógicas del software, que es descripción abstracta del software. La información física incluye clases, métodos de las clases y los campos de clases de software [30].
- Modelos conceptuales (mentales) capturan nuestra comprensión actual acerca de la estructura y el funcionamiento de un sistema. El proceso de construcción de modelos (reglas), así como el formalismo usado (sintaxis) puede ser diferente de un caso a otro. No hay una norma definida para el modelado conceptual, considerando que la práctica de modelado conceptual puede variar desde completamente informal (por ejemplo, imágenes "-agitando la mano" o ricos en un rotafolio) a muy ordenado y estructurado (por ejemplo, la dinámica de sistemas formalismo) [16].
- El modelo conceptual explica su existencia, sus principios científicos, filosóficos éticos y sus valores; con base en ello permite elaborar teorías para facilitar su aplicación. Estos modelos ayudan a establecer indicadores de calidad, que se rigen a una visión de la realidad, lugar y relación con la sociedad, con una base de conocimiento única. No es necesaria su existencia física, son esquemas mentales que orientan la práctica y pensamiento lógico para la toma de decisiones [31].

Al no existir normas que establezcan como se deben elaborar los modelos conceptuales se pueden considerar la propuesta de Pignataro como los elementos fundamentales (o principios) de una mejor práctica para el enfoque de modelado conceptual: (1) Utilizar un modelo de proceso de desarrollo abierto y transparente, (2) encapsular y comunicar conceptos efectivamente, (3) Establecer y mantener modelos elegantes, (4) Crear modelos robustos y adaptables, (5) Utilizar un enfoque formal para modelar la representación, (6)Prueba y volver a probar los modelos, (7) Explorar el comportamiento del modelo a través de escenarios y (8)Asegurarse de que el modelo se puede convertir en una forma operativa [16].

2.2.2.4 Modelado basado en agentes. Un modelo basado en agentes permite el estudio de los componentes de un sistema, a partir de su comportamiento e interacción, generando un comportamiento macroscópico por la intervención de nuevas variables; haciéndolo idóneo para modelar sistemas complejos, requiriendo simulación computacional. Considerado como un modelo complementario a métodos analíticos como es el caso del modelo matemático que es más preciso, menos intuitivo y más complejo.

Algunos autores expresan su explicación de los modelos basados en agente:

- Los modelos basados en agentes son modelos computacionales cuyo análisis debe hacerse a través de simulación y comparada con un modelo matemático se considera que la representación matemática es más precisa pero menos intuitiva y más compleja al estar basada en polinomios [32].
- En ciencias sociales, ha sido ampliamente usada para explorar los fenómenos sociales con simulación computacional. La simulación basada en agentes ha demostrado ser una técnica potente para modelar los sistemas complejos y especialmente los sistemas sociales [33].
- Con el modelado basado en agentes se modelan los elementos microscópicos que constituyen el sistema así como la dinámica de estos a partir del conocimiento que se dispone sobre su comportamiento y, como resultado de las interacciones de los agentes, emerge un comportamiento macroscópico del sistema que se valida sobre la realidad observable. Este modelado estudia, cómo a partir de la formulación matemática de la dinámica de los agentes (sistemas dinámicos cuyos estados evolucionan en el tiempo) se puede determinar el comportamiento macroscópico de las variables agregadas, sin embargo su resolución algebraica no es factible en la práctica y no se adaptan a las necesidades propias del campo de la Ingeniería de Sistemas y Automática [32].
- Es una técnica de modelación que complementa los métodos analíticos tradicionales [34].

2.2.3 Gestión de Operaciones.- En la gestión de la operación es clave la innovación en la base de las tecnologías para mejorar la competitividad de las empresas [35]. La Gestión de operaciones es una función encargada de coordinar, ejecutar y supervisar las actividades, bienes y servicios de las empresas con el fin de reducir costos y optimizar recursos.

Aseveraciones sobre el concepto de Gestión de Operaciones:

- Gestión de Operaciones es un proceso que consiste en la coordinación y ejecución de actividades y procedimientos operativos requeridos para dar servicios de TI internos y subcontratados, integrando procedimientos operativos estándar predefinidos y las actividades de supervisión requeridas [17].
- Gestión de la operación basada en el cálculo de costes, tiene como principales objetivos optimizar la asignación de recursos, para reducir el costo, crear más valor para los clientes y realizar el valor de una empresa e incluye tres pasos: (1) Encontrar oportunidades para mejorar el funcionamiento mediante el análisis. (2) Averiguar las

clases de coste y asegúrese de que las causas de desecho. (3) Establecer un sistema de medición del desempeño para evaluar el desempeño de la gestión de la operación [36].

- Es la función de gestión responsable de la producción de los bienes físicos y los servicios que ofrece una empresa en el mercado. Su objetivo es lograr simultáneamente los objetivos de calidad, flexibilidad, costes y plazos. Entre otras actividades, de gestión de operaciones incluye la contratación (logística de entrada), operaciones que transforma entradas en salidas, control de calidad y distribución (logística de salida) [35].

2.2.3.1 Características e implicaciones de la Gestión de Operaciones. La gestión de las operaciones es considerada un proceso del cual se obtienen resultados a largo plazo, de aquellas actividades recurrentes de las empresas, tomando en cuenta su presupuesto y la asignación de responsabilidades para la toma de decisiones que afectaran en gran medida el desarrollo y nivel competitivo de las empresas.

La gestión de las operaciones generalmente se caracteriza por [37]:

- Ser un proceso a largo plazo (potencialmente ilimitado) y de trabajo continuo;
- Requiere un presupuesto a largo plazo con los costos sólo parcialmente definidos o estimados previamente; un presupuesto cíclico y la gestión de costes;
- Asignación de personal permanente al proyecto durante mucho tiempo.

Esto implica que [37]:

- El gerente de operaciones y el supervisor es dueño de un negocio real; siendo imposible tratar asuntos técnicos por separado de las cuestiones de costos; puesto que la decisión técnica de hoy afectará en gran medida el costo de mañana y la persona que está a cargo de la gestión técnica también será considerado responsable de los costos;
- Los costos son recurrentes durante la vida útil operaciones de largo; y el gerente de operaciones debe estar preocupado por el costo de cada ciclo con el objetivo de implementar un proceso de mejora continua;
- Se debe aplicar una cultura de la optimización de costes;
- Los costos deben ser asignados en el momento justo para apoyar la comparación ciclos; debido a la gran cantidad de datos y los requisitos de tiempo real, se necesita apoyo herramienta informática para realizar esta tarea;
- Los gerentes de operaciones deben mirar más allá de los costos financieros con el fin de investigar y vigilar las causas fundamentales de esos gastos.

2.2.4 Gestión de Servicios de Seguridad. Los servicios de seguridad consisten en resguardar la información de la empresa en base a políticas de seguridad para garantizar el cumplimiento de los principios de seguridad de la información con el fin de mantener y supervisar los niveles de riesgo.

Algunos autores expresan sus argumentos sobre la gestión servicios de seguridad:

- Los Servicios de seguridad Protegen la información de la empresa para mantener el nivel de riesgo acorde con los parámetros de seguridad de las empresas de acuerdo con sus políticas de seguridad. Establecer y mantener las funciones de seguridad de información y los privilegios de acceso y llevar a cabo la supervisión de seguridad [17].
- Los servicios de seguridad Informática brindan una opción al alcance de las necesidades de cada empresa, para asegurar la integridad y la privacidad de los datos pertenecientes a la misma [38].
- Las políticas de seguridad se han utilizado tradicionalmente para especificar requisitos de seguridad de las redes y sistemas distribuidos que se ponen en marcha para proteger sus servicios [39].

2.2.4.1 Gestión de Seguridad. La seguridad radica en la disminución de riesgos a través de una buena gestión [40]; siendo la información y las tecnologías componentes básicos en el manejo y desarrollo de toda la empresa estos vienen a considerarse temas difíciles de administrar eficientemente que requieren estándares que faciliten su gestión apropiada, documentada y conocida por todos los niveles organizacionales de la empresa.

Importancia de la Seguridad de la Información.- La información que maneja una empresa es de suma importancia, lo que hace que deba protegérsela a toda costa de todos los riesgos que existen debido al desarrollo de las tecnologías y el desconocimiento total o parcial de las formas de mitigar los riesgos, lo que hace fundamental diseñar e implantar estrategias que mejoren la seguridad de la información de las empresas [6].

Gestión de la seguridad de la información.- Se remonta a los inicios de la civilización principalmente empleada en tiempos de guerra por grandes estrategas.

Sin duda alguna los avances tecnológicos han aumentado las amenazas a la seguridad; por ello implementar una seguridad proactiva [41] que evalúe riesgos permite a las empresas enfrentar los cambios en la infraestructura o la aparición de nuevas líneas de negocio. En la actualidad la gestión de la seguridad de la información en las empresas

depende mucho del conocimiento de las actividades del negocio, con el fin de establecer protocolos para la disponibilidad, integridad y confidencialidad de la información.

Principios de la Seguridad de la información. Los principios de la seguridad pueden considerarse como los servicios que otorga la gestión de la seguridad para resguardar la información y tecnologías de las organizaciones. Los principios de la seguridad son:

- Confidencialidad: la información será accesible para aquellas personas o entidades que cuenten con los permios o autorización correspondiente.
- Integridad: la información debe mantenerse completa y exacta
- Disponibilidad: la información debe ser accesible a los procesos requeridos cuando se la necesite.

La Gestión de la Seguridad debe, por tanto, velar por que la información sea correcta y completa, esté siempre a disposición del negocio y sea utilizada sólo por aquellos que tienen autorización para hacerlo [42].

2.2.4.2 Principales servicios de seguridad. En una política de seguridad de servicios electrónicos establecida en la norma ISO 7498-2, el identifica las 5 categorías principales de servicios de seguridad y [39] otras 5 categorías para la gestión de servicios de seguridad:

- Autenticación
- Control de acceso
- Confidencialidad de los datos
- Integridad de los datos
- No repudio
- De registro con seguridad - de transacciones de usuario por el proveedor
- Certificación - usuario o proveedor de usarían alguna autoridad de certificación para certificar credenciales
- Detección de Malware - usuario o proveedor podría utilizar algún software anti-malware para detectar y eliminar el malware de sus plataformas de computación
- Aplicación Seguimiento - monitoreo plataforma de usuario para aplicaciones con licencia, verificados y autorizados

2.2.5 Tecnologías de Información.- Las Tecnologías de Información son innovaciones que consienten el procesamiento y acumulación de enormes cantidades de información [18] siendo necesarias para la gestión y transformación de la información, [19] permitiendo editar, producir, almacenar, intercambiar, transmitir [20], proteger y

recuperar esa datos [19] entre diferentes sistemas de información, facilitando el acceso al conocimiento [20].

Las TI son de uso general cuyo uso está orientado a las decisiones políticas, por el ecosistema urbano de los ciudadanos, proveedores de tecnologías y autoridades locales en función de hábitos que se presenten en las ciudades [43].

2.2.6 Estrategias para la gestión de tecnologías de información aplicadas en las empresas

2.2.6.1 Departamento de Operaciones.- En la ciudad de Redlands, California se desarrolla un modelo similar al Departamento de Operaciones que ha sido evaluado por aproximadamente 20 directores municipales de TI, quienes han considerado que es un modelo favorable; en el que se destaca por el cambio de un presupuesto reactivo (forma tradicional basado en proyectos), a un presupuesto basado en prioridades organizacionales; sin embargo existen limitaciones a cambios en las pequeñas empresas que dificultan su implantación inmediata [44].

2.2.6.2 Segregación de actividades por equipos.- El HOSPITAL INTERNACIONAL EN TAILANDIA ha dividido la gestión y apoyo a las TI en tres equipos, el equipo de soporte de TI, el equipo de infraestructura de red y el equipo de sistema Hospitalaria (HIS), quienes son los que reciben las instrucciones del Director de tecnologías, quien a su vez las recibe del CEO del Hospital. Estos equipos atienden los incidentes que se presentan en cada uno de los departamentos en el orden de prioridad al que estos sean clasificados [12].

Cuadro 6. Equipos encargados del Apoyo de TI en el Hospital Internacional en Tailandia

Equipos	Descripción
Soporte TI:	*Prestación de servicios de TI generales y solución a problemas básicos del ordenador* [12].
Infraestructura de Red:	*Soporte de servidores, bases de datos, redes informáticas, y las empresas de externalización que se ocupan de la infraestructura TI (hardware y software)* [12].
HIS:	*Cuenta expertos médicos de servicios y profesionales que discuten con Microsoft sobre el desarrollo de sistemas computarizados* [12].

Fuente: Elaboración Propia, basado en [12].

Emplear equipos de gestión y apoyo para las TI, que este dirigidos por un Director de tecnologías o un CEO puede ser factible en el caso de disponer con los recursos y capacidades del personal, sin embargo las empresas deben alentar la educación en

materia de gestión de TI y seguridad de la Información para lograr futuros expertos internos. Establecer un equipo reducido de personal en donde se asigne a una persona que represente la gestión de cada área, es decir en el soporte de TI e Infraestructura de red, además de un Director de TI que mantenga un contacto directo con la junta directiva, jefes departamentales y agentes externos como los proveedores de tareas externalizadas sería una opción viable ante la falta de recursos.

2.2.6.3 Centros de Gestión de Servicios.- La gestión de las operaciones TI dentro de una empresa depende de la amplitud de los servicios ofrecidos siendo estos los casos que se pueden presentar[45]:

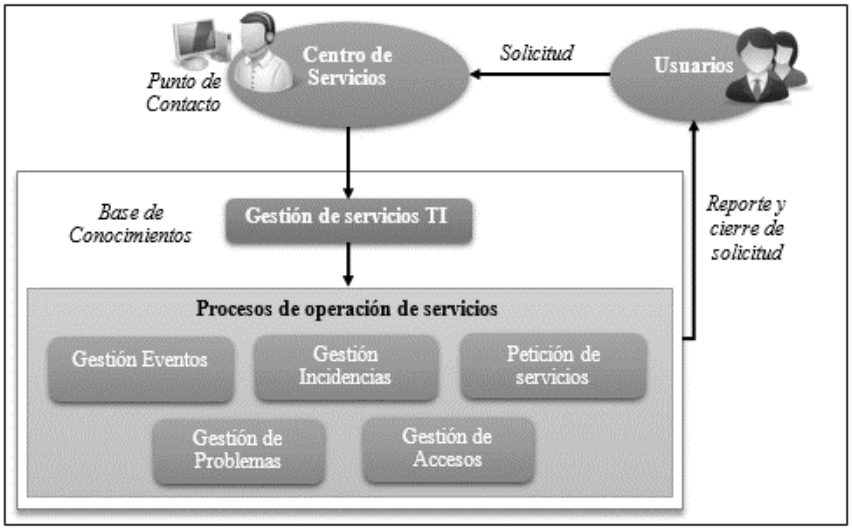
Cuadro 7. Características de Centros de Gestión de Servicios TI según su amplitud

Centros de Gestión de Servicios TI según su amplitud	
Centro de llamadas Call Center	• Gestionar un alto volumen de llamadas • Redirigir usuarios a los expertos (excepto asuntos de soporte y/o comerciales).
Centro de Soporte Help Desk	• Ofrecer soporte técnico • Resolver en el menor tiempo interrupciones en el servicio
Centro de Servicios Service Desk	• Comunicar a clientes y usuarios de todos los servicios TI, enfocado en los procesos de negocio. • Servicios adicionales: o Supervisión de los contratos de mantenimiento y niveles de servicio. o Canalización de las Peticiones de Servicio de los clientes. o Gestión de las licencias de software. o Centralización de todos los procesos asociados a la Gestión TI.

Fuente: Elaboración Propia

Los tipos de centros de gestión que abarcan más actividades o procesos de negocio son el Centro de Soporte y Centro de Servicios, por esto son las más usadas en las empresas; sin embargo cada uno de ellos tiene su propósito con soluciones a problemas específicos y el otro a soluciones estratégicas.

Figura 2. Procesos de un Centro de Servicios



Fuente: Elaboración Propia

Un centro de servicios interactúa con los usuarios o miembros del departamento TI son los que solicitan servicios, informes de funcionamiento o de niveles de servicio al centro de operaciones, en donde se gestionan los servicios TI por medio de los procesos de operación, además de acumular conocimientos para encontrar mejores soluciones en el futuro con base a la experiencia adquirida para la mejora continua en la entrega de servicios tecnológicos en la organización.

Las solicitudes que recibe un centro de servicios por parte de los usuarios pueden ser por [46]: Vía telefónica, Correo electrónico, Módulo de atención al cliente, Chat, Portal web, Personalmente o por solicitud (documentación).

Cuadro 8. Procesos para la Operación de los Servicios TI

PROCESOS PARA LA OPERACIÓN DE LOS SERVICIOS TI		
Gestión de Eventos	*Gestión de incidencias*	*Petición de Servicios*
Monitorear eventos sobre la infraestructura TI y ayudar a prevenir incidencias futuras	*Registrar incidencias, verificar niveles de calidad del servicio y restaurarlos en el menor tiempo posible*	*Gestionar peticiones de usuarios que requieren pequeños cambios en la prestación del servicio.*
Gestión de Problemas		*Gestión de Acceso a los servicios de TI*
Analizar y ofrecer soluciones a los incidentes recurrentes		*Garantizar la protección de la información implementando permisos.*

Fuente: Elaboración Propia, basado en [47]

Las relaciones entre los procesos de la gestión de TI son importantes para establecer un centro de servicios eficaz y funcional contemplando la continuidad del negocio como uno de sus principales objetivos.

Una encuesta en línea realizada en el año 2011 a 169 empresas tecnológicas (38%) y no tecnológicas (64%) de 8 países de América Latina (México, Colombia, Perú, Guatemala, Ecuador, Republica Dominicana y Brasil) para determinar la importancia de la creación de una oficina de gestión de servicios, en las que incluyeron preguntas sobre la empresa, datos del encuestado, actividades del departamento de TI (como la evaluación del rendimiento, herramientas de escritorio, entre otras), preguntas relacionadas con ITIL, y preguntas acerca de la existencia o la conveniencia de una oficina de soporte de servicios (SMO) dentro de la estructura organizativa. De las empresas que participaron en la encuesta el 19% fueron pequeñas, el 17% mediana y el 64% de gran tamaño, siendo el 82% de ellas empresas profesionales relacionadas con la gestión de TI. Luego de un análisis probabilístico se determinó que en el 66% de estas empresas está representado un departamento de TI, el 56% se encuentra satisfecho con una solución Help Desk para la gestión de servicios y el 60% de las empresas en las que no se ha implementado un departamento de TI considera que la persona idónea para liderarlo debe ser el Director de TI [48].

La implementación de un centro de gestión de servicios TI es necesario para orientar a las empresas hacia la mejora continua de sus procesos, sin importar el tamaño o número de empleados de los cuales dispongan para la gestión de TI, ya que en un ambiente de constantes cambios tecnológico, la utilización de marcos de gestión en las empresas pueden impulsar su crecimiento.

2.2.6.4 El outsouring o externalización.- El outsouring es un proceso que consiste en encomendar a un agente especializado un área o actividades con la finalidad de mejorar su eficiencia [49].

La ejecución de procesos y actividades relacionadas con las TI de una organización por parte de un tercero a quien se le transfiere responsabilidades y se rige a un contrato que contiene acuerdos de nivel de servicio es considerada como outsouring o externalización [50].

La externalización de actividades es un proceso en el que la responsabilidad parcial o total de las TI son es asignada a un ente independiente que es monitoreado por medio de contratos o acuerdo de calidad de servicio.

En las últimas décadas el auge de actividades externalizadas ha surgido por la reducción de costes, sin embargo los retos críticos como la seguridad de los datos y la erosión de conocimientos internos generan problemas a los subcontratistas, que pueden ser controlados con Acuerdos de Nivel de Servicio (ANS) o contratos que a menudo contempla clausulas para reducir contingencias, riesgos, entre otros inconvenientes [11].

La decisión de externalizar como tal debe formar parte de la dirección estratégica en función de las capacidades o competencias que tiene la empresa en las actividades tomando como referencia su actividad con el fin de obtener la capacidades que la empresa requiere, por esto se deben externalizar aquellas actividades que no estén basadas en recursos estratégicos, siendo las de un valor estratégico medio y bajo candidatas a ser externalizadas [51].

Existen 2 tipos de outsourcing que puede emplear una empresa en el desarrollo de sus actividades [49]: Periférica en donde la empresa externaliza actividades poco relevantes y la Central en donde la empresa externaliza actividades estratégicas y de larga duración en donde el departamento de sistemas de información pasa a manos de un proveedor externo.

En un análisis realizado en la ciudad de valencia se determinó que las pequeñas (24%) y medianas (31%) consideran a la reducción de costes como una de las mayores ventajas de la externalización mientras que en las grandes empresas destacan el acceso a perfiles, conocimiento y tecnología como la mayor ventaja. Aunque el 20% de las empresas encuestadas no mencionara inconvenientes para externalizar tareas algunas de ellas consideran a la pérdida de control, coste, falta de agilidad y capacidad de respuesta del proveedor y dificultad de comunicación con el proveedor razones que obstaculizan la implementación de esta modalidad de servicios, siendo los más externalizados en el área de servicios TI las Infraestructuras como las Aplicaciones y Sistemas que en porcentajes representa el 11,3% de empresas que externalizan únicamente la gestión de infraestructura, el 27,6% exclusivamente las aplicaciones informáticas y el 60,1% que contrata ambas [52].

2.2.7 COBIT 5 Business framework.- COBIT 5 es un Marco de negocio usado para el Gobierno y la Gestión de las TI para las empresas [53], adaptable para todo tipo de empresa sea esta del sector comercial, productivo o de ningún propósito lucrativo, empresas públicas o privadas y permite que las tecnologías sean dirigidas por toda la organización de forma global es decir cubre a la empresa completa de inicio a fin,

considera áreas funcionales que compromete la responsabilidad de la tecnología de la información [4].

El marco se compone de 5 principios, 7 catalizadores y 36 procesos dispersos entre los dominios y áreas clave (gobierno y gestión).

ISACA [53] establece los siguientes principios de COBIT 5:

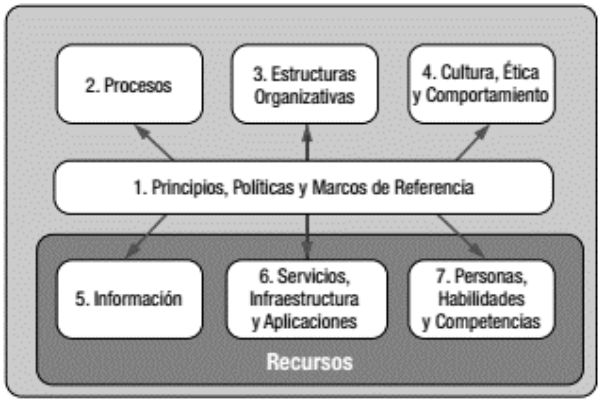
Figura 3. Principios de COBIT 5.

Fuente: P. C. Mercado, ISACA [53]

1. Como integrador: Un marco de referencia de gobierno y gestión para la información y tecnología relacionada que inicia por evaluar las necesidades de tecnología de los stakeholders.
2. Motivado por el valor a los stakeholders
3. Enfocado en el negocio y su contexto
4. Basado en habilitadores, definidos en el marco de referencia como aquellos recursos que permiten el éxito de TI
5. Estructurado en el gobierno y gestión En esencia, COBIT 5 cubre de manera completa la organización y provee una base de integración de otros marcos de referencia, estándares y mejores prácticas que algunas organizaciones pueden ya estar usando.

Los catalizadores de COBIT 5 le permiten optimizar las inversiones de las TI y uso con el propósito de beneficiar a las partes interesadas.

Figura 4. Catalizadores de COBIT 5.



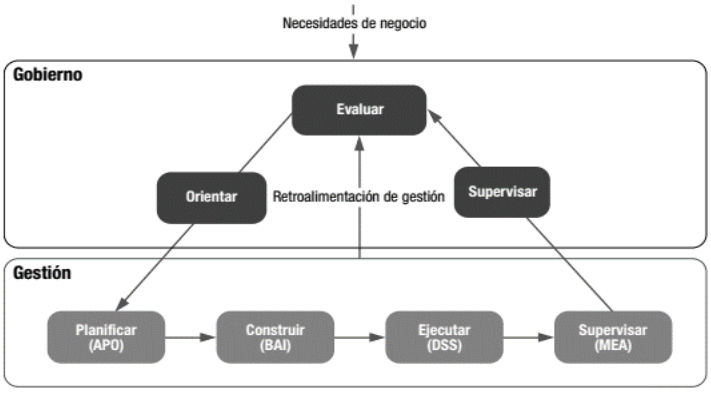
Fuente: P. C. Mercado, ISACA [53]

COBIT 5 distingue al gobierno y gestión como áreas clave de su modelo, por tal motivo las define como:

Gobierno: Permite asegurar que se valoren las necesidades, condiciones y opciones de los interesados para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; [53].

Gestión: Permite planificar, construir, ejecutar y controlar actividades alineadas con la trazado establecido por el cuerpo de gobierno para lograr las metas de las empresa [53].

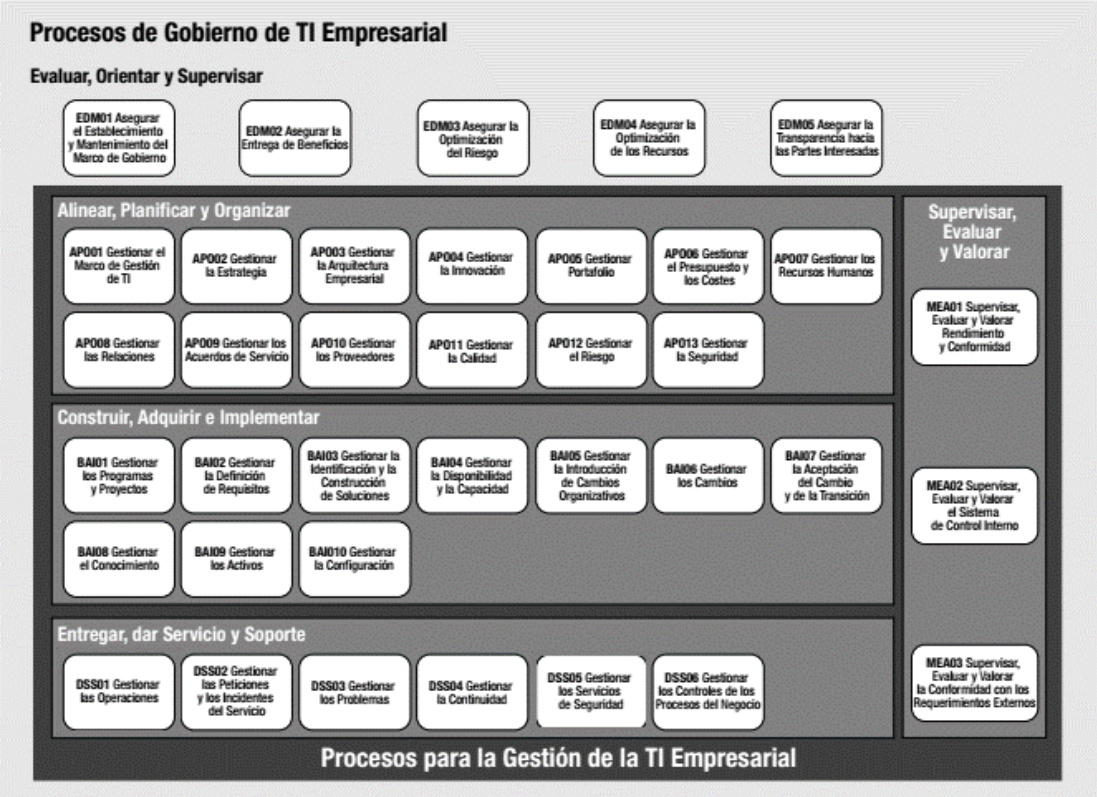
Figura 5. Áreas clave de Gobierno y Gestión de COBIT 5.



Fuente: P. C. Mercado, ISACA [53]

De los 36 procesos con los que cuenta COBIT 5, su análisis se limitara a los procesos de Gestión de Operaciones y Gestión de Servicios de Seguridad, de acuerdo al contexto de investigación.

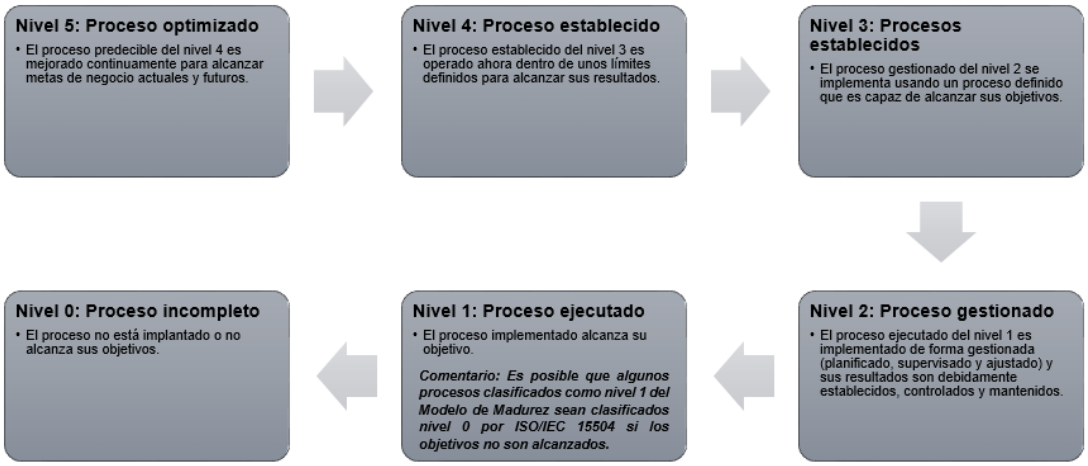
Figura 6. Modelo de Referencias de Procesos de COBIT 5.



Fuente: P. C. Mercado, ISACA [53]

COBIT 5 ya no usa el niveles de madurez descrito en su versión anterior, en cambio empresa niveles de capacidad tomados de la norma ISO/IEC 15504 para la evaluación de la capacidad de procesos; resultando como requisitos de cada proceso: “descripción del proceso, con la declaración de propósitos, prácticas base y los productos de trabajo, que son el equivalente a las entradas y salidas en términos de COBIT 5” [53].

Figura 7. Capacidad del Proceso basada en ISO/IEC 15504.



Fuente: Elaboración Propia

2.2.7.1 Proceso DSS01: Gestión de Operaciones. COBIT 5 determina que este proceso se encargara de la coordinación ejecución de actividades y procedimientos operativos requeridos para conceder servicios de TI tanto internos y subcontratados [53], este proceso requiere de la ejecución de procedimientos operativos y actividades de supervisión, con el propósito de que entregar los resultados de los servicios operativos como se habían concebido.

Cuadro 9. Prácticas del proceso DSS01: Gestión de Operaciones

DSS01 GESTION DE OPERACIONES		
DSS01.01 Realizar procedimientos operacionales.		
Contexto	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente	
ACTIVIDADES	1	Desarrollar y mantener procedimientos operativos y actividades relacionadas para dar apoyo a todos los servicios entregados.
	2	Mantener una programación de actividades operativas, ejecutar las actividades y gestionar el desempeño y rendimiento (throughput) de las actividades programadas.

Cuadro 9. (Continuación)

DSS01 GESTION DE OPERACIONES		
DSS01.01 Realizar procedimientos operacionales.		
ACTIVIDADES	3	Asegurar que se cumple con los estándares de seguridad aplicables para la recepción, procesamiento, almacenamiento y salida de datos de forma tal que se satisfagan los objetivos empresariales, la política de seguridad de la empresa y los requerimientos regulatorios.
	4	Verificar que todos los datos esperados para su procesamiento sean recibidos y procesados por completo y de una forma precisa y oportuna. Entregar los resultados de acuerdo con los requisitos de la empresa. Dar soporte a las necesidades de reinicio y reprocesamiento. Asegurar que los usuarios reciben los resultados adecuados de una forma segura y oportuna.
	5	Programar, realizar y registrar las copias de respaldo de acuerdo con las políticas y procedimientos establecidos.
DSS01.02 Gestionar los servicios de TI externalizados.		
Contexto	Gestionar la operación de servicios externalizados de TI para mantener la protección de la información empresarial y la confiabilidad de la entrega del servicio.	
ACTIVIDADES	1	Asegurar que los procesos de información se adhieren a los requerimientos de inseguridad de la empresa y conformes con los contratos y ANS con terceros que alojan o proveen servicios.
	2	Asegurar que los requerimientos operativos del negocio y de procesamiento de TI, así como a las prioridades en la entrega del servicio se adhieren y son conformes a los contratos y ANS con terceros que alojan o proveen servicios.
	3	Integrar los procesos críticos de TI con los de los proveedores de servicios externalizados cubriendo, por ejemplo, la planificación de la capacidad y el rendimiento, la gestión de cambio, la gestión de configuración, la gestión de peticiones de servicio y de incidentes, la gestión de problemas, la gestión de la seguridad, la continuidad de negocio y la monitorización y notificación del desempeño de procesos.

Cuadro 9. (Continuación)

DSS01 GESTION DE OPERACIONES		
DSS01.02 Gestionar los servicios de TI externalizados.		
ACTIVIDADES	4	Planificar la realización de auditorías y aseguramientos independiente de los entornos operativos de los proveedores de externalización (outsourcing) para confirmar que los requerimientos acordados están recibiendo el tratamiento adecuado.
DSS01.03 Supervisar la infraestructura de TI.		
Contexto	Supervisar la infraestructura TI y los eventos relacionados con ella. Almacenar la suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias de tiempo y las actividades relacionadas con el soporte de esas operaciones y las actividades relacionadas con el soporte de esas operaciones.	
ACTIVIDADES	1	Registrar eventos, identificando el nivel de información a ser grabada sobre la base de una consideración del riesgo y el rendimiento.
	2	Identificar y mantener una lista de los activos de infraestructura que necesiten ser monitorizados en base a la criticidad del servicio y la relación entre los elementos de configuración y los servicios que de ellos dependen.
	3	Definir e implementar reglas que identifican y registren violaciones de umbral y condiciones de eventos. Encontrar un equilibrio entre la generación de eventos falsos menores y eventos significativos, de forma tal que los registros de eventos no estén sobrecargados con información innecesaria.
	4	Producir registros de eventos y retenerlos por un periodo apropiado para asistir en investigaciones futuras.
	5	Establecer procedimientos para supervisar los registros de eventos y llevar a cabo revisiones periódicas.

Cuadro 9. (Continuación)

DSS01 GESTION DE OPERACIONES		
DSS01.03 Supervisar la infraestructura de TI.		
ACTIVIDADES	6	Asegurar que se crean oportunamente los tiques de incidente cuando la monitorización identifica desviaciones de los umbrales definidos.
DSS01.04 Gestionar el medio ambiente.		
Contexto	Mantener las medidas para la protección contra factores ambientales. Instalar equipamiento y dispositivos especializados para supervisar y controlar el entorno.	
ACTIVIDADES	1	Identificar desastres naturales y causados por el ser humano que puedan ocurrir en el área donde se encuentran las instalaciones de TI. Evaluar el efecto potencial en las instalaciones de TI.
	2	Identificar de qué manera el equipamiento de TI, incluyendo el equipamiento móvil y el ubicado fuera de las instalaciones, está protegido contra las amenazas del entorno. Asegurar que la política limite o impida comer, beber y fumar en áreas sensibles y que se prohíba almacenamiento de material de oficina y otros suministros que puedan representar un riesgo de incendio en los centros de procesamiento de datos.
	3	Ubicar y construir las instalaciones de TI para minimizar y mitigar la susceptibilidad ante las amenazas del entorno.
	4	Supervisar y mantener de forma periódica a los dispositivos que detectan proactivamente las amenazas del entorno (p. ej. Fuego, agua, humo, humedad)
	5	Responder a las alarmas y otras notificaciones del entorno. Documentar y probar los procedimientos, lo que debería incluir la priorización de alarmas y el contacto con las autoridades locales de respuesta ante emergencias y entrenar al personal en estos procedimientos.

Cuadro 9. (Continuación)

DSS01 GESTION DE OPERACIONES		
DSS01.04 Gestionar el medio ambiente.		
ACTIVIDADES	6	Comparar medidas y planes de contingencia respecto a los requerimientos de las pólizas de seguros e informar de los resultados. Atender a los puntos de no-conformidad de manera oportuna.
	7	Asegurar que los sitios de TI están construidos y diseñados para minimizar el impacto del riesgo del entorno (p. ej. Robo, aire, fuego, humo, agua, vibración, terrorismo, vandalismo, productos químicos, explosivos). Considerar zonas específicas de seguridad o celdas a prueba de incendio (p. ej. ubicando los entornos/servicios de producción y de desarrollo alejados entre si).
	8	Mantener en todo momento a los sitios de TI y las salas de servidores limpias y en una condición segura (es decir, sin desorden, sin papel ni cajas de cartón, sin papeleras llenas, sin productos químicos o materiales inflamables).
DSS01.05 Manejo de las instalaciones.		
Contexto	Gestionar las instalaciones, incluyendo equipos de electricidad y comunicaciones, en línea con las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo.	
ACTIVIDADES	1	Examinar los requerimientos de las instalaciones de TI respecto a la protección frente a la fluctuación y cortes de la energía eléctrica, en relación con otros requerimientos de la planificación de la continuidad del negocio. Disponer de equipamiento adecuado de alimentación interrumpida (p. ej. baterías, generadores) para dar soporte a la planificación de continuidad de negocio.
	2	Probar periódicamente los mecanismos del sistema de alimentación interrumpida (SAI) y asegurar que la electricidad puede ser conmutada al sistema sin efectos significativos en las operaciones del negocio.

Cuadro 9. (Continuación)

DSS01 GESTION DE OPERACIONES		
DSS01.05 Manejo de las instalaciones.		
ACTIVIDADES	3	Asegurar que las instalaciones que alojan los sistemas de TI tienen más de un proveedor para los servicios públicos indispensables (p. ej. Electricidad, telecomunicaciones, agua, gas). Separar la acometida de cada servicio.
	4	Confirmar que el cableado externo al sitio TI está bajo tierra o que tiene una protección alternativa adecuada. Determinar que el cableado en el sitio TI está contenido en productos asegurados y que los armarios de cableado tienen su acceso restringido al personal autorizado. Proteger adecuadamente al cableado contra el daño causado por fuego, humo, agua, interceptación e interferencia.
	5	Asegurar que el cableado y el patching físico (datos y telefonía) están estructurados y organizados. Las estructuras de cableado y de conductos debieran estar documentadas (p. ej. Olano del edificio y diagramas de cableado).
	6	Analizar las instalaciones que alojan los sistemas de alta disponibilidad para verificar el cumplimiento de los requerimientos de cableado (externo e interno) en cuanto a redundancia y tolerancia a fallos.
	7	Asegurar que los sitios e instalaciones de TI cumplen de manera sistemática con la legislación, regulaciones, directrices y especificaciones relevantes de salud y seguridad en el trabajo.
	8	Proporcionar periódicamente formación al personal en la legislación, regulaciones y directrices relevantes de salud y seguridad en el trabajo. Capacitar al personal en simulacros de incendio y rescate para asegurar el adecuado conocimiento y las acciones apropiadas a tomar en caso de incendio o incidentes similares.
	9	Registrar, supervisar, gestionar y resolver incidentes en las instalaciones siguiendo los procesos de gestión de incidentes de TI. Poner a disposición proveedor. El mantenimiento debe ser realizado únicamente por personal autorizado.

Cuadro 9. (Continuación)

DSS01 GESTION DE OPERACIONES		
DSS01.05 Manejo de las instalaciones.		
ACTIVIDADES	10	Asegurar que los sitios y el equipamiento de TI son mantenidos de acuerdo con los intervalos de servicio y las especificaciones recomendados por el proveedor. El mantenimiento debe ser realizado únicamente por personal autorizado.
	11	Analizar las alteraciones físicas a los sitios o localizaciones de TI para reevaluar el riesgo del entorno (p. ej. Daño por fuego o agua). Informar los resultados de este análisis a los niveles directivos de comunidad de negocio y de gestión de edificios.

Fuente: ISACA, [17]

Luego de analizar la magnitud que le que le asigna COBIT 5 a este proceso, se puede determinar que la Gestión de Operaciones es un proceso que requiere actividades para monitorear la infraestructura TI, supervisar los servicios externalizados, mantener un historial de eventos, que faciliten la reconstrucción de las operaciones internas o externas en el caso de imprevistos, además de establecer medidas de protección al medio ambiente y cumplimiento de leyes, reglamentos y requisitos técnicos para el buen manejo de las instalaciones con ayuda de procedimientos predefinidos.

2.2.7.2 Proceso DSS05: Gestión de Servicios de Seguridad. COBIT 5 determina que este proceso se encargara de "proteger la información de la empresa para mantener el nivel de riesgo aceptable de la información de acuerdo con la política de seguridad" [53]; este proceso requiere definir y conservar los roles y privilegios de seguridad para el acceso de la información y supervisarlos con el propósito de disminuir el impacto que provoca en el negocio las falencias de la de seguridad de la información operativa e incidentes.

Cuadro 10. Practicas del proceso DSS01: Gestión de Servicios de Seguridad.

DSS05 GESTION DE SERVICIOS DE SEGURIDAD		
DSS05.01 Proteger contra el malware.		
Contexto	Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía -spyware- y correo basura).	
ACTIVIDADES	1	Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.
	2	Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).
	3	Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.
	4	Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).
	5	Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de pishing).
	6	Realizar formación periódica sobre software malicioso en el uso del correo electrónico e internet. Formar a los usuarios para no instalarse software compartido o no autorizado.
DSS05.02 Gestión de la red y la seguridad de la conexión.		
Contexto	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.	
ACTIVIDADES	1	Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones.
	2	Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña.

Cuadro 10. (Continuación)

DSS05 GESTION DE SERVICIOS DE SEGURIDAD		
DSS05.02 Gestión de la red y la seguridad de la conexión.		
ACTIVIDADES	3	Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.
	4	Cifrar la información en tránsito de acuerdo con su clasificación.
	5	Aplicar los protocolos de seguridad aprobados a las conexiones de red.
	6	Configurar equipos de red de forma segura.
	7	Establecer mecanismos de confianza para apoyar la transmisión segura y recepción de información.
	8	Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.
	9	Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.
DSS05.03 Administrar la seguridad del punto final.		
Contexto	Asegurar que los puestos de usuario final (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida).	
ACTIVIDADES	1	Configurar los sistemas operativos de forma segura.
	2	Implementar mecanismos de bloqueo del dispositivo.
	3	Cifrar la información de almacenamiento de acuerdo con su clasificación.
	4	Gestionar el acceso y control remoto.
	5	Gestionar la configuración de la red de forma segura.
	6	Implementar el filtrado del tráfico de la red en dispositivos de usuario final.
	7	Proteger la integridad del sistema.
	8	Proveer de protección física a los dispositivos de usuario final.
	9	Deshacerse de los dispositivos de usuario final de forma segura.

Cuadro 10. (Continuación)

DSS05 GESTION DE SERVICIOS DE SEGURIDAD		
DSS05.04 Manejo de la identidad del usuario y el acceso lógico.		
Contexto	Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio.	
ACTIVIDADES	1	Mantener los derechos de acceso de usuario de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer.
	2	Identificar unívocamente todas las actividades de proceso de la información de roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos por el propio negocio en las aplicaciones de procesos de negocio.
	3	Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación con aplicaciones usadas en procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.
	4	Administrar todos los cambios de derecho de acceso (creación, modificación, eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.
	5	Segregar y gestionar cuentas de usuarios privilegiadas.
	6	Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.
	7	Asegúrese de que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocios, infraestructura de TI, las operaciones del sistema, desarrollo y mantenimiento) son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información por usuario.

Cuadro 10. (Continuación)

DSS05 GESTION DE SERVICIOS DE SEGURIDAD		
DSS05.04 Manejo de la identidad del usuario y el acceso lógico.		
	8	Mantener una pista de auditoría de accesos a la información clasificada como altamente sensible.
DSS05.05 Administrar el acceso físico a los activos de TI.		
Contexto	Definir e implementar procedimientos para conceder, limitar y revocar el acceso a locales, edificios y áreas de acuerdo a las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, empleados temporales, clientes, vendedores, visitantes o cualquier otra tercera parte.	
ACTIVIDADES	1	Gestionar las peticiones y concesión de acceso a las instalaciones de procesamiento. Las peticiones formales de acceso deben ser completadas y autorizadas por la dirección de la ubicación de TI, y guardado el registro de petición. Los formularios deberían identificar específicamente las áreas a las que el individuo tiene acceso concebido.
	2	Asegurarse de que todos los puntos de entrada están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en funciones de trabajo y responsabilidades.
	3	Registrar y supervisar todos los puntos de entrada a los sitios de TI. Registrar a todos los visitantes de la ubicación, incluyendo contratistas y vendedores.
	4	Instruir a todo el personal para mantener visible la identificación en todo momento. Prevenir la expedición de tarjetas o placas de identidad sin la autorización adecuada.
	5	Escoltar a los visitantes en todo momento mientras esté en la ubicación. Si se encuentra a un individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, se deberá alertar al personal de seguridad.

Cuadro 10. (Continuación)

DSS05 GESTION DE SERVICIOS DE SEGURIDAD		
DSS05.05 Administrar el acceso físico a los activos de TI.		
ACTIVIDADES	6	Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores. Asegurar que los dispositivos registren el acceso y disparen una alarma en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas llave, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos.
	7	Realizar regularmente formación de concienciación de seguridad física.
DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.		
Contexto	Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (token) de seguridad.	
ACTIVIDADES	1	Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formas especiales y dispositivos de salida, dentro, en y fuera de la empresa.
	2	Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basadas en el principio del menor privilegio, equilibrando riesgos y requisitos de negocio.
	3	Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones.
	4	Establecer salvaguardas físicas apropiadas sobre formularios especiales y dispositivos sensibles.
	5	Destruir la información sensible y proteger dispositivos de salida (por ejemplo, la desmagnetizando soportes magnéticos, destruir físicamente dispositivos de memoria, poniendo trituradoras o papeleras cerradas disponibles para distribuir formularios especiales y otros documentos confidenciales).

Cuadro 10. (Continuación)

DSS05 GESTION DE SERVICIOS DE SEGURIDAD		
DSS05.07 Supervisar la infraestructura para eventos relacionados con la seguridad.		
Contexto	Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.	
ACTIVIDADES	1	Registrar los sucesos relacionados con la seguridad reportada por las herramientas de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo. Retenerla por un periodo apropiado para asistir en futuras investigaciones.
	2	Definir y comunicar la naturaleza y las características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta conmensurada.
	3	Revisar regularmente los registros de eventos para los incidentes potenciales.
	4	Mantener un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales y asegurar que todos los empleados están concienciados de los requerimientos.
	5	Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.

Fuente: ISACA, [17]

Luego de analizar la magnitud que le que le asigna COBIT 5 a este proceso, se puede determinar que la Gestión de Servicios de Seguridad se encarga de hacer cumplir los privilegios de acceso lógico y físico de los usuarios, además del mantenimiento, seguimiento y protección del software, hardware y conexión a las redes.

2.2.8 Marco de Trabajo ITIL V3 2011. La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL, es un marco de trabajo con buenas prácticas destinadas a ofrecer tanto a los proveedores como receptores las tareas y procesos que faciliten la entrega de servicios TI. “ITIL es a veces considerado

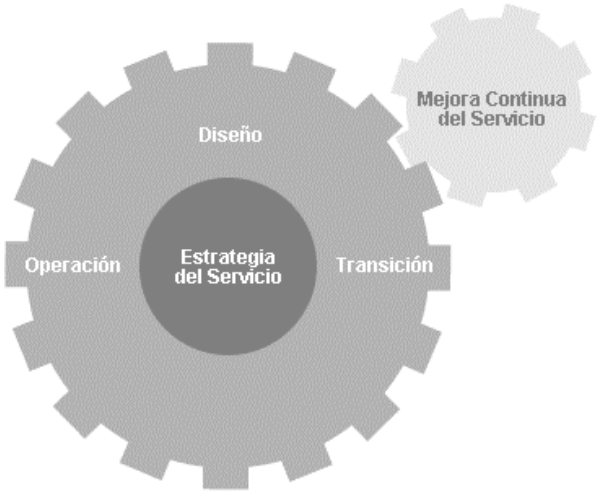
como un marco para el Gobierno TI sus objetivos son más modestos pues se limitan exclusivamente a aspectos de gestión" [5]. Mediante los procesos que propone ITIL, un departamento de TI puede supervisar y gestionar eficazmente los sistemas, el mantenimiento rutinario, las operaciones de externalización y la administración de las TI [54].

2.2.8.1 Inicios del Marco de Trabajo ITIL V3 2011.- ITIL fue creado en el reino unido por la Oficina de comercio gubernamental (OGC) para organizar la gestión de TI en el sector público; ahora administrado por el Foro de Tecnología de Gestión de Servicios de Información (itSMF). Uno de los objetivos principales de ITIL es transformar los departamentos de TI en organizaciones orientadas a servicios. En la actualidad ITIL es el enfoque más ampliamente aceptado para la gestión de servicios en el mundo, pues tiene un proceso iterativo, multidimensional y ciclo de vida en estructura [55].

2.2.8.2 Ciclo de Vida de los Servicios.- ITIL proporciona una visión global de la gestión de servicios TI compuesta por procesos y funciones a lo largo de cada una de las fases del ciclo de vida del servicio. ITIL v3 comprende cinco libros: Estrategia del Servicio, Diseño del Servicio, Transición del Servicio, Operación del Servicio y Mejora Continua del Servicio [56]. En [5] se desglosa 5 fases:

- Estrategia del Servicio: Destinada a tratar a la gestión de servicios como un activo estratégico.
- Diseño del Servicio: Enmarca principios y métodos imprescindibles para la transformación los objetivos estratégicos en portafolios de servicios y activos.
- Transición del Servicio: Enmarca la transición para poner en funcionamiento nuevos servicios o su mejora.
- Operación del Servicio: Enmarca las prácticas para la gestión diaria en la operación del servicio.
- Mejora Continua del Servicio: provee una guía para la creación y sostenimiento del valor ofrecido a los clientes en las fases anteriores y obtener un servicio optimizado.

Figura 8. Ciclo de Vida del Servicio.



Fuente: OSIATIS S.A. [5].

Durante todo el marco de gestión de servicios TI se emplean conceptos básicos de función, proceso y rol; estos conceptos facilitan su comprensión.

Definiciones básicas usadas por ITIL;

- Función “es una unidad especializada en la realización de una cierta actividad y es la responsable de su resultado” [6] e incorporan todos los recursos, capacidades y estructuras necesarias para el correcto desarrollo de un proceso específico.
- Proceso “es un conjunto de actividades interrelacionadas orientadas a cumplir un objetivo específico” [6]. Los procesos ron la respuesta a eventos suscitados que pueden ser medidos en base a su rendimiento.
- Rol “es un conjunto de actividades y responsabilidades asignada a una persona o un grupo. Una persona o grupo puede desempeñar simultáneamente más de un rol” [6]. Los roles genéricos de la gestión de servicios TI son Gestor del Servicio, Propietario del Servicio, Gestor del Proceso y Propietario del Proceso.

Figura 9. Procesos y Funciones del Ciclo de Vida de Servicios.

Fuente: Elaboración Propia

Cada una de las fases contiene procesos y actividades, como se presenta a continuación:

Cuadro 11. Procesos y Actividades de ITIL V3:2011

1	**Fase de Estrategia**
1.1.	**Gestión Financiera**
1.1.1	Presupuesto
1.1.2	Contabilidad
1.2.	**Gestión del Portfolio de Servicios**
1.2.1	Definición del Negocio
1.2.2	Desarrollo de la Oferta
1.3.	**Gestión de la Demanda**
1.3.1	Análisis de actividad
1.3.2	Desarrollo de la oferta
2	**Fase de Diseño**
2.1.	**Gestión del Catálogo de Servicios**
2.1.1	Definición de las familias principales de servicios a prestar, registro de los servicios en activo y de la documentación asociada a los mismos.
2.1.2	Mantenimiento y actualización del Catálogo de Servicios

Cuadro 11. (Continuación)

2	Fase de Diseño
2.2.	**Gestión de Niveles de Servicio**
2.2.1.	Planificación de los Niveles de Servicio
2.2.2.	Implementación de los Acuerdos de Niveles de Servicio:
2.2.3.	Supervisión y revisión de los Acuerdos de Nivel de Servicio:
2.3.	**Gestión de la Capacidad**
2.3.1	Monitorización de los recursos de la infraestructura TI.
2.3.2	Supervisión de la capacidad
2.4.	**Gestión de la Disponibilidad**
2.4.1	Determinar cuáles son los requisitos de disponibilidad reales del negocio.
2.4.2	Desarrollar un plan de disponibilidad donde se estime el futuro a corto y medio plazo.
2.4.3	Mantenimiento del servicio en operación y recuperación del mismo en caso de fallo.
2.5.	**Gestión de la Continuidad de los Servicios TI**
2.5.1	Establecer las políticas y alcance de la ITSCM.
2.5.2	Evaluar el impacto en el negocio de una interrupción de los servicios TI.
2.5.3	Analizar y prever los riesgos a los que está expuesto la infraestructura TI.
2.5.4	Establecer las estrategias de continuidad del servicio TI.
2.5.5	Desarrollar los planes de contingencia.
2.5.6	Poner a prueba dichos planes.
2.5.7	Revisar periódicamente los planes para adaptarlos a las necesidades reales del negocio.
2.6.	**Gestión de la Seguridad de la Información**
2.6.1	Constituya política de seguridad que oriente a la empresa
2.6.2	Realizar un Plan de Seguridad que integre los límites de seguridad adecuados descritos en los acuerdos de servicio firmados con proveedores internos y externo
2.6.3	Supervisión proactiva de los límites de seguridad analizando tendencias, nuevos riesgos y vulnerabilidades.
2.7.	**Gestión de Proveedores**
2.7.1	Los requisitos de contratación que se van a exigir a los proveedores.
2.7.2	Los procesos de evaluación y selección de proveedores.
2.7.3	La clasificación y documentación de la relación con los proveedores.
2.7.4	Gestión del Rendimiento de los proveedores
2.7.5	Renovación o terminación.

Cuadro 11. (Continuación)

3	Fase de Transición
3.1.	**Planificación y soporte a la Transición**
3.1.1.	Estrategia de transición
3.1.2.	Preparación de transición
3.1.3.	Planificación de la transición
3.2.	**Gestión de Cambios**
3.2.1	Registro de peticiones
3.2.2	Aceptación y Clasificación del cambio
3.2.3	Aprobación y Planificación del cambio
3.2.4	Implementación del cambio
3.2.5	Evaluación del cambio
3.2.6	Cambios de emergencia
3.3	**Gestión de la Configuración y Activos del Servicio**
3.3.1	Planificación de la Configuración
3.3.2	Clasificación y registro de los Elementos de Configuración
3.3.3	Monitorización y Control de los Elementos de Configuración
3.3.4	Realización de auditorías
3.4.	**Gestión de Entregas y Despliegues**
3.4.1.	Planificación de entregas
3.4.2.	Desarrollo del despliegue
3.4.3.	Implementación de la entrega
3.4.4.	Comunicación y formación al cliente
3.5.	**Validación y pruebas**
3.5.1	Validación, planificación y verificación de tests
3.5.2	Construcción de tests
3.5.3	Pruebas de Validación
3.5.4	Aceptación y reporte
3.5.5	Limpieza y cierre
3.6.	**Evaluación**
3.6.1.	Planificación de la evaluación.
3.6.2.	Evaluación del rendimiento previsto.
3.6.3.	Evaluación del rendimiento real.
3.7.	**Gestión del Conocimiento**
3.7.1.	Puntualizar una estrategia de Gestión del Conocimiento y divulgarla a toda la empresa.
3.7.2.	Mejora la transmisión de conocimiento entre personas, equipos y departamentos
3.7.3.	Gestionar la información para certificar su calidad y utilidad.

Cuadro 11. (Continuación)

3	**Fase de Transición**
3.7.	**Gestión del Conocimiento**
3.7.	Gestión del Conocimiento
3.7.4.	Uso del Sistema de Gestión del Conocimiento del Servicio (SKMS).
4	**Fase de Operación**
4.1.	**Gestión de Eventos**
4.1.1	Notificación de eventos
4.1.2	Detección y filtrado de eventos
4.1.3	Clasificación de eventos
4.1.4	Correlación
4.1.5	Disparadores
4.2.	**Gestión de Incidencias**
4.2.1	Registro y clasificación
4.2.2	Análisis, resolución y cierre
4.3.	**Gestión de Peticiones**
4.3.1	Selección de peticiones
4.3.2	Aprobación financiera
4.3.3	Tramitación y cierre
4.4.	**Gestión de Problemas**
4.5.1	Control de Problemas
4.5.2	Control de Errores
4.5.	**Gestión de Acceso a los Servicios TI**
4.5.1	Verificación.
4.5.2	Monitorización de identidad.
4.5.3	Registro y monitorización de accesos.
4.5.4	Eliminación y restricción de derechos.
5	**Fase de Mejora**
5.1.	**Proceso de Mejora**
5.2.	**Informes de Servicios TI**

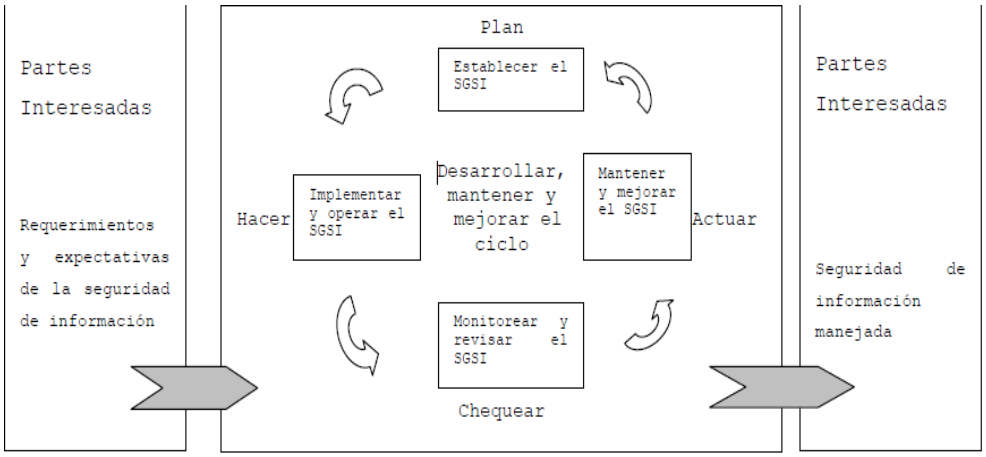
Fuente: OSIATIS S.A. [5].

*2.2.9 Estándar ISO/IEC 27001:2005***.-** Es una norma internacional que proporciona modelos para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora del sistema de gestión de seguridad de la información de una empresa [57], en donde se encuentran los estándares y las mejores acciones de seguridad de la información (objetivos de control y los controles), ya que debido a que las empresas tienen un gran manejo de tecnologías de la información, las cuales ayudan

a realizar transacciones comerciales vía web y en general, ha generado que existan riesgos o amenazas en el medio que afectan en el correcto desarrollo de las actividades del negocio, para contrarrestar amenazas las empresas han tenido que acudir a planes para hacerles frente a estos riesgos, dicho plan es conocido como sistema de gestión de seguridad (SGSI) [6].

2.2.9.1 Modelo PDCA.- ISO/IEC 27001:2005 adopta un Modelo PDCA aplicado a los procesos para el diseño e implementación de un Sistema de Gestión de Seguridad de la Información como se muestra a continuación:

Figura 10. Modelo PDCA.



Fuente: O. I. para la Estandarización and Comisión Electrotécnica Internacional, [14]

El modelo PDCA con sus 4 fases cíclicas le permite a un SGSI orientar los objetivos de control y controles de seguridad de la información a una mejora continua, puesto que inicialmente se plantean políticas, procedimientos y controles, posteriormente se implantan a la empresa, se monitorea y reporta su desempeño para identificar falencias en el SGSI y aplicar acciones correctivas y preventivas que permitan mejorar su efectividad.

Para la gestión de Operaciones y gestión de Servicios de Seguridad existen los objetivos de control y controles que entran en el contexto de la investigación. A continuación se muestran los controles usados por un SGSI:

Cuadro 12. Objetivos y controles de seguridad del Estándar ISO 27001:2005.

A.5	**Política de seguridad**
A.5.1	Política de seguridad de información
A.6	**Organización de la seguridad de la información**
A.6.1	Organización interna
A.6.2	Entidades externas
A.7	**Gestión de activos**
A.7.1	Responsabilidad por los activos
A.7.2	Clasificación de la información
A.8	**Seguridad de los recursos humanos**
A.8.1	Antes del empleo
A.8.2	Durante el empleo
A.8.3	Terminación o cambio del empleo
A.9	**Seguridad física y ambiental**
A.9.1	Áreas seguras
A.9.2	Seguridad del equipo
A.10	**Gestión de las comunicaciones y operaciones**
A.10.1	Procedimientos y responsabilidades operacionales
A.10.2	Gestión de la entrega del servicio de terceros
A.10.3	Planeación y aceptación del sistema
A.10.4	Protección contra software malicioso y código móvil
A.10.7	Gestión de medios
A.10.8	Intercambio de información
A.10.9	Servicios de comercio electrónico
A.10.10	Monitoreo

Cuadro 13. (Continuación)

A.11	**Control de acceso**
A.11.1	Requerimiento comercial para el control del acceso
A.11.2	Gestión del acceso del usuario
A.11.3	Responsabilidades del usuario
A.11.4	Control de acceso a redes
A.11.5	Control de acceso al sistema de operación
A.11.6	Control de acceso a la aplicación e información
A.11.7	Computación móvil y tele-trabajo
A.12	**Adquisición, desarrollo y mantenimiento de los sistemas de información**
A.12.1	Requerimientos de seguridad de los sistemas
A.12.2	Procesamiento correcto en las aplicaciones
A.12.3	Controles criptográficos
A.12.4	Seguridad de los archivos del sistema
A.12.5	Seguridad en los procesos de desarrollo y soporte
A.12.6	Gestión de vulnerabilidad técnica
A. 13	**Gestión de incidentes en la seguridad de la información**
A.13.1	Reporte de eventos y debilidades en la seguridad de la información
A.13.2	Gestión de incidentes y mejoras en la seguridad de la información
A.14	**Gestión de la continuidad comercial**
A.14.1	Aspectos de la seguridad de la información de la gestión de la continuidad comercial
A.15	**Cumplimiento**
A.15.1	Cumplimiento con requerimientos legales
A.15.2	Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico

Fuente: O. I. para la Estandarización and Comisión Electrotécnica Internacional, [14]

2.3 Objetivos del prototipo

2.3.1 Objetivo General

Proponer un modelo de Gestión de Operaciones y Servicios de Seguridad para las Tecnologías de Información mediante COBIT 5, ITILV3:2011 e ISO 27001:2005.

2.3.2 Objetivos Específicos

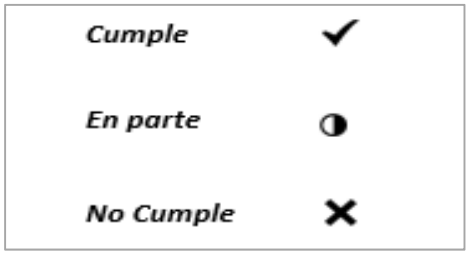
- Reforzar los procesos de Gestión de Operaciones y Gestión de Servicios de Seguridad planteados por COBIT 5 mediante ITIL V3:2011 e ISO 27001:2005.
- Realizar el mapeo entre el Marco de negocio usado para el Gobierno y la Gestión de las TI en las empresas - COBIT 5, marco de trabajo ITIL V3:2011 y el Estándar Internacional ISO 27001:2005.
- Validar el modelo a través de la opinión efectuada por expertos.

2.4 Diseño del prototipo

2.4.1 Mapeo entre COBIT 5, ITIL V3:2011 e ISO 27001:2005

Entre los modelos analizados COBIT 5 entra en el contexto de investigación por su enfoque de gestión de operaciones y servicios de seguridad, mientras que ITIL V3:2011 enmarca procesos y funciones que facilitan las operaciones de la gestión de la infraestructura de Tecnologías e ISO 27001 como estándar para crear, mantener o mejorar un Sistema de Gestión de la Seguridad Información; que trata parcialmente objetivos y controles útiles para gestionar los servicios de seguridad. A continuación se muestra un mapeo realizado en base a los procesos de COBIT 5.

Figura 11. Figuras de resultado de comparación del mapeo



Fuente: Elaboración Propia

2.4.1.1 Mapeo de los procesos de Gestión de Operaciones y Gestión de Servicios de Seguridad de COBIT 5 con los procesos de ITIL V3:2011.- Se realizara una respectiva comparación entre estas actividades, procesos y controles mencionados. Este análisis se lo ejecutara con el fin de identificar dentro de los procesos de Gestión de Operaciones y Gestión de Servicios de Seguridad del marco de gestión analizado cuales son las actividades que cumplen en su totalidad o en parte con lo planteado el Marco de Trabajo de ITIL V3:2011. Para realizar este análisis se utilizara la Figura 11 (Ver Anexo A).

Justificación del mapeo de los procesos de Gestión de Operaciones y Gestión de Servicios de Seguridad de COBIT 5 con los procesos de ITIL V3:2011 y los controles de ISO 27001:2005.

1. Fase de Estrategia

1.1 Gestión Financiera

1.1.1 Presupuesto VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **1.1.1** del proceso de **"Gestión Financiera"** de **ITIL V3:2011** propone realizar un **"Presupuesto"**, que consiste en

planificar el gasto de inversión TI a largo plazo, además de asegurar que los servicios TI están suficientemente financiados, la cual no encaja en el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas propone llevar a cabo presupuestos.

1.1.2 Contabilidad VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **1.1.2** del proceso de **"Gestión Financiera"** de **ITIL V3:2011** propone realizar revisar la **"Contabilidad"**, que consiste en realizar una correcta evaluación de los costes reales para su comparación con lo presupuestado, además de tomar decisiones de negocios basados en los costes de servicios, la cual no encaja en el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas propone llevar a cabo el control de la contabilidad en base a coste reales de TI.

1.1.3 Política de Precios VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **1.1.3** del proceso de **"Gestión del Portafolio de Servicios"** de **ITIL V3:2011** propone realizar una **"Política de Precios"**, que consiste establecer una política de fijación de precios, además de determinar las tarifas de los servicios, en función de la política elegida, los servicios solicitados, costes asociados y los precios vigentes en el mercado, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas propone establecer políticas de precios a los servicios prestados por la empresa.

1.2 Gestión del Portafolio de Servicios

1.2.1 Definición del Negocio VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **1.2.1** del proceso de **"Gestión del Portafolio de Servicios"** de **ITIL V3:2011** propone realizar la **"Definición del Negocio"**, que consiste en definir el nivel competitivo del negocio, encontrando sus puntos fuertes en el mercado, buscar las necesidades de los clientes existentes o potenciales, mantener un inventario de los servicios ofertados, la cual no cumple con los procesos DSS01 y DSS05 que propone COBIT 5; esto se debe a que el contexto que

se desarrolla en ellos no se enfoca hacia la definición del negocio orientado a la oferta de servicios en el mercado.

1.2.2 Análisis de servicios VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **1.2.2** del proceso de **"Gestión del Portafolio de Servicios"** de **ITIL V3:2011** propone realizar la **"Análisis de servicios"**, que consiste en establecer objetivos, prioridades de acción, actualizaciones y planificación de los servicios, la cual no cumple con los procesos DSS01 y DSS05 que propone COBIT 5; esto se debe a que el contexto que se desarrolla en ellos no se enfoca en realizar un análisis de servicios.

1.3 Gestión de la Demanda

1.3.1 Análisis de la actividad VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **1.3.1** del proceso de **"Gestión de la Demanda"** de **ITIL V3:2011** propone realizar la **"Análisis de la actividad"**, consiste en monitorizar patrones de actividad sobre la demanda de servicios en los procesos del negocio, con el propósito de predecir su demanda, la cual no cumple con los procesos DSS01 y DSS05 que propone COBIT 5; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas propone llevar a cabo el análisis de la actividad referente a la demanda de servicios.

1.3.2 Desarrollo de la Oferta VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **1.3.2** del proceso de **"Gestión de la Demanda"** de **ITIL V3:2011** propone realizar la **"Desarrollo de la Oferta"**, consiste en distinguir entre los servicios esenciales y de soporte para la elaboración de una serie de paquetes de servicio adaptados a los distintos segmentos de clientes.; la cual no cumple con los procesos DSS01 y DSS05 que propone COBIT 5; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas propone desarrollar la oferta de los servicios.

2. Fase de Diseño

2.1 Gestión del Catálogo de Servicios

2.1.1 Definición de las familias principales de servicios a prestar VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.1.1** del proceso de **"Gestión del Catálogo de Servicios"** de **ITIL V3:2011** propone realizar una **"Definición de las familias principales de servicios a prestar"**, consiste en el registro de los servicios prestados por la empresa, clientes y precios de cada servicio, la definición de este proceso no entra en el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas se refiere a dar una definición a cada uno de los servicios prestados.

2.1.2 Mantenimiento y actualización del Catálogo de Servicios VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.1.2** del proceso de **"Gestión del Catálogo de Servicios"** de **ITIL V3:2011** propone realizar el **"Mantenimiento y actualización del Catálogo de Servicios"**, consiste en aquellas tareas para la actualización de la actualización del catálogo de servicios; la definición de este proceso no entra en el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5 ; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas dar una definición a cada uso de los servicios prestados.

2.2 Gestión de Niveles de Servicio

2.2.1 Planificación de los Niveles de Servicio VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.2.1** del proceso de **"Gestión de Niveles de Servicio"** de **ITIL V3:2011** propone realizar una **"Planificación de los Niveles de Servicio"**, consiste en la asignación de recursos, elaboración de catálogos de servicio, desarrollo de los acuerdos de servicio, el estudio de las necesidades de los clientes, elaborar los requisitos de los niveles de servicio, en los que se plasma las necesidades de los clientes, expectativas, rendimiento, nivel de servicio y la elaboración de hojas de especificación, que ayudan a determinar a las empresas los procesos que pueden ser externalizados, por lo cual se considera que [17]:

- ***Proceso de Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

No cumple en la comparación con las actividades de la práctica DSS01.02 “Gestionar los servicios de TI externalizados”, pero si cumple con el contexto de la práctica (Ver cuadro 9 y 10).

La comparación de la actividad 2.2.1 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.
→ VS DSS01.03 Supervisar la infraestructura de TI.
→ VS DSS01.04 Gestionar el medio ambiente.
→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.
→ VS DSS05.02Gestión de la red y la seguridad de la conexión.
→ VS DSS05.03 Administrar la seguridad del punto final.
→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
→ VS DSS05.05 Administrar el acceso físico a los activos de TI.
→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de Niveles de Servicio** perteneciente a **ITIL V3:2011.**

2.2.2 Implementación de los Acuerdos de Niveles de Servicio VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.2.2** del proceso de **“Gestión de Niveles de Servicio”** de **ITIL V3:2011** propone realizar la **“Implementación de los Acuerdos de Niveles de Servicio”**, consiste en el proceso de negociación y elaboración de acuerdos y contratos por lo cual se considera que [53]:[17]:

- ***Proceso de Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

No cumple en la comparación con las actividades de la práctica DSS01.02 “Gestionar los servicios de TI externalizados”, pero si cumple con el contexto de la práctica (Ver cuadro 9 y 10).

La comparación de la actividad 2.2.2 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

→ VS DSS01.03 Supervisar la infraestructura de TI.

→ VS DSS01.04 Gestionar el medio ambiente.

→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

→ VS DSS05.03 Administrar la seguridad del punto final.

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de Niveles de Servicio** perteneciente a **ITIL V3:2011.**

2.2.3 Supervisión y revisión de los Acuerdos de Nivel de Servicio VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.2.3** del proceso de **“Gestión de Niveles de Servicio”** de **ITIL V3:2011** propone realizar la **“Supervisión y revisión de los Acuerdos de Nivel de Servicio”**, consiste en la elaboración de informes de rendimiento y el control de los proveedores externos lo cual [17]:

- ***Proceso de Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

No cumple en la comparación con la práctica DSS01.02 “Gestionar los servicios de TI externalizados”, en algunas de sus actividades. Esto se debe a que estas actividades **(1, 2)** (Ver cuadro 9 y 10) no se relacionan con la con el contexto de la actividad **2.2.3 “Supervisión y revisión de los Acuerdos de Nivel de Servicio”**, por tener otro

objetivo a desarrollar como lo es asegurar el cumplimiento de los requisitos establecidos en los contratos y acuerdos de niveles de servicio.

Pero también se considera ciertas coincidencias en las siguientes actividades de la práctica DSS01.02 de COBIT 5 las cuales tienen cierta relación con la actividad 2.2.3 de ITIL V3:2011, puesto que se considera que cumple con las actividades **3 y 4** (Ver cuadro 9 y 10) porque se refieren al seguimiento del proceso de rendimiento, presentación de informes y planificación de auditorías para el aseguramiento de los entornos operativos de los proveedores externos.

La comparación de la actividad 2.2.3 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***
  - → VS DSS01.01 Realizar procedimientos operacionales.
  - → VS DSS01.03 Supervisar la infraestructura de TI.
  - → VS DSS01.04 Gestionar el medio ambiente.
  - → VS DSS01.05 Manejo de las instalaciones.
- ***Gestión de Servicios de Seguridad***
  - → VS DSS05.01 Proteger contra el malware.
  - → VS DSS05.02Gestión de la red y la seguridad de la conexión.
  - → VS DSS05.03 Administrar la seguridad del punto final.
  - → VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
  - → VS DSS05.05 Administrar el acceso físico a los activos de TI.
  - → VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de Niveles de Servicio** perteneciente a **ITIL V3:2011.**

2.3 Gestión de la Capacidad

2.3.1 Monitorización de los recursos de la infraestructura TI VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.3.1** del proceso de **"Gestión de la Capacidad"** de **ITIL V3:2011** propone realizar una "**Monitorización de los recursos de la infraestructura TI"**, consiste en asignar recursos adecuados de hardware, software y personal a cada servicio y aplicación lo cual [17]:

- ***Proceso de Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

No cumple en la comparación con la práctica DSS01.01 "Realizar procedimientos operacionales", esto se debe a que las actividades de esta práctica son orientadas a mantener y llevar a cabo procedimientos operativos y las tareas operativas de una forma fiable y consistente, por lo que su propósito no se acerca a ninguna de las actividades de del proceso de la **Gestión de la Capacidad** perteneciente a **ITIL V3:2011.**

→ VS DSS01.03 Supervisar la infraestructura de TI.

No cumple en la comparación con la práctica DSS01.03 "Supervisar la infraestructura de TI.", en algunas de sus actividades. Esto se debe a que la actividad **(1, 3, 4, 5, 6)** (Ver cuadro 9 y 10) no se relaciona con el contexto de la actividad **2.3.1 "Monitorización de los recursos de la infraestructura TI"**, por tener otro objetivo a desarrollar como, mantener un registro de los eventos relacionados con la operaciones y almacenarlos de forma cronológica y tomar como referencia dichos eventos para investigaciones futuras.

Pero también se considera ciertas coincidencias en las siguientes actividades de la práctica DSS01.03 de COBIT 5 las cuales tienen cierta relación con la actividad 2.3.2 de ITIL V3:2011, puesto que se considera en parte a la actividad **(2)** porque se refiere a asignar recursos adecuados para cada servicio y aplicación.

La comparación de la actividad 2.3.1 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

→ VS DSS01.04 Gestionar el medio ambiente.

→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

→ VS DSS05.03 Administrar la seguridad del punto final.

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de Capacidad** perteneciente a **ITIL V3:2011.**

2.3.2 Supervisión de la capacidad VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.3.2** del proceso de **"Gestión de la Capacidad"** de **ITIL V3:2011** propone realizar la "**Supervisión de la capacidad"**, consiste en un proceso continuo iterativo que monitoriza, analiza y evalúa el rendimiento y capacidad de la infraestructura lo cual [17]:

- ***Proceso de Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

No cumple en la comparación con la práctica DSS01.02 "Gestionar los servicios de TI externalizados", en algunas de sus actividades. Esto se debe a que estas actividades **(1, 4)** (Ver cuadro 9 y 10) no se relacionan con el contexto de la actividad **2.3.2 "Supervisión de la capacidad"**, por tener otro objetivo a desarrollar como lo es mantener monitorizado el rendimiento de la infraestructura informática, analizar, evaluar su rendimiento y la adopción de cambios por medio de acciones correctivas; además de verificar que la infraestructura sea la adecuada con los requisitos de los ANS.

Pero también se considera ciertas coincidencias en las siguientes actividades de la práctica DSS01.02 de COBIT 5, las cuales tienen cierta relación con la actividad 2.3.2 de ITIL V3:2011, puesto que se considera que cumple las actividades **(2, 3)** (Ver cuadro 9 y 10) porque se refieren a asegurar que los requisitos de las ANS se cumplan, se dé seguimiento al rendimiento, y al manejo de la gestión de cambios de los servicios.

La comparación de la actividad 2.3.2 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.
→ VS DSS01.03 Supervisar la infraestructura de TI.
→ VS DSS01.04 Gestionar el medio ambiente.
→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.
→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

→ VS DSS05.03 Administrar la seguridad del punto final.

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de la Capacidad** perteneciente a **ITIL V3:2011.**

2.4 Gestión de la Disponibilidad

2.4.1 Determinar cuáles son los requisitos de disponibilidad reales del negocio VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.4.1** del proceso de **"Gestión de la Disponibilidad"** de **ITIL V3:2011** propone **"Determinar cuáles son los requisitos de disponibilidad reales del negocio"**, que consiste cuantificar los requisitos de la disponibilidad para la correcta elaboración de los ANS manteniendo el balance entre las necesidades reales del negocio y la posibilidad económica de la organización, para evitar altos niveles de disponibilidad que generen gastos injustificados; por lo cual [17]:

- ***Proceso de Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

No cumple en la comparación con la práctica DSS01.02 "Gestionar los servicios de TI externalizados", en algunas de sus actividades. Esto se debe a que estas actividades **(1, 3, 4)** (Ver cuadro 9 y 10) no se relacionan con la con el contexto de la actividad **2.4.1 "Determinar cuáles son los requisitos de disponibilidad reales del negocio"**, por tener otro objetivo a desarrollar como lo es asegurar el cumplimiento de los requisitos establecidos en los contratos acuerdos de niveles de servicio y la planificación de auditorías para los entornos de los proveedores externos.

Pero también se considera ciertas coincidencias en las siguientes actividades de la práctica DSS01.02 de COBIT 5 las cuales tienen cierta relación con la actividad 2.4.1 de ITIL V3:2011, puesto que se considera en parte a la actividad **(2)** porque se refieren a asegurar que se cumplan los requisitos de para la prestación de servicios.

La comparación de la actividad 2.4.1 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

→ VS DSS01.03 Supervisar la infraestructura de TI.

→ VS DSS01.04 Gestionar el medio ambiente.

→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

→ VS DSS05.03 Administrar la seguridad del punto final.

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de la Disponibilidad** perteneciente a **ITIL V3:2011.**

2.4.2 Desarrollar un plan de disponibilidad donde se estime el futuro a corto y medio plazo VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.4.2** del proceso de **"Gestión de la Disponibilidad"** de **ITIL V3:2011** propone **"Desarrollar un plan de disponibilidad donde se estime el futuro a corto y medio plazo"**, que consiste en establecer los niveles de disponibilidad adecuados según la necesidades reales de la empresa y determinar los intervalos de interrupción de los servicios dependiendo de su impacto, por lo cual se considera que [17]:

- ***Proceso de Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

No cumple en la comparación con las actividades de la práctica DSS01.02 "Gestionar los servicios de TI externalizados", pero si cumple con el contexto de la práctica (Ver cuadro 9 y 10).

La comparación de la actividad 2.4.2 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

→ VS DSS01.03 Supervisar la infraestructura de TI.

→ VS DSS01.04 Gestionar el medio ambiente.

→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

→ VS DSS05.03 Administrar la seguridad del punto final.

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **"Gestión de la Disponibilidad"** perteneciente a **ITIL V3:2011.**

2.4.3 Mantenimiento del servicio en operación y recuperación del mismo en caso de fallo VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.4.3** del proceso de **"Gestión de la Disponibilidad"** de **ITIL V3:2011** propone realizar el **"Mantenimiento del servicio en operación y recuperación del mismo en caso de fallo"**, que consiste en recuperar el servicio en el menor tiempo posible en el caso de interrupciones del servicio por incidencias o por tareas planificadas de mantenimiento, tomando en cuenta temas de seguridad para quien y cuando estarán disponibles los servicios; por lo cual [17]:

- ***Proceso de Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

No cumple en la comparación con las actividades de la práctica DSS01.01 "Realizar procedimientos operacionales", pero si cumple con el contexto de la práctica (Ver cuadro 9 y 10).

La comparación de la actividad 2.4.3 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***
  - → VS DSS01.02 Gestionar los servicios de TI externalizados.
  - → VS DSS01.03 Supervisar la infraestructura de TI.
  - → VS DSS01.04 Gestionar el medio ambiente.
  - → VS DSS01.05 Manejo de las instalaciones.
- ***Gestión de Servicios de Seguridad***
  - → VS DSS05.01 Proteger contra el malware.
  - → VS DSS05.02Gestión de la red y la seguridad de la conexión.
  - → VS DSS05.03 Administrar la seguridad del punto final.
  - → VS DSS05.05 Administrar el acceso físico a los activos de TI.
  - → VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.
  - → VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de Niveles de Servicio** perteneciente a **ITIL V3:2011.**

2.5 Gestión de la Continuidad de los servicios TI

2.5.1 Establecer las políticas y alcance de la ITSCM VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.5.1** del proceso de **"Gestión de la Continuidad de los servicios TI"** de **ITIL V3:2011** propone **"Establecer las políticas y alcance de la ITSCM."**, que consiste en establecer claramente sus objetivos generales, su alcance y el compromiso de la organización TI; no entra en el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5, esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas se refiere a establecer las políticas y alcance de la Gestión de la continuidad de servicios TI (ITSCM).

2.5.2 Evaluar el impacto en el negocio de una interrupción de los servicios TI VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.5.2** del proceso de **"Gestión de la Continuidad de los servicios TI"** de **ITIL V3:2011** propone **"Evaluar el impacto en el negocio de una interrupción de los servicios TI."**, que consiste en determinar el impacto que una interrupción de los servicios TI pueden tener en el negocio y determinar qué servicios requieren mayor atención de las actividades de prevención; no entra en el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5, esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas se refiere a evaluar el impacto en el negocio de una interrupción de los servicios TI.

2.5.3 Analizar y prever los riesgos a los que está expuesto la infraestructura TI VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.5.3** del proceso de **"Gestión de la Continuidad de los servicios TI"** de **ITIL V3:2011** propone **"Analizar y prever los riesgos a los que está expuesto la infraestructura TI"**, que consiste en conocer a profundidad la infraestructura TI, detectar puntos débiles, analizar amenazas y estimar su probabilidad; no entra en el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5, esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas se refiere a analizar y prever los riesgos a los que está expuesto la infraestructura TI.

2.5.4 Establecer las estrategias de continuidad del servicio TI VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.5.4** del proceso de **"Gestión de la Continuidad de los servicios TI"** de **ITIL V3:2011** propone **"Establecer las estrategias de continuidad del servicio TI"**, que consiste en buscar medidas preventivas, que eviten la interrupción de los niveles aceptables de servicio en el menor tiempo posible; no entra en el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5, esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas se refiere a establecer las estrategias de continuidad del servicio TI.

2.5.5 Desarrollar los planes de contingencia VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.5.5** del proceso de **"Gestión de la Continuidad de los servicios TI"** de **ITIL V3:2011** propone **"Desarrollar los planes de contingencia"**, que consiste en analizar los riesgos y vulnerabilidades, definir estrategias de prevención y recuperación siendo necesario asignar y organizar los recursos necesarios en base al alcance de la Gestión de la continuidad de servicios TI; no entra en el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5, esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas se refiere a desarrollar los planes de contingencia.

2.5.6 Poner a prueba dichos planes VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.5.6** del proceso de **"Gestión de la Continuidad de los servicios TI"** de **ITIL V3:2011** propone **"Poner a prueba dichos planes"**, que consiste en conocer a profundidad la infraestructura TI, detectar puntos débiles, analizar amenazas y estimar su probabilidad; por lo cual [17]:

- ***Proceso de Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

No cumple en la comparación con la práctica DSS01.02 "Gestionar los servicios de TI externalizados", en algunas de sus actividades. Esto se debe a que estas actividades **(1, 2, 4)** no se relacionan con el contexto de la actividad **2.5.6 "Poner a prueba dichos planes"**, por tener otro objetivo a desarrollar, como lo es asegurar el cumplimiento de los requisitos establecidos en los contratos y acuerdos de niveles de servicio y el seguimiento de los proveedores con la ayuda de planes de auditoria.

Pero también se considera ciertas coincidencias en las siguientes actividades de la práctica DSS01.02 de COBIT 5, las cuales tienen cierta relación con la actividad **2.5.6** de ITIL V3:2011, puesto se considera que cumple la actividad **(3)** porque se refiere a la continuidad del negocio y a integrar procesos críticos de gestión entre la empresa y el proveedor de servicios.

La comparación de la actividad 2.5.6 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

→ VS DSS01.03 Supervisar la infraestructura de TI.

→ VS DSS01.04 Gestionar el medio ambiente.

→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

→ VS DSS05.03 Administrar la seguridad del punto final.

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de la Continuidad de los Servicios** perteneciente a **ITIL V3:2011.**

2.5.7 Revisar periódicamente los planes para adaptarlos a las necesidades reales del negocio VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.5.7** del proceso de **"Gestión de la Continuidad de los servicios TI"** de **ITIL V3:2011** propone **"Revisar periódicamente los planes para adaptarlos a las necesidades reales del negocio"**, que consiste en actualizar periódicamente los planes para verificar que responden a los requerimientos de la empresa de forma integral; por lo cual [17]:

- ***Proceso de Gestión de Operaciones***

→ VS DSS01.04 Gestionar el medio ambiente.

No cumple en la comparación con la práctica DSS01.04 "Gestionar el medio ambiente", en algunas de sus actividades. Esto se debe a que estas actividades **(1, 2, 3, 4, 5, 7, 8)** (Ver cuadro 9 y 10) no se relacionan con el contexto de la actividad **2.5.7 "Revisar periódicamente los planes para adaptarlos a las necesidades reales del negocio"**, por tener otro objetivo a desarrollar, como lo es identificar desastres naturales y

artificiales, proteger contra amenazas ambientales a los equipos informáticos, construcción de ambientes seguros y limpios para las TI.

Pero también se considera ciertas coincidencias en las siguientes actividades de la práctica DSS01.04 de COBIT 5, las cuales tienen cierta relación con la actividad 2.5.7 de ITIL V3:2011, puesto que se considera que la actividad **(6)** cumple porque se refiere a un análisis comparativo de las medidas y planes de contingencia.

La comparación de la actividad 2.5.7 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***
  - → VS DSS01.01 Realizar procedimientos operacionales.
  - → VS DSS01.02 Gestionar los servicios de TI externalizados.
  - → VS DSS01.03 Supervisar la infraestructura de TI.
  - → VS DSS01.05 Manejo de las instalaciones.
- ***Gestión de Servicios de Seguridad***
  - → VS DSS05.01 Proteger contra el malware.
  - → VS DSS05.02Gestión de la red y la seguridad de la conexión.
  - → VS DSS05.03 Administrar la seguridad del punto final.
  - → VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
  - → VS DSS05.05 Administrar el acceso físico a los activos de TI.
  - → VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.
  - → VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de la Continuidad de los Servicios** perteneciente a **ITIL V3:2011.**

2.6 Gestión de la Seguridad de la Información

2.6.1 Constituya política de seguridad que oriente a la empresa VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.6.1** del proceso de **"Gestión de la Seguridad de la Información"** de **ITIL V3:2011** propone que se **"Constituya política de seguridad que oriente a la empresa"**, que consiste en establecer una política global y clara sobre la seguridad, en donde se fijen aspectos tales como los

objetivos, responsabilidades y recursos; no entra en el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5, esto se debe a que en el contenido general de estos procesos, en ninguna de sus prácticas se refiere a establecer las políticas de seguridad.

2.6.2 Realizar un Plan de Seguridad que integre los límites de seguridad adecuados descritos en los acuerdos de servicio firmados con proveedores internos y externo VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.6.2** del proceso de **"Gestión de la Seguridad de la Información"** de **ITIL V3:2011** propone que se **"Realizar un Plan de Seguridad que integre los límites de seguridad adecuados descritos en los acuerdos de servicio firmados con proveedores internos y externo "**, que consiste en fijar los niveles de seguridad que han de ser incluidos como parte de los ANS, OLAs y UCs, incluyendo métricas o indicadores para evaluar los niveles de seguridad; no entra en el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5, esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas se refiere a elaborar un plan de seguridad.

2.6.3 Supervisión proactiva de los límites de seguridad analizando tendencias, nuevos riesgos y vulnerabilidades. VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.6.3** del proceso de **"Gestión de la Seguridad de la Información"** de **ITIL V3:2011** propone que se **"Supervisión proactiva de los límites de seguridad analizando tendencias, nuevos riesgos y vulnerabilidades"**, que consiste en mantener al día el Plan de Seguridad y las secciones de seguridad de los ANS respecto a nuevos riesgos y vulnerabilidades, frente a software malicioso, denegación del servicio, adoptando medidas para la actualización de recursos, incluyendo la formación del personal; por lo cual [17]:

- ***Proceso de Gestión de Operaciones***
  - → VS DSS01.02 Gestionar los servicios de TI externalizados.

No cumple en la comparación con la práctica DSS01.02 "Gestionar los servicios de TI externalizados", en algunas de sus actividades. Esto se debe a que estas actividades **(2, 3, 4)** (Ver cuadro 9 y 10) no se relacionan con el contexto de la actividad **2.6.3 "Supervisión proactiva de los límites de seguridad analizando tendencias, nuevos riesgos y vulnerabilidades"**, por tener otro objetivo a desarrollar, como lo es asegurar

un negocio operativo en base a las prioridades de prestación de servicios, integración de los procesos de gestión críticos con los de los proveedores de servicios y auditoria del entorno operativo de los proveedores.

Pero también se considera ciertas coincidencias en las siguientes actividades de la práctica DSS01.02 de COBIT 5, las cuales tienen cierta relación con la actividad 2.6.3 de ITIL V3:2011, puesto que se considera en parte a la actividad **(1)** porque se refiere a asegurar el cumplimiento de los requisitos de seguridad estipulados en los ANS.

- ***Proceso de Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

No cumple en la comparación con la práctica DSS01.05 “Proteger contra el malware”, en algunas de sus actividades. Esto se debe a que estas actividades **(2, 3, 5)** no se relacionan con el contexto de la actividad **2.6.5 “Supervisión proactiva de los límites de seguridad analizando tendencias, nuevos riesgos y vulnerabilidades”**, por tener otro objetivo a desarrollar, como lo es asegurar un negocio operativo en base a las prioridades de prestación de servicios, integración de los procesos de gestión críticos con los de los proveedores de servicios y auditoria del entorno operativo de los proveedores.

Pero también se considera ciertas coincidencias en las siguientes actividades de la práctica DSS05.01 de COBIT 5, las cuales tienen cierta relación con la actividad 2.6.3 de ITIL V3:2011, puesto que se considera en parte a las actividades **(1, 4, 6)** porque se refiere a la prevención concienciación y formación del personal sobre software malicioso, y la actualización sobre nuevas amenazas.

La comparación de la actividad 2.6.3 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

→ VS DSS01.03 Supervisar la infraestructura de TI.

→ VS DSS01.04 Gestionar el medio ambiente.

→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

→ VS DSS05.03 Administrar la seguridad del punto final.

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de la Seguridad de la Información** perteneciente a **ITIL V3:2011.**

2.7 Gestión de Proveedores

2.7.1 Los requisitos de contratación que se van a exigir a los proveedores VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.7.1** del proceso de **"Gestión de los Proveedores"** de **ITIL V3:2011** propone realizar **"Los requisitos de contratación que se van a exigir a los proveedores"**, que consiste analizar las estrategias generales de la organización y los servicios que presta, para definir sus necesidades de contratación; por lo cual se considera que [17]:

- ***Proceso de Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

No cumple en la comparación con las actividades de la práctica DSS01.02 "Gestionar los servicios de TI externalizados", pero si cumple con el contexto de la práctica (Ver cuadro 9 y 10).

La comparación de la actividad 2.7.1 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

→ VS DSS01.03 Supervisar la infraestructura de TI.

→ VS DSS01.04 Gestionar el medio ambiente.

→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

→ VS DSS05.03 Administrar la seguridad del punto final.

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de los Proveedores** perteneciente a **ITIL V3:2011.**

2.7.2 Los procesos de evaluación y selección de proveedores VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.7.2** del proceso de **"Gestión de Proveedores"** de **ITIL V3:2011** propone realizar **"Los procesos de evaluación y selección de proveedores"**, que consiste en elegir un proveedor acorde con los requisitos de la empresa, tomando en cuenta sus referencias, capacidad, disponibilidad y el financiamiento del cual dispone la empresa; no entra en el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5, esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas se refiere a la evaluación y selección de proveedores.

2.7.3 La clasificación y documentación de la relación con los proveedores VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.7.3** del proceso de **"Gestión de Proveedores"** de **ITIL V3:2011** propone realizar **"La clasificación y documentación de la relación con los proveedores"**, que consiste en crear una base de datos que reúna información de los proveedores, contratos, nivel de atención y su relación con otros procesos de gestión; no entra en el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5, esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas se refiere a la clasificación y documentación de la relación con los proveedores.

2.7.4 Gestión del Rendimiento de los proveedores VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.7.4** del proceso de **"Gestión de Proveedores"** de **ITIL V3:2011** propone realizar **"Gestión del Rendimiento de los proveedores"**, que consiste verificar que se estén cumpliendo los niveles de calidad y disponibilidad acordados en los contratos; por lo cual [17]:

- ***Proceso de Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

No cumple en la comparación con la práctica DSS01.02 “Gestionar los servicios de TI externalizados”, en algunas de sus actividades. Esto se debe a que estas actividades **(1, 2, 4)** no se relacionan con el contexto de la actividad **2.7.4** (Ver cuadro 9 y 10) **“Gestión del Rendimiento de los proveedores”,** por tener otro objetivo a desarrollar, como lo es asegurar un negocio operativo en base a las prioridades de prestación de servicios, integración de los procesos de gestión críticos con los de los proveedores de servicios y auditoria del entorno operativo de los proveedores.

Pero también se considera ciertas coincidencias en las siguientes actividades de la práctica DSS01.02 de COBIT 5, las cuales tienen cierta relación con la actividad **2.7.4** de ITIL V3:2011, puesto que se considera que cumple la actividad **(3)** porque se refiere al seguimiento del proceso del rendimiento.

La comparación de la actividad 2.7.4 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.
→ VS DSS01.03 Supervisar la infraestructura de TI.
→ VS DSS01.04 Gestionar el medio ambiente.
→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.
→ VS DSS05.02Gestión de la red y la seguridad de la conexión.
→ VS DSS05.03 Administrar la seguridad del punto final.
→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
→ VS DSS05.05 Administrar el acceso físico a los activos de TI.
→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.
→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de los Proveedores** perteneciente a **ITIL V3:2011.**

2.7.5 Renovación o terminación VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **2.7.5** del proceso de **"Gestión de Proveedores"** de **ITIL V3:2011** propone realizar **"Renovación o terminación"**, que consiste en asesorar a los directivos sobre la renovación o terminación de contratos de los proveedores, considerando su rendimiento, perspectivas de crecimiento de la empresa y cumplimiento de contrato; no entra en el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5, esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas se refiere a la renovación o terminación de servicios.

3. Fase de Transición

3.1 Planificación y soporte a la Transición

3.1.1 Estrategia de transición VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **3.1.1** del proceso de **"Planificación y soporte a la Transición"** de **ITIL V3:2011** propone realizar una **"Estrategia de transición"**, que consiste en establecer propósitos, metas, objetivos, responsabilidades, marcos de trabajo, planificación de entregables, criterios de evaluación y aceptación de cambios de los servicios, sea este nuevo o a modificar, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas propone establecer una estrategia de transición de servicios.

3.1.2 Preparación de transición VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **3.1.2** del proceso de **"Planificación y soporte a la Transición"** de **ITIL V3:2011** propone realizar una **"Preparación de transición"**, que consiste en la revisión de los recursos TI que intervendrán en la ejecución de cambios en los servicios, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas propone la preparación de la transición de servicios.

3.1.3 Planificación de la transición VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **3.1.3** del proceso de **"Planificación y soporte a la Transición"** de **ITIL V3:2011** propone realizar una **"Planificación de la transición"**, que consiste en una serie de pruebas y evaluaciones con respecto a elementos de configuración, descripción de tareas, asignación de recursos y especificación de plazo para cada una, referentes al cambio o implementación de un servicio, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas propone establecer una planificación de la transición de servicios.

3.2 Gestión de Cambios

3.2.1 Registro de peticiones VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **3.2.1** del proceso de **"Gestión de Cambios"** de **ITIL V3:2011** propone realizar un **"Registro de peticiones"**, que consiste en registrar las peticiones detallando su propósito, sea esta el desarrollo de nuevos servicios, cambio estratégico empresarial, actualizaciones de hardware a terceros o peticiones de los clientes para mejorar los servicios; el registro requiere de constante actualización sobre el estado de la petición, fecha de recepción, fecha de aceptación, prioridad, recursos asignados y fecha de cierre, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5.

3.2.2 Aceptación y Clasificación del cambio VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **3.2.2** del proceso de **"Gestión de Cambios "** de **ITIL V3:2011** propone realizar la **"Aceptación y Clasificación del cambio"**, que consiste en la aceptación o rechazo de las peticiones de cambio dependiendo de su justificación; en el caso de su aceptación se le asigna una prioridad y categoría que permita establecer un calendario de cambios según dicha prioridad y determinar su impacto en la empresa de acuerdo a la categoría, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5.

3.2.3 Aprobación y Planificación del cambio VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **3.2.3** del proceso de **"Gestión de Cambios"** de **ITIL V3:2011** propone realizar la **"Aprobación y Planificación del cambio"**, que consiste aprobar los cambios de acuerdo a los beneficios, justificación de costes, riesgos asociados, impacto en la infraestructura, calidad de los servicios TI mientras se planifican recursos y tiempo, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5.

3.2.4 Implementación del cambio VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **3.2.4** del proceso de **"Gestión de Cambios"** de **ITIL V3:2011** propone realizar la **"Implementación del cambio"**, que consiste supervisar y coordinar el proceso de cambio, asegurando los recursos se ajustan a las especificaciones y cumplimiento de calendario, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5.

3.2.5 Evaluación del cambio VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **3.2.5** del proceso de **"Gestión de Cambios"** de **ITIL V3:2011** propone realizar una **"Evaluación del cambio"**, que consiste analizar si los cambios cumplen con los objetivos previstos y verificar que ellos no afecten la calidad de los servicios, para luego proceder al cierre del cambio, requiriendo de protocolos de validación para proceder a la implementación del cambio, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5..

3.2.6 Cambios de emergencia VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **3.2.6** del proceso de **"Gestión de Cambios"** de **ITIL V3:2011** propone realizar **"Cambios de emergencia"**, que consiste en restaurar el servicio luego de una planificación deficiente en el caso de la interrupción de un servicio de alto impacto, requiriendo de protocolos de validación para proceder a la implementación del cambio, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5.

3.3 Gestión de la Configuración y Activos del Servicio

3.3.1 Planificación de la Configuración VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **3.1.1** del proceso de **"Gestión de la Configuración y Activos del Servicio"** de **ITIL V3:2011** propone realizar la **"Planificación de la Configuración"**, que consiste en establecer propósitos, metas, objetivos, responsabilidades, marcos de trabajo, planificación de entregables, criterios de evaluación y aceptación de cambios de los servicios, sea este nuevo o a modificar, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas propone establecer una estrategia de transición de servicios.

3.3.2 Clasificación y registro de los Elementos de Configuración VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **3.3.2** del proceso de **"Gestión de la Configuración y Activos del Servicio"** de **ITIL V3:2011** propone realizar **"Clasificación y registro de los Elementos de Configuración"**, que consiste en registrar en una Base de datos de configuraciones los sistemas de hardware y software que se consideren críticos, elementos de configuración y el estado de su ciclo de vida, detallando sus atributos, tipo de relaciones lógicas, físicas, profundidad (subcomponentes) y su nomenclatura para identificarlos y clasificarlos; por lo cual [17]:

- ***Proceso de Gestión de Operaciones***

→ VS DSS01.03 Supervisar la infraestructura de TI.

No cumple en la comparación con la práctica DSS01.03 "Supervisar la infraestructura de TI.", en algunas de sus actividades. Esto se debe a que la actividad **(1, 3, 4, 5, 6)** (Ver cuadro 9 y 10) no se relaciona con el contexto de la actividad 3**.3.2 "Clasificación y registro de los Elementos de Configuración"**, por tener otro objetivo a desarrollar como, mantener un registro de los eventos relacionados con la operaciones y almacenarlos de forma cronológica y tomar como referencia dichos eventos para investigaciones futuras.

Pero también se considera ciertas coincidencias en las siguientes actividades de la práctica DSS01.03 de COBIT 5 las cuales tienen cierta relación con la actividad 3.3.2

de ITIL V3:2011, puesto que se considera en parte a la actividad **(2)** (Ver cuadro 9 y 10) porque se refiere a mantener un listado de los activos de la infraestructura.

La comparación de la actividad 3.3.2 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***
  - → VS DSS01.01 Realizar procedimientos operacionales.
  - → VS DSS01.02 Gestionar los servicios de TI externalizados.
  - → VS DSS01.04 Gestionar el medio ambiente.
  - → VS DSS01.05 Manejo de las instalaciones.
- ***Gestión de Servicios de Seguridad***
  - → VS DSS05.01 Proteger contra el malware.
  - → VS DSS05.02Gestión de la red y la seguridad de la conexión.
  - → VS DSS05.03 Administrar la seguridad del punto final.
  - → VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
  - → VS DSS05.05 Administrar el acceso físico a los activos de TI.
  - → VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.
  - → VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de la Configuración y Activos del Servicio** perteneciente a **ITIL V3:2011.**

3.3.3 Monitorización y Control de los Elementos de Configuración VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **3.3.3** del proceso de **"Gestión de la Configuración y Activos del Servicio"** de **ITIL V3:2011** propone realizar la **"Monitorización y Control de los Elementos de Configuración"**, que consiste en asegurar que todos los elementos de configuración se encuentren registrados y conocer su estado actual, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5.

3.3.4 Realización de auditorías VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **3.3.4** del proceso de **"Gestión de la Configuración y Activos del Servicio"** de **ITIL V3:2011** propone la **"Realización de auditorías"**, que consiste en asegurar que la información registrada con la Base de datos de configuración coincide con la configuración real de la estructura TI de la empresa, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5.

3.4 Gestión de entrega y despliegues VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A el proceso **3.4 "Gestión de entrega y despliegues"** de **ITIL V3:2011** se encarga de desarrollar, probar e implementar nuevas versiones de software o hardware, conforme con los niveles de calidad y servicios estipulados por el cliente. Las actividades que conforman este proceso son las siguientes:

3.4.1 Planificación de entregas
3.4.2 Desarrollo del despliegue
3.4.3 Implementación de la entrega
3.4.4 Comunicación y formación al cliente

Se determina que no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5**"**; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas propone establecer actividades para la entrega y despliegue de servicios TI.

3.5 Validación y pruebas VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A el proceso **3.5 "Validación y pruebas"** de **ITIL V3:2011** se encarga validar mediante pruebas las nuevas versiones de software o hardware, verificando el cumplimiento de los niveles de calidad establecidos con el cliente con el propósito de evitar errores cuando estén operativas. Las actividades que conforman este proceso son las siguientes:

3.5.1 Validación, planificación y verificación de tests
3.5.2 Construcción de tests
3.5.3 Pruebas de Validación

3.5.4 Aceptación y reporte

3.5.5 Limpieza y cierre

Se determina que no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5**"**; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas propone establecer actividades para la validación y pruebas de servicios TI.

3.6 Evaluación VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A el proceso **3.6 "Evaluación"** de **ITIL V3:2011** se encarga de evaluar el rendimiento de un elemento específico del servicio, mediante el análisis de la información del nuevo o cambio de servicios TI y elaborar los informes necesarios al respecto. Las actividades que conforman este proceso son las siguientes:

3.6.1 Planificación de la evaluación.

3.6.2 Evaluación del rendimiento previsto.

3.6.3 Evaluación del rendimiento real.

Se determina que no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5**"**; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas propone establecer actividades para la evaluación de servicios TI.

3.7 Gestión del Conocimiento

3.7.1 Puntualizar una estrategia de Gestión del Conocimiento y divulgarla a toda la empresa VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **3.7.1** del proceso de **"Gestión del Conocimiento"** de **ITIL V3:2011** propone **"Puntualizar una estrategia de Gestión del Conocimiento y divulgarla a toda la empresa"**, que consiste en definir, desarrollar y difundir una estrategia de conocimiento en la que se reflejen las condiciones de administración, roles, procedimientos de registro y validación de información, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas propone establecer una estrategia de transición de servicios.

3.7.2 Mejora la transmisión de conocimiento entre personas, equipos y departamentos VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **3.7.2** del proceso de **"Gestión del Conocimiento"** de **ITIL V3:2011** propone **"Mejora la transmisión de conocimiento entre personas, equipos y departamentos"**, que consiste en transferir los conocimientos entre los miembros de la empresa, inculcando el registro de la información con el propósito de mejorar la cultura de aprendizaje del personal y mejorar el conocimiento de la posesión y propietarios de la información, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas propone transferir conocimientos entre los miembros de la empresa.

3.7.3 Gestionar la información para certificar su calidad y utilidad VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **3.7.3** del proceso de **"Gestión del Conocimiento"** de **ITIL V3:2011** propone realizar **"Gestionar la información para certificar su calidad y utilidad"**, que consiste en verificar que la información se mantenga disponible, completa y actualizada; por lo cual [17]:

- ***Proceso de Gestión de Operaciones***
  - → VS DSS01.01 Realizar procedimientos operacionales.

No cumple en la comparación con la práctica DSS01.01 "Realizar procedimientos operacionales", en algunas de sus actividades:

Esto se debe a que estas actividades **(1, 2, 4, 5)** (Ver cuadro 9 y 10) no se relacionan con el contexto de la actividad **3.7.3 "Gestionar la información para certificar su calidad y utilidad"**, por tener otro objetivo a desarrollar, como lo es garantizar que se cumplan las normas de seguridad adecuadas y la planificación y registro de copias de seguridad.

Pero también se considera ciertas coincidencias en las siguientes actividades de la práctica DSS01.01 de COBIT 5, las cuales tienen cierta relación con la actividad 3.7.3 de ITIL V3:2011, puesto que se considera que cumple la actividad **(3)** porque se refiere a garantizar que los datos se entreguen de forma oportuna y completa.

La comparación de la actividad 3.7.3 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***
  - → VS DSS01.02 Gestionar los servicios de TI externalizados.
  - → VS DSS01.03 Supervisar la infraestructura de TI.
  - → VS DSS01.04 Gestionar el medio ambiente.
  - → VS DSS01.05 Manejo de las instalaciones.
- ***Gestión de Servicios de Seguridad***
  - → VS DSS05.01 Proteger contra el malware.
  - → VS DSS05.02Gestión de la red y la seguridad de la conexión.
  - → VS DSS05.03 Administrar la seguridad del punto final.
  - → VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
  - → VS DSS05.05 Administrar el acceso físico a los activos de TI.
  - → VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.
  - → VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión del Conocimiento** perteneciente a **ITIL V3:2011.**

3.7.4 Uso del Sistema de Gestión del Conocimiento del Servicio (SKMS) VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **3.7.4** del proceso de **"Gestión del Conocimiento"** de **ITIL V3:2011** propone **"Uso del Sistema de Gestión del Conocimiento del Servicio (SKMS)"**, que consiste en un repositorio de todos los documentos generados por los demás procesos, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas propone el uso de un Sistema de Gestión del Conocimiento del Servicio.

4 Fase de Operación

4.1 Gestión de Eventos

4.1.1 Notificación de eventos VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **4.1.1** del proceso de **"Gestión de Eventos"** de **ITIL V3:2011** propone la **"Notificación de eventos"**, que consiste en aplicar herramientas que ayuden a notificar al equipo o responsable de gestión la aparición de un evento, lo cual [17]:

- ***Proceso de Gestión de Servicios de Seguridad***

→ VS DSS05.07 Supervisar la infraestructura para eventos relacionados con la seguridad

No cumple en la comparación con la práctica DSS05.07 "Supervisar la infraestructura para eventos relacionados con la seguridad", en algunas de sus actividades. Esto se debe a que estas actividades **(2, 3, 4, 5)** (Ver cuadro 9 y 10) no se relacionan con la con el contexto de la actividad **4.1.1 "Notificación de eventos"**, por tener otro objetivo a desarrollar como lo es definir y comunicar la incidencias de seguridad y revisión de eventos para las incidencias potenciales.

Pero también se considera ciertas coincidencias en una actividad de la práctica DSS05.07 de COBIT 5 las cuales tienen cierta relación con la actividad 4.1.1 de ITIL V3:2011, puesto que se considera que la actividad **(1)** (Ver cuadro 9 y 10) cumple porque se refiere al uso de herramientas de supervisión.

La comparación de la actividad 4.1.1 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.
→ VS DSS01.02 Gestionar los servicios de TI externalizados.
→ VS DSS01.03 Supervisar la infraestructura de TI.
→ VS DSS01.04 Gestionar el medio ambiente.
→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.
→ VS DSS05.02Gestión de la red y la seguridad de la conexión.
→ VS DSS05.03 Administrar la seguridad del punto final.
→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
→ VS DSS05.05 Administrar el acceso físico a los activos de TI.
→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de Eventos** perteneciente a **ITIL V3:2011.**

4.1.2 Detección y filtrado de eventos VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **4.1.2** del proceso de **"Gestión de Eventos"** de **ITIL V3:2011** propone la **"Detección y filtrado de eventos"**, que consiste en la interpretación del suceso para determinar su profundidad y a quién requiere ser notificado, con el fin de prestarle mayor atención, lo cual [17]:

- ***Proceso de Gestión de Operaciones***

  → VS DSS01.03 Supervisar la infraestructura de TI.

No cumple en la comparación con la práctica DSS01.03 "Supervisar la infraestructura de TI.", en algunas de sus actividades. Esto se debe a que estas actividades **(2, 3, 4, 5, 6)** (Ver cuadro 9 y 10) no se relacionan con la con el contexto de la actividad **"Detección y filtrado de eventos"**, por tener otro objetivo a desarrollar como lo es definir reglar, infracciones y condiciones de los eventos, registrar los eventos en logs, revisiones y asegurar que la entradas de las incidencias son creadas de forma oportuna.

Pero también se considera ciertas coincidencias en una actividad de la práctica DSS01.03 de COBIT 5 las cuales tienen cierta relación con la actividad 4.1.2 de ITIL V3:2011, puesto que se considera que la actividad **(1)** (Ver cuadro 9 y 10) cumple porque se refiere al registro de eventos considerando su riesgo y rendimiento.

La comparación de la actividad 4.1.2 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

→ VS DSS01.04 Gestionar el medio ambiente.

→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

→ VS DSS05.03 Administrar la seguridad del punto final.

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de Eventos** perteneciente a **ITIL V3:2011.**

4.1.3 Clasificación de eventos VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **4.1.3** del proceso de **"Gestión de Eventos"** de **ITIL V3:2011** propone la **"Clasificación de eventos"**, que consiste en una clasificación según la importancia del servicio TI y su infraestructura, lo cual [17]:

- ***Proceso de Gestión de Operaciones***

→ VS DSS01.03 Supervisar la infraestructura de TI.

No cumple en la comparación con la práctica DSS01.03 "Supervisar la infraestructura de TI", en algunas de sus actividades. Esto se debe a que estas actividades **(2, 3, 4, 5, 6)** (Ver cuadro 9 y 10) no se relacionan con la con el contexto de la actividad **"Clasificación de eventos"**, por tener otro objetivo a desarrollar como lo es definir reglar, infracciones y condiciones de los eventos, registrar los eventos en logs, revisiones y asegurar que la entradas de las incidencias son creadas de forma oportuna.

Pero también se considera ciertas coincidencias en una actividad de la práctica DSS01.03 de COBIT 5 las cuales tienen cierta relación con la actividad 4.1.3 de ITIL V3:2011, puesto que se considera que la actividad cumple **(1)** (Ver cuadro 9 y 10) porque se refiere al registro de eventos considerando su riesgo y rendimiento

La comparación de la actividad 4.1.3 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

→ VS DSS01.04 Gestionar el medio ambiente.

→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.
→ VS DSS05.03 Administrar la seguridad del punto final.
→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
→ VS DSS05.05 Administrar el acceso físico a los activos de TI.
→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.
→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de Eventos** perteneciente a **ITIL V3:2011.**

4.1.4 Correlación VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **4.1.4** del proceso de **"Gestión de Eventos"** de **ITIL V3:2011** propone la **"Correlación"**, que consiste dimensionar la importancia del evento y establecer conexiones con otros con el fin de ahorrar tiempo en la búsqueda de soluciones, lo cual [17]:

- ***Proceso de Gestión de Operaciones***

→ VS DSS01.03 Supervisar la infraestructura de TI.

No cumple en la comparación con las actividades de la práctica DSS01.03 "Supervisar la infraestructura de TI", pero si cumple con el contexto de la práctica (Ver cuadro 9 y 10).

La comparación de la actividad 4.1.4 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.
→ VS DSS01.02 Gestionar los servicios de TI externalizados.
→ VS DSS01.04 Gestionar el medio ambiente.
→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.
→ VS DSS05.02Gestión de la red y la seguridad de la conexión.
→ VS DSS05.03 Administrar la seguridad del punto final.
→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de Eventos** perteneciente a **ITIL V3:2011.**

4.1.5 Disparadores VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **4.1.5** del proceso de **"Gestión de Eventos"** de **ITIL V3:2011** propone **"Disparadores"**, que consisten en dimensionar la importancia del evento y establecer conexiones con otros con el fin de ahorrar tiempo en la búsqueda de soluciones, lo cual [17]:

- ***Proceso de Gestión de Servicios de Seguridad***

→ VS DSS05.07 Supervisar la infraestructura para eventos relacionados con la seguridad.

No cumple en la comparación con la práctica DSS05.07 "Supervisar la infraestructura para eventos relacionados con la seguridad", en algunas de sus actividades. Esto se debe a que estas actividades **(2, 3, 4, 5)** (Ver cuadro 9 y 10) no se relacionan con el contexto de la actividad **"Disparadores"**, por tener otro objetivo a desarrollar como lo es definir y comunicar las características de los incidentes de seguridad, además de vigilar los incidentes potenciales.

Pero también se considera ciertas coincidencias en una actividad de la práctica DSS01.03 de COBIT 5 las cuales tienen cierta relación con la actividad 4.1.5 de ITIL V3:2011, puesto que se considera que la actividad **(1)** (Ver cuadro 9 y 10) cumple porque se refiere al uso de herramientas de supervisión de seguridad.

La comparación de la actividad 4.1.5 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

→ VS DSS01.03 Supervisar la infraestructura de TI.

→ VS DSS01.04 Gestionar el medio ambiente.

→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

→ VS DSS05.03 Administrar la seguridad del punto final.

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de Eventos** perteneciente a **ITIL V3:2011.**

4.2 Gestión de Incidencias

4.2.1 Registro y clasificación TI VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **4.2.1** del proceso de **"Gestión de Incidencias"** de **ITIL V3:2011** propone el **"Registro y clasificación"**, que consiste en el registro oportuno de las incidencias para evitar que luego se conviertan en una solución más costosa, lo cual [17]:

- ***Proceso de Gestión de Operaciones***

→ VS DSS01.03 Supervisar la infraestructura de TI

No cumple en la comparación con la práctica DSS01.03 "Supervisar la infraestructura de TI", en algunas de sus actividades. Esto se debe a que estas actividades **(1, 2, 3, 4, 6)** (Ver cuadro 9 y 10) no se relacionan con el contexto de la actividad **"Registro y clasificación"**, por tener otro objetivo a desarrollar como lo es el registro de eventos, identificación y mantenimiento de activos y el seguimiento de eventos.

Pero también se considera ciertas coincidencias en una actividad de la práctica DSS01.03 de COBIT 5 las cuales tienen cierta relación con la actividad 4.2.1 de ITIL V3:2011, puesto que se considera que la actividad **(6)** (Ver cuadro 9 y 10) cumple porque se refiere al registro de las incidencias de forma oportuna.

- ***Proceso de Gestión de Servicios de Seguridad***

→ VS DSS05.07 Supervisar la infraestructura para eventos relacionados con la seguridad.

No cumple en la comparación con la práctica DSS05.07 “Supervisar la infraestructura para eventos relacionados con la seguridad”, en algunas de sus actividades. Esto se debe a que estas actividades **(1, 2, 3, 4)** (Ver cuadro 9 y 10) no se relacionan con el contexto de la actividad **“Registro y clasificación”**, por tener otro objetivo a desarrollar como lo es el registro de sucesos con herramientas de supervisión, definir, comunicar y vigilar incidencias.

Pero también se considera ciertas coincidencias en una actividad de la práctica DSS05.07 de COBIT 5 las cuales tienen cierta relación con la actividad 4.2.1 de ITIL V3:2011, puesto que se considera que la actividad **(5)** (Ver cuadro 9 y 10) cumple porque se refiere al registro de las incidencias de seguridad de forma oportuna.

La comparación de la actividad 4.2.1 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.
→ VS DSS01.02 Gestionar los servicios de TI externalizados.
→ VS DSS01.04 Gestionar el medio ambiente.
→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.
→ VS DSS05.02Gestión de la red y la seguridad de la conexión.
→ VS DSS05.03 Administrar la seguridad del punto final.
→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
→ VS DSS05.05 Administrar el acceso físico a los activos de TI.
→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de Incidencias** perteneciente a **ITIL V3:2011.**

4.2.2 Análisis, resolución y cierre VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **4.2.2** del proceso de **"Gestión de Incidencias"** de **ITIL V3:2011** propone el **"Análisis, resolución y cierre"**, que consiste en examinar las incidencias con el fin de encontrar alguna ya resuelta para aplicar su procedimiento asignado, además de reclasificar el incidente en caso de ser necesario, lo cual [17]:

- ***Proceso de Gestión de Operaciones***

  → VS DSS01.05 Manejo de las instalaciones.

No cumple en la comparación con la práctica DSS01.05 "Manejo de las instalaciones", en algunas de sus actividades. Esto se debe a que estas actividades **(1, 2, 3, 4, 5, 6, 7, 8, 10, 11)** (Ver cuadro 9 y 10) no se relacionan con el contexto de la actividad **"Análisis, resolución y cierre"**, por tener otro objetivo a desarrollar como lo es el registro de eventos, identificación y mantenimiento de activos y el manejo de las instalaciones TI, implementación de mecanismos, reglamentos y leyes para asegurar su funcionamiento ininterrumpido.

Pero también se considera ciertas coincidencias en una actividad de la práctica DSS01.05 de COBIT 5 las cuales tienen cierta relación con la actividad 4.2.2 de ITIL V3:2011, puesto que se considera la actividad **(9)** (Ver cuadro 9 y 10) cumple porque se refiere al registro de las incidencias de forma oportuna.

La comparación de la actividad 4.2.2 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***
  - → VS DSS01.01 Realizar procedimientos operacionales.
  - → VS DSS01.02 Gestionar los servicios de TI externalizados.
  - → VS DSS01.03 Supervisar la infraestructura de TI.
  - → VS DSS01.04 Gestionar el medio ambiente.
- ***Gestión de Servicios de Seguridad***
  - → VS DSS05.01 Proteger contra el malware.
  - → VS DSS05.02Gestión de la red y la seguridad de la conexión.
  - → VS DSS05.03 Administrar la seguridad del punto final.
  - → VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
  - → VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de Incidencias** perteneciente a **ITIL V3:2011.**

4.3 Gestión de Peticiones

4.3.1 Selección de Peticiones VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **4.3.1** del proceso de **"Gestión de Peticiones"** de **ITIL V3:2011** propone la **"Selección de Peticiones"**, que permite al cliente escoger la petición a través de una interfaz, peticiones estándar respecto a la información y acceso rápido a los servicios, estas pueden ser peticiones de cambios estándar, solicitudes de información o consejo o solicitud de servicios TI, lo cual [17]:

- ***Proceso de Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

No cumple en la comparación con la práctica DSS01.02 "Gestionar los servicios de TI externalizados", en algunas de sus actividades. Esto se debe a que estas actividades **(1, 2, 4)** no se relacionan con el contexto de la actividad **"Selección de Peticiones"**, por tener otro objetivo a desarrollar como lo es asegurar que el negocio se mantenga operativo bajo los requisitos de seguridad de la empresa y elaborar un plan de auditoria para el seguimiento del entono de los proveedores externos.

Pero también se considera ciertas coincidencias en una actividad de la práctica DSS01.02 de COBIT 5 las cuales tienen cierta relación con la actividad 4.3.1 de ITIL V3:2011, puesto que se considera que la actividad **(3) cumple** porque se refiere a integrar el proceso de solicitud del servicio.

- ***Proceso de Gestión de Servicios de Seguridad***

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

No cumple en la comparación con la práctica DSS05.05 "Administrar el acceso físico a los activos de TI", en algunas de sus actividades. Esto se debe a que estas actividades **(2, 3, 4, 5, 6, 7)** (Ver cuadro 9 y 10) no se relacionan con el contexto de la actividad **"Selección de Peticiones"**, por tener otro objetivo a desarrollar como lo es el registro de sucesos con herramientas de supervisión, definir, comunicar y vigilar incidencias.

Pero también se considera ciertas coincidencias en una actividad de la práctica DSS05.07 de COBIT 5 las cuales tienen cierta relación con la actividad 4.3.1 de ITIL V3:2011, puesto que se considera en parte a la actividad **(1)** (Ver cuadro 9 y 10) porque se refiere a la solicitud de acceso a instalaciones TI.

La comparación de la actividad 4.3.1 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***
  - → VS DSS01.01 Realizar procedimientos operacionales.
  - → VS DSS01.03 Supervisar la infraestructura de TI.
  - → VS DSS01.04 Gestionar el medio ambiente.
  - → VS DSS01.05 Manejo de las instalaciones.
- ***Gestión de Servicios de Seguridad***
  - → VS DSS05.01 Proteger contra el malware.
  - → VS DSS05.02Gestión de la red y la seguridad de la conexión.
  - → VS DSS05.03 Administrar la seguridad del punto final.
  - → VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
  - → VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.
  - → VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de Peticiones** perteneciente a **ITIL V3:2011.**

4.3.2 Aprobación financiera VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **4.3.2** del proceso de **"Gestión de Peticiones"** de **ITIL V3:2011** propone la **"Aprobación financiera"**, que considera costos para aquellas peticiones que requieran de algún gasto fuera del curso normal financiero; permitiendo decidir si se tramita la petición o no. Se pueden establecer costos fijos para peticiones estándar predefinidas, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5.

4.3.3 Tramitación y cierre VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **4.3.3** del proceso de **"Gestión de Peticiones"** de **ITIL V3:2011** propone la **"Tramitación y cierre"**, que consiste en poner en marcha la petición y comprobar la satisfacción del usuario, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas propone una actividad para la tramitación y cierre de peticiones.

4.4 Gestión de Problemas

4.4.1 Control de Problemas VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **4.4.1** del proceso de **"Gestión de Problemas"** de **ITIL V3:2011** propone la **"Control de Problemas"**, que consiste en la identificación de problemas en base a las incidencias registradas de las cuales se desconocen su causa y son cerradas mediante una solución temporal, con el propósito de convertirlos en errores conocidos. El registro de los problemas consiste en el detalle de los servicios involucrados, niveles de prioridad, urgencia, impacto y su estado (activo, error conocido, cerrado), la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5.

4.4.2 Control de Errores VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **4.4.2** del proceso de **"Gestión de Problemas"** de **ITIL V3:2011** propone la **"Control de Errores"**, que consiste en el registro de las causas encontradas a los problemas (error conocido), analizar costos, impactos en la infraestructura TI y efectos en las ANS para la investigación de las soluciones. Para el cierre de un problema se debe analizar los resultados de las soluciones, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5.

4.5 Gestión de Acceso a los Servicios TI

4.5.1 Verificación VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **4.5.1** del proceso de **"Gestión de Acceso a los Servicios TI"** de **ITIL V3:2011** propone la **"Verificación"**, que permite

definir las vías de petición de acceso ya sea esta una petición estándar del departamento de recursos humanos, una solicitud de cambio o al ejecutar una tarea automatizada planificada con anterioridad, lo cual [17]:

- ***Proceso de Gestión de Servicios de Seguridad***

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

No cumple en la comparación con la práctica DSS05.04 “Manejo de la identidad del usuario y el acceso lógico”, en las algunas de sus actividades. Esto se debe a que estas actividades **(3, 4, 5, 8)** (Ver cuadro 9 y 10) no se relacionan con el contexto de la actividad **“Verificación”**, por tener otro objetivo a desarrollar (Ver cuadro 9 y 10). Pero también se considera ciertas coincidencias en una actividad de la práctica DSS05.04 de COBIT 5 las cuales tienen cierta relación con la actividad 4.5.2 de ITIL V3:2011, puesto que se considera que cumplen las actividad **(1, 2, 6 ,7)** (Ver cuadro 9 y 10) porque se refiere a mantener los derechas de acceso, identificaciones de actividades en relación a los roles y sus privilegios de todos los usuarios.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

No cumple en la comparación con la práctica DSS05.05 “Administrar el acceso físico a los activos de TI”, en las algunas de sus actividades. Esto se debe a que estas actividades **(1, 3, 4, 5, 6, 7)** no se relacionan con el contexto de la actividad **“Verificación”**, por tener otro objetivo a desarrollar, sin embargo, cumple en parte con el concepto de la práctica (Ver cuadro 9 y 10).

Pero también se considera ciertas coincidencias en una actividad de la práctica DSS05.04 de COBIT 5 las cuales tienen cierta relación con la actividad 4.5.1 de ITIL V3:2011, puesto que se considera que cumple la actividad **(2)** porque se refiere a solicitudes de acceso a las instalaciones.

La comparación de la actividad 4.5.1 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.
→ VS DSS01.02 Gestionar los servicios de TI externalizados.
→ VS DSS01.03 Supervisar la infraestructura de TI.
→ VS DSS01.04 Gestionar el medio ambiente.
→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02 Gestión de la red y la seguridad de la conexión.

→ VS DSS05.03 Administrar la seguridad del punto final.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de Acceso a los Servicios TI** perteneciente a **ITIL V3:2011.**

4.5.2 Monitorización de identidad VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **4.5.2** del proceso de **"Gestión de Acceso a los Servicios TI"** de **ITIL V3:2011** propone la **"Monitorización de identidad"**, que consiste en monitorizar los cambios de permisos y roles de los usuarios que trabajan en la empresa por causas como ascensos, despidos, jubilación, fallecimiento, lo cual [17]:

- ***Proceso de Gestión de Servicios de Seguridad***

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

No cumple en la comparación con la práctica DSS05.04 "Manejo de la identidad del usuario y el acceso lógico", en las algunas de sus actividades. Esto se debe a que estas actividades **(1, 2, 3, 5, 6, 7, 8)** no se relacionan con el contexto de la actividad **"Monitorización de identidad"**, por tener otro objetivo a desarrollar (Ver cuadro 9 y 10).

Pero también se considera ciertas coincidencias en una actividad de la práctica DSS05.04 de COBIT 5 las cuales tienen cierta relación con la actividad 4.5.2 de ITIL V3:2011, puesto que se considera que la actividad **(4)** (Ver cuadro 9 y 10) cumple porque se refiere a la gestión de los cambios de los derechos de acceso basándose en transacciones aprobadas y autorizadas que consten en documentos.

La comparación de la actividad 4.5.2 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

→ VS DSS01.03 Supervisar la infraestructura de TI.

→ VS DSS01.04 Gestionar el medio ambiente.

→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02 Gestión de la red y la seguridad de la conexión.

→ VS DSS05.03 Administrar la seguridad del punto final.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de Acceso a los Servicios TI** perteneciente a **ITIL V3:2011.**

4.5.3 Registro y monitorización de acceso VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **4.5.3** del proceso de **"Gestión de Acceso a los Servicios TI"** de **ITIL V3:2011** propone la **"Registro y monitorización de acceso"**, que consiste en registrar y monitorizar los permisos, con el fin de asegurar que fueron otorgados los accesos de forma correcta, lo cual [17]:

- ***Proceso de Gestión de Servicios de Seguridad***

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

No cumple en la comparación con la práctica DSS05.04 "Manejo de la identidad del usuario y el acceso lógico", en las algunas de sus actividades. Esto se debe a que estas actividades **(1, 2, 3, 4, 5, 6, 7)** no se relacionan con el contexto de la actividad **"Registro y monitorización de acceso"**, por tener otro objetivo a desarrollar (Ver cuadro 9 y 10).

Pero también se considera ciertas coincidencias en una actividad de la práctica DSS05.04 de COBIT 5 las cuales tienen cierta relación con la actividad 4.5.3 de ITIL V3:2011, puesto que se considera que la actividad **(8)** (Ver cuadro 9 y 10) cumple porque se refiere a la gestión de los cambios de los derechos de acceso basándose en transacciones aprobadas y autorizadas que consten en documentos.

La comparación de la actividad 4.5.3 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

→ VS DSS01.03 Supervisar la infraestructura de TI.

→ VS DSS01.04 Gestionar el medio ambiente.

→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02 Gestión de la red y la seguridad de la conexión.

→ VS DSS05.03 Administrar la seguridad del punto final.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de Acceso a los Servicios TI** perteneciente a **ITIL V3:2011.**

4.5.4 Eliminación y restricción de derechos VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A la actividad **4.5.4** del proceso de **"Gestión de Acceso a los Servicios TI"** de **ITIL V3:2011** propone la **"Eliminación y restricción de derechos"**, que consiste en revocar o limitar permisos de acceso por diversas circunstancias como el fallecimiento, despido, cambio de roles, traslados o renuncia, lo cual [17]:

- ***Proceso de Gestión de Servicios de Seguridad***

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

No cumple en la comparación con la práctica DSS05.04 "Manejo de la identidad del usuario y el acceso lógico", en las algunas de sus actividades. Esto se debe a que estas actividades **(1, 2, 3, 5, 6, 7, 8)** no se relacionan con el contexto de la actividad **"Eliminación y restricción de derechos"**, por tener otro objetivo a desarrollar (Ver cuadro 9 y 10).

Pero también se considera ciertas coincidencias en una actividad de la práctica DSS05.04 de COBIT 5 las cuales tienen cierta relación con la actividad 4.5.4 de ITIL V3:2011, puesto que se considera que la actividad **(4)** (Ver cuadro 9 y 10) cumple porque se refiere a la gestión de los cambios de los derechos de acceso basándose en transacciones aprobadas y autorizadas que consten en documentos.

La comparación de la actividad 4.5.4 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***
  - → VS DSS01.01 Realizar procedimientos operacionales.
  - → VS DSS01.02 Gestionar los servicios de TI externalizados.
  - → VS DSS01.03 Supervisar la infraestructura de TI.
  - → VS DSS01.04 Gestionar el medio ambiente.
  - → VS DSS01.05 Manejo de las instalaciones.
- ***Gestión de Servicios de Seguridad***
  - → VS DSS05.01 Proteger contra el malware.
  - → VS DSS05.02 Gestión de la red y la seguridad de la conexión.
  - → VS DSS05.03 Administrar la seguridad del punto final.
  - → VS DSS05.05 Administrar el acceso físico a los activos de TI.
  - → VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.
  - → VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del proceso de la **Gestión de Acceso a los Servicios TI** perteneciente a **ITIL V3:2011**

5 Fase de Mejora

5.1 Proceso de mejorar CSI VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A el proceso **5.1 "Proceso de mejorar CSI"** de **ITIL V3:2011** se compone de 7 pasos para la medición del rendimiento de los servicios TI útil para determinar las actividades y procesos que requieran optimización. Las actividades que conforman este proceso son las siguientes:

5.1.1 Decidir qué se debe medir.

5.1.2 Definir lo que finalmente se medirá.

5.1.3 Realizar dichas mediciones.

5.1.4 Procesar los datos recogidos.

5.1.5 Analizar la información recabada.

5.1.6 Proponer y documentar posibles mejoras en base al conocimiento adquirido.

5.1.7 Implementar las mejoras propuestas.

Se determina que no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5**”**; esto se debe a que se consideran como actividades como no relevantes al ámbito de estudio

5.2 Informes de servicios TI VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo A el proceso **5.2 “Informes de servicios”** de **ITIL V3:2011** se compone de 7 pasos para la medición del rendimiento de los servicios TI útil para determinar las actividades y procesos que requieran optimización. Las actividades que conforman este proceso son las siguientes:

5.2.1 Recopilación de datos

5.2.2 Análisis de datos

5.2.3 Documentación

Se determina que no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5**”**; esto se debe a que se consideran como actividades como no relevantes al ámbito de estudio.

2.4.1.2 Mapeo de los procesos de Gestión de Operaciones y Gestión de Servicios de Seguridad de COBIT 5 con los controles de ISO 27001:2005.- Se realizara una respectiva comparación entre estas actividades, procesos y controles mencionados. Este análisis se lo realizara con el fin de identificar dentro de los procesos de Gestión de Operaciones y Gestión de Servicios de Seguridad del marco de gestión analizado cuales son las actividades que cumplen en su totalidad o en parte con lo planteado por el estándar ISO 27001:2005. Para realizar este análisis se utilizara la Figura 11 (Ver Anexo B).

Justificación del mapeo de los procesos de Gestión de Operaciones y Gestión de Servicios de Seguridad de COBIT 5 con los controles de ISO 27001:2005

A.5 Política de Seguridad

A.5.1 Política de la seguridad de información VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.5.1 no contiene controles que cumplan con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad. Estas actividades ya están analizadas con ITILV3:2011.

A.6 Organización de la seguridad de la información

A.6.1 Organización interna VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.6.1 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y esta actividad es:

- ***Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

A.6.1.5 Acuerdos de confidencialidad.- Cumple con el contexto de la actividad **(1)** de la práctica DSS01.02 (Ver cuadro 9 y 10).

La comparación del objetivo de control A.6.1 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

→ VS DSS01.03 Supervisar la infraestructura de TI.

→ VS DSS01.04 Gestionar el medio ambiente.

→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

→ VS DSS05.03 Administrar la seguridad del punto final.

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de control **Organización interna** perteneciente a **ISO 27001:2005.**

A.6.2 Organización externa VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.6.2 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y esta actividad es:

- ***Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

A.6.2.2 Tratamiento de la seguridad cuando se trabaja con clientes.- Cumple con el contexto de la actividad **(1)** de la práctica (Ver cuadro 9 y 10).

A.6.2.3 Tratamiento de la seguridad en contratos con terceras personas.- Cumple con el contexto de la actividad **(1)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.6.2 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

→ VS DSS01.03 Supervisar la infraestructura de TI.

→ VS DSS01.04 Gestionar el medio ambiente.

→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

→ VS DSS05.03 Administrar la seguridad del punto final.

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de control **Organización externa** perteneciente a **ISO 27001:2005.**

A.7 Gestión de activos

A.7.1 Responsabilidad de los activos VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.7.1 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

A.7.1.3 Uso aceptable de los activos.- Cumple con el contexto de la actividad **(1)** de la práctica (Ver cuadro 9 y 10).

→ VS DSS01.03 Supervisar la infraestructura de TI.

A.7.1.1 Inventarios de activos.- Cumple con el contexto de la actividad **(2)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.7.1 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

→ VS DSS01.04 Gestionar el medio ambiente.

→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

→ VS DSS05.03 Administrar la seguridad del punto final.

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de control **Gestión de activos** perteneciente a **ISO 27001:2005.**

A.7.2 Clasificación de la Información VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.7.2 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

A.7.2.2 Etiquetado y manejo de la información.- Cumple con el contexto de la actividad **(1)** de la práctica (Ver cuadro 9 y 10).

→ VS DSS01.03 Supervisar la infraestructura de TI.

A.7.2.1 Lineamientos de clasificación.- Cumple con el contexto de la actividad **(1)** de la práctica (Ver cuadro 9 y 10).

A.7.2.2 Etiquetado y manejo de la información.- Cumple con el contexto de la actividad **(1)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.7.2 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.
→ VS DSS01.04 Gestionar el medio ambiente.
→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.
→ VS DSS05.02Gestión de la red y la seguridad de la conexión.
→ VS DSS05.03 Administrar la seguridad del punto final.
→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
→ VS DSS05.05 Administrar el acceso físico a los activos de TI.
→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.
→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de control **Gestión de activos** perteneciente a **ISO 27001:2005.**

A.8 Gestión de seguridad de los recursos humanos

A.8.1 Antes del empleo VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.8.1 no contiene controles que cumplan con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad. Estas actividades ya están analizadas con ITILV3:2011.

A.8.2 Durante el empleo VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.8.2 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

A.8.2.1 Gestión de responsabilidades.- Cumple con el contexto de la actividad **(1)** de la práctica (Ver cuadro 9 y 10).

→ VS DSS01.04 Gestionar el medio ambiente.

A.8.2.2 Capacitación y educación en seguridad de la información.- Cumple con el contexto de la actividad **(5)** de la práctica (Ver cuadro 9 y 10).

→ VS DSS01.05 Manejo de las instalaciones.

A.8.2.2 Capacitación y educación en seguridad de la información.- Cumple con el contexto de la actividad **(8)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.8.2 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.
→ VS DSS01.03 Supervisar la infraestructura de TI.
→ VS DSS01.04 Gestionar el medio ambiente.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.
→ VS DSS05.02Gestión de la red y la seguridad de la conexión.
→ VS DSS05.03 Administrar la seguridad del punto final.
→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
→ VS DSS05.05 Administrar el acceso físico a los activos de TI.
→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.
→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de control **Seguridad de los recursos humanos** perteneciente a **ISO 27001:2005.**

A.8.3 Terminación o cambio del empleo VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.8.3 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

A.8.3.1 Responsabilidades de terminación.- Cumple con el contexto de la actividad **(4)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.8.3 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.
→ VS DSS01.02 Gestionar los servicios de TI externalizados.
→ VS DSS01.03 Supervisar la infraestructura de TI.
→ VS DSS01.04 Gestionar el medio ambiente.
→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.
→ VS DSS05.02Gestión de la red y la seguridad de la conexión.
→ VS DSS05.03 Administrar la seguridad del punto final.
→ VS DSS05.05 Administrar el acceso físico a los activos de TI.
→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.
→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de control **Seguridad de los recursos humanos** perteneciente a **ISO 27001:2005.**

A.9 Seguridad física y ambiental

A.9.1 Áreas seguras VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.9.1 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

A.9.1.6 Áreas de acceso público, entrega y carga.- Cumple con el contexto de la actividad **(3)** de la práctica (Ver cuadro 9 y 10).

→ VS DSS01.04 Gestionar el medio ambiente.

A.9.1.4 Protección contra amenazas externas y ambientales.- Cumple con el contexto de la actividad **(1)** de la práctica (Ver cuadro 9 y 10).

A.9.1.1 Perímetro de seguridad física.- Cumple con el contexto de la actividad **(3)** de la práctica (Ver cuadro 9 y 10).

A.9.1.5 Trabajo en áreas seguras.- Cumple con el contexto de la actividad **(7)** de la práctica (Ver cuadro 9 y 10).

→ VS DSS01.05 Manejo de las instalaciones.

A.9.1.3 Seguridad de oficinas, habitaciones y medios.- Cumple con el contexto de la actividad **(11)** de la práctica (Ver cuadro 9 y 10).

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.03 Administrar la seguridad del punto final.

A.9.1.1 Perímetro de seguridad física.- Cumple con el contexto de la actividad **(8)** de la práctica (Ver cuadro 9 y 10).

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

A.9.1.1 Perímetro de seguridad física.- Cumple con el contexto de la actividad **(6)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.9.1 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

→ VS DSS01.03 Supervisar la infraestructura de TI.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de control **Seguridad física y ambiental** perteneciente a **ISO 27001:2005.**

A.9.2 Seguridad del Equipo VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.9.2 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Operaciones***

→ VS DSS01.04 Gestionar el medio ambiente.

A.9.2.1 Ubicación y protección del equipo.- Cumple con el contexto de la actividad **(2)** de la práctica (Ver cuadro 9 y 10).

A.9.2.5 Seguridad del equipo fuera-del local.- Cumple con el contexto de la actividad **(5)** de la práctica (Ver cuadro 9 y 10).

A.9.2.1 Ubicación y protección del equipo.- Cumple con el contexto de la actividad **(4)** de la práctica (Ver cuadro 9 y 10).

→ VS DSS01.05 Manejo de las instalaciones.

A.9.2.3 Seguridad en el cableado.- Cumple con el contexto de la actividad **(4)** de la práctica (Ver cuadro 9 y 10).

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.03 Administrar la seguridad del punto final.

A.9.2.6 Eliminación seguro o re-uso del equipo.- Cumple con el contexto de la actividad **(9)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.9.2 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

→ VS DSS01.03 Supervisar la infraestructura de TI.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de control **Seguridad física y ambiental** perteneciente a **ISO 27001:2005.**

A.10 Gestión de las comunicaciones y las operaciones

A.10.1 Procedimientos y responsabilidades operacionales VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.10.1 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

A.10.1.1 Procedimientos de operación documentados.- Se considera en parte porque cumple con el contexto de la actividad **(1)** de la práctica (Ver cuadro 9 y 10).

A.10.1.3 Segregación de deberes.- Se considera en parte porque cumple con el contexto de la actividad **(1)** de la práctica (Ver cuadro 9 y 10).

Esto se debe a que la actividad 1 del proceso DSS01.01 se encarga de desarrollar y mantener procedimientos.

La comparación del objetivo de control A.10.1 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***
  - → VS DSS01.02 Gestionar los servicios de TI externalizados.
  - → VS DSS01.03 Supervisar la infraestructura de TI.
  - → VS DSS01.04 Gestionar el medio ambiente.
  - → VS DSS01.05 Manejo de las instalaciones.
- ***Gestión de Servicios de Seguridad***
  - → VS DSS05.01 Proteger contra el malware.
  - → VS DSS05.02Gestión de la red y la seguridad de la conexión.
  - → VS DSS05.03 Administrar la seguridad del punto final.
  - → VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
  - → VS DSS05.05 Administrar el acceso físico a los activos de TI.
  - → VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.
  - → VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de control **Gestión de las comunicaciones y las operaciones** perteneciente a **ISO 27001:2005.**

A.10.2 Gestión de la entrega de servicios a terceros VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.10.2 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Operaciones***
  - → VS DSS01.02 Gestionar los servicios de TI externalizados.

A.10.2.1 Entrega del servicio.- Cumple con el contexto de la actividad **(2)** de la práctica (Ver cuadro 9 y 10).

A.10.2.2 Monitoreo y revisión de los servicios de terceros.- Cumple con el contexto de la actividad **(3, 4)** de la práctica (Ver cuadro 9 y 10).

A.10.2.3 Manejar los cambios en los servicios de terceros.- Cumple con el contexto de la actividad **(3)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.10.2 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***
  - → VS DSS01.01 Realizar procedimientos operacionales.
  - → VS DSS01.03 Supervisar la infraestructura de TI.
  - → VS DSS01.04 Gestionar el medio ambiente.
  - → VS DSS01.05 Manejo de las instalaciones.
- ***Gestión de Servicios de Seguridad***
  - → VS DSS05.01 Proteger contra el malware.
  - → VS DSS05.02Gestión de la red y la seguridad de la conexión.
  - → VS DSS05.03 Administrar la seguridad del punto final.
  - → VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
  - → VS DSS05.05 Administrar el acceso físico a los activos de TI.
  - → VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.
  - → VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de control **Gestión de las comunicaciones y las operaciones** perteneciente a **ISO 27001:2005.**

A.10.3 Gestión de la entrega de servicios a terceros VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.10.3 no contiene controles que cumplan con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad. Estas actividades ya están analizadas con ITILV3:2011.

A.10.4 Protección contra software malicioso y código móvil VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.10.4 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

A.10.4.1 Controles contra Software malicioso.- Cumple con el contexto de la actividad **(1, 2)** de la práctica (Ver cuadro 9 y 10).

→ VS DSS05.03 Administrar la seguridad del punto final.

A.10.4.1 Controles contra Software malicioso.- Cumple con el contexto de la actividad **(7)** de la práctica (Ver cuadro 9 y 10).

A.10.4.2 Controles contra códigos móviles.- Cumple con el contexto de la actividad **(7)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.10.4 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.
→ VS DSS01.02 Gestionar los servicios de TI externalizados.
→ VS DSS01.03 Supervisar la infraestructura de TI.
→ VS DSS01.04 Gestionar el medio ambiente.
→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.
→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
→ VS DSS05.05 Administrar el acceso físico a los activos de TI.
→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.
→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de control **Gestión de las comunicaciones y las operaciones** perteneciente a **ISO 27001:2005.**

A.10.5 Respaldo (back-up) VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.10.5 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

A.10.5.1 *Back-up o respaldo de la información*.- Cumple con el contexto de la actividad **(5)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.10.5 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.
→ VS DSS01.03 Supervisar la infraestructura de TI.
→ VS DSS01.04 Gestionar el medio ambiente.
→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.
→ VS DSS05.02Gestión de la red y la seguridad de la conexión.
→ VS DSS05.03 Administrar la seguridad del punto final.
→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
→ VS DSS05.05 Administrar el acceso físico a los activos de TI.
→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.
→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de control **Gestión de las comunicaciones y las operaciones** perteneciente a **ISO 27001:2005.**

A.10.6 Gestión de seguridad de redes VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.10.6 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.03 Administrar la seguridad del punto final.

A.10.6.1 Controles de red.- Cumple con el contexto de la actividad **(3)** de la práctica (Ver cuadro 9 y 10).

A.10.6.2 Seguridad de los servicios de red.- Se considera en parte porque cumple con el contexto de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.10.6 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.
→ VS DSS01.02 Gestionar los servicios de TI externalizados.
→ VS DSS01.03 Supervisar la infraestructura de TI.
→ VS DSS01.04 Gestionar el medio ambiente.
→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.
→ VS DSS05.02 Gestión de la red y la seguridad de la conexión.
→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
→ VS DSS05.05 Administrar el acceso físico a los activos de TI.
→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.
→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de control **Gestión de las comunicaciones y las operaciones** perteneciente a **ISO 27001:2005.**

A.10.7 Gestión de medios VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.10.7 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

A.10.7.3 Procedimientos de manejo de la información.- Cumple con el contexto de la actividad **(4)** de la práctica (Ver cuadro 9 y 10).

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.03 Administrar la seguridad del punto final.

A.10.7.2 Eliminación de medios.- Cumple con el contexto de la actividad **(9)** de la práctica (Ver cuadro 9 y 10).

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

A.10.7.4 Seguridad de documentación del sistema.- Cumple con el contexto de la actividad **(2)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.10.7 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.
→ VS DSS01.03 Supervisar la infraestructura de TI.
→ VS DSS01.04 Gestionar el medio ambiente.
→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.
→ VS DSS05.02Gestión de la red y la seguridad de la conexión.
→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
→ VS DSS05.05 Administrar el acceso físico a los activos de TI.
→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de control **Gestión de las comunicaciones y las operaciones** perteneciente a **ISO 27001:2005.**

A.10.8 Intercambio de información VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.10.8 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

A.10.8.4 Mensajes electrónicos.- Cumple con el contexto de la actividad **(5, 6)** de la práctica (Ver cuadro 9 y 10).

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

A.10.8.3 Medios físicos en tránsito.- Cumple con el contexto de la actividad **(1)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.10.8 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.
→ VS DSS01.02 Gestionar los servicios de TI externalizados.
→ VS DSS01.03 Supervisar la infraestructura de TI.
→ VS DSS01.04 Gestionar el medio ambiente.
→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.
→ VS DSS05.03 Administrar la seguridad del punto final.
→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
→ VS DSS05.05 Administrar el acceso físico a los activos de TI.
→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de control **Gestión de las comunicaciones y las operaciones** perteneciente a **ISO 27001:2005.**

A.10.9 Servicios de comercio electrónico VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Existe una actividad pertenecientes a este objetivo de control, que aunque no cumplen con las el contexto de las prácticas que propone COBIT 5, es relevante para en sus procesos DSS01 y DSS05.

A.10.9.1 Comercio electrónico.- no cumple con el contexto de las actividades de las prácticas de los procesos DSS01 y DSS05 de la práctica (Ver cuadro 9 y 10).

A.10.9.2 Transacciones en línea.- no cumple con el contexto de las actividades de las prácticas de los procesos DSS01 y DSS05 de la práctica (Ver cuadro 9 y 10).

A.10.9.3 Información disponible públicamente.- no cumple con el contexto de las actividades de las prácticas de los procesos DSS01 y DSS05 de la práctica (Ver cuadro 9 y 10).

A.10.10 Servicios de comercio electrónico VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.10.10 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

A.10.10.2 Uso del sistema de monitoreo.- Se considera que cumple en parte con el contexto de la actividad **(1)** de la práctica (Ver cuadro 9 y 10).

→ VS DSS01.03 Supervisar la infraestructura de TI.

A.10.10.1 Medios físicos en tránsito.- Cumple con el contexto de la actividad **(4)** de la práctica (Ver cuadro 9 y 10).

A.10.10.5 Registro de fallas.- Cumple con el contexto de la actividad **(5)** de la práctica (Ver cuadro 9 y 10).

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

A.10.10.1 Registro del administrador y operador.- Cumple con el contexto de la actividad **(7)** de la práctica (Ver cuadro 9 y 10).

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

A.10.10.1 Medios físicos en tránsito.- Cumple con el contexto de la actividad **(1)** de la práctica (Ver cuadro 9 y 10).

A.10.10.5 Registro de fallas.- Cumple con el contexto de la actividad **(1)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.10.10 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

→ VS DSS01.04 Gestionar el medio ambiente.

→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

→ VS DSS05.03 Administrar la seguridad del punto final.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de control **Gestión de las comunicaciones y las operaciones** perteneciente a **ISO 27001:2005.**

A.11 Control de Acceso

A.11.1 Control de acceso VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Existe una actividad pertenecientes a este objetivo de control, que aunque no cumplen con las el contexto de las practicas que propone COBIT 5, es relevante para en sus procesos DSS01 y DSS05.

A.11.1.1 Política de control de acceso.- no cumple con el contexto de las actividades de las prácticas de los procesos DSS01 y DSS05 (Ver cuadro 9 y 10), actividad anteriormente tratada con ITILV3:2011.

A.11.2 Gestión del acceso del usuario VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.11.2 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

A.11.2.1 Inscripción del usuario.- Se considera que cumple en parte con el contexto de la actividad **(1)** de la práctica (Ver cuadro 9 y 10).

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico

A.11.2.1 Inscripción del usuario.- Cumple con el contexto de la actividad **(6)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.11.2 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.
→ VS DSS01.03 Supervisar la infraestructura de TI.
→ VS DSS01.04 Gestionar el medio ambiente.
→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.
→ VS DSS05.02Gestión de la red y la seguridad de la conexión.
→ VS DSS05.03 Administrar la seguridad del punto final.
→ VS DSS05.05 Administrar el acceso físico a los activos de TI.
→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.
→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de **Control de Acceso** perteneciente a **ISO 27001:2005.**

A.11.3 Responsabilidades del usuario VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.11.3 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

A.11.3.1 Uso de clave.- Se considera que cumple en parte con el contexto de la actividad **(7)** de la práctica (Ver cuadro 9 y 10).

A.11.3.2 Equipo de usuario desatendido.- Se considera que cumple en parte con el contexto de la actividad **(7)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.11.3 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.
→ VS DSS01.02 Gestionar los servicios de TI externalizados.
→ VS DSS01.03 Supervisar la infraestructura de TI.
→ VS DSS01.04 Gestionar el medio ambiente.
→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.
→ VS DSS05.02Gestión de la red y la seguridad de la conexión.
→ VS DSS05.03 Administrar la seguridad del punto final.
→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.
→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de **Control de acceso** perteneciente a **ISO 27001:2005.**

A.11.4 Control de acceso VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.11.2 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

A.11.4.1 Política sobre el uso de servicios en red.- Cumple con el contexto de la actividad **(1)** de la práctica (Ver cuadro 9 y 10).

A.11.4.3 Identificación del equipo en red.- Cumple con el contexto de la actividad **(2)** de la práctica (Ver cuadro 9 y 10).

A.11.4.4 Protección del puerto de diagnóstico remoto.- Cumple con el contexto de la actividad **(3)** de la práctica (Ver cuadro 9 y 10).

A.11.4.6 Control de conexiones a redes.- Cumple con el contexto de la actividad **(1, 2, 5)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.11.4 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.
→ VS DSS01.02 Gestionar los servicios de TI externalizados.
→ VS DSS01.03 Supervisar la infraestructura de TI.
→ VS DSS01.04 Gestionar el medio ambiente.
→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.
→ VS DSS05.03 Administrar la seguridad del punto final.
→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de **Control de acceso** perteneciente a **ISO 27001:2005.**

A.11.5 Control de acceso al sistema de operación VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.11.2 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

A.11.5.5 Sesión inactiva.- Se considera que cumple en parte con el contexto de la actividad **(2)** de la práctica (Ver cuadro 9 y 10).

A.11.5.6 Limitación de tiempo de conexión.- Se considera que cumple en parte con el contexto de la actividad **(2)** de la práctica (Ver cuadro 9 y 10).

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.03 Administrar la seguridad del punto final.

A.11.5.1 Procedimientos de registro en el terminal.- Cumple con el contexto de la actividad **(1)** de la práctica (Ver cuadro 9 y 10).

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

A.11.5.2 Identificación y autenticación del usuario.- Cumple con el contexto de la actividad **(3, 7)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.11.5 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

→ VS DSS01.03 Supervisar la infraestructura de TI.

→ VS DSS01.04 Gestionar el medio ambiente.

→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de **Control de Acceso** perteneciente a **ISO 27001:2005.**

A.11.6 Control de acceso a la aplicación VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.11.2 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Operaciones***

→ VS DSS01.05 Manejo de las instalaciones.

A.11.6.1 Restricción al acceso a la información.- Cumple con el contexto de la actividad **(10)** de la práctica (Ver cuadro 9 y 10).

A.11.6.2 Aislamiento del sistema sensible.- Cumple con el contexto de la actividad **(10)** de la práctica (Ver cuadro 9 y 10).

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.03 Administrar la seguridad del punto final.

A.11.6.1 Restricción al acceso a la información.- Cumple con el contexto de la actividad **(10)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.11.6 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.

→ VS DSS01.02 Gestionar los servicios de TI externalizados.

→ VS DSS01.03 Supervisar la infraestructura de TI.

→ VS DSS01.04 Gestionar el medio ambiente.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.

→ VS DSS05.05 Administrar el acceso físico a los activos de TI.

→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de control **Gestión de las comunicaciones y las operaciones** perteneciente a **ISO 27001:2005.**

A.11.6 Control de acceso a la aplicación VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Existe una actividad pertenecientes a este objetivo de control, que aunque no cumplen con las el contexto de las practicas que propone COBIT 5, es relevante para en sus procesos DSS01 y DSS05.

A.11.7.1 Computación móvil y comunicaciones.- no cumple con el contexto de las actividades de las prácticas de los procesos DSS01 y DSS05 de la práctica (Ver cuadro 9 y 10).

A.11.7.2 Tele-trabajo.- no cumple con el contexto de las actividades de las prácticas de los procesos DSS01 y DSS05 de la práctica (Ver cuadro 9 y 10).

A.12 Adquisición y mantenimiento de los sistemas de información

A.12.1 Requerimientos de seguridad de los sistemas VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.12.1 no contiene controles que cumplan con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad. Estas actividades ya están analizadas con ITILV3:2011.

A.12.2 Procesamiento correcto de las aplicaciones VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.12.1 no contiene controles que cumplan con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad. Estas actividades ya están analizadas con ITILV3:2011.

A.12.3 Controles criptográficos VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.12.3 contiene controles que cumplen con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad y estas actividades son:

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.02Gestión de la red y la seguridad de la conexión.

A.12.3.1 Política sobre el uso de controles criptográficos.- Cumple con el contexto de la actividad **(4)** de la práctica (Ver cuadro 9 y 10).

A.12.3.2 Gestión clave.- Cumple con el contexto de la actividad **(4)** de la práctica (Ver cuadro 9 y 10).

La comparación del objetivo de control A.12.3 realizada con las actividades de las siguientes prácticas:

- ***Gestión de Operaciones***

→ VS DSS01.01 Realizar procedimientos operacionales.
→ VS DSS01.02 Gestionar los servicios de TI externalizados.
→ VS DSS01.03 Supervisar la infraestructura de TI.
→ VS DSS01.04 Gestionar el medio ambiente.
→ VS DSS01.05 Manejo de las instalaciones.

- ***Gestión de Servicios de Seguridad***

→ VS DSS05.01 Proteger contra el malware.
→ VS DSS05.03 Administrar la seguridad del punto final.
→ VS DSS05.04 Manejo de la identidad del usuario y el acceso lógico.
→ VS DSS05.05 Administrar el acceso físico a los activos de TI.
→ VS DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.

→ VS DSS05.07Supervisar la infraestructura para eventos relacionados con la seguridad.

No se encuentran coincidencias porque su contexto (Ver cuadro 9 y 10) no se acerca a ninguna de las actividades del objetivo de control **Adquisición y mantenimiento de los sistemas de información** perteneciente a **ISO 27001:2005.**

A.12.4 Controles criptográficos VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.12.4 contiene controles que cumplan con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad. Estas actividades ya están analizadas con ITILV3:2011.

A.12.5 Seguridad en los procesos de desarrollo y soporte VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.12.5 contiene controles que cumplan con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad. Estas actividades ya están analizadas con ITILV3:2011.

A.12.6 Gestión de vulnerabilidad técnica VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.12.6 contiene controles que cumplan con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad. Estas actividades ya están analizadas con ITILV3:2011.

A.13 Adquisición y mantenimiento de los sistemas de información VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.13 no contiene controles que cumplan con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad. Estas actividades ya están analizadas con ITILV3:2011.

A.14 Adquisición y mantenimiento de los sistemas de información VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el Anexo B el objetivo de control A.14 no contiene controles que cumplan con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad. Estas actividades ya están analizadas con ITILV3:2011.

A.15 Adquisición y mantenimiento de los sistemas de información VS Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad.

Como se puede observar en el cuadro 15 el objetivo de control A.15 no contiene controles que cumplan con las actividades de las prácticas del Marco de referencia COBIT 5 – DSS01 Gestión de Operaciones y DSS05 Gestión de Servicios de Seguridad. Estas actividades ya están analizadas con ITILV3:2011.

2.4.2 Limitaciones del modelo

De acuerdo al análisis realizado durante el mapeo de las actividades de COBIT 5, procesos de ITIL V3:2011 y controles de ISO: 27001, se encontraron las siguientes limitaciones y para el modelo propuesto.

Cuadro 13. Limitaciones de las actividades de ITIL V3:2011 hacia el marco de referencia COBIT 5.

Fase: Estrategia		
Proceso:	**1.1 Gestión Financiera**	
Actividades	**Tipo de Limitación**	**Justificación**
1.1.1 Presupuesto	Práctica	Como se puede observar en el **Anexo A** la actividad **1.1.1** del proceso de **"Gestión Financiera"** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone COBIT 5, pero se considera crear una práctica para el proceso DSS01 para llevar a cabo planificación el gasto de inversión TI a largo plazo.

Cuadro 13. (Continuación)

Fase: Estrategia		
Proceso: **1.1 Gestión Financiera**		
Actividades	**Tipo de Limitación**	**Justificación**
1.1.2 Contabilidad	Práctica	Como se puede observar en el **Anexo A** la actividad **1.1.2** del proceso de **"Gestión Financiera"** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone COBIT 5, pero se considera crear una práctica para el proceso DSS01 para llevar a cabo una correcta evaluación de los costes reales para su comparación con lo presupuestado.
1.1.3 Política de Precios	Sin Acción	No se considera esta actividad para los procesos DSS01, ni DSS05 debido a que esta, tiene un enfoque para los proveedores de servicios, mas no para la gestión de TI por parte de las empresas, por esta razón no se la puede considerar Actividad, ni práctica.
Proceso: **1.2 Gestión del Portafolio de Servicios**		
Actividades	**Tipo de Limitación**	**Justificación**
1.2.1 Definición del Negocio	Sin Acción	No se considera esta actividad para los procesos DSS01, ni DSS05 debido a que esta, tiene un enfoque para los proveedores de servicios, mas no para la gestión de TI por parte de las empresas, por esta razón no se la puede considerar Actividad, ni práctica.
1.2.2 Análisis de servicios	Sin Acción	No se considera esta actividad para los procesos DSS01, ni DSS05 debido a que esta, tiene un enfoque para los proveedores de servicios, mas no para la gestión de TI por parte de las empresas, por esta razón no se la puede considerar Actividad, ni práctica.

Cuadro 13. (Continuación)

Fase: Estrategia		
Proceso:	**1.3 Gestión de la Demanda**	
Actividades	**Tipo de Limitación**	**Justificación**
1.3.1 Análisis de la actividad	Sin Acción	No se considera esta actividad para los procesos DSS01, ni DSS05 debido a que esta, tiene un enfoque para los proveedores de servicios, mas no para la gestión de TI por parte de las empresas, por esta razón no se la puede considerar Actividad, ni práctica.
1.3.2 Desarrollo de la Oferta	Sin Acción	No se considera esta actividad para los procesos DSS01, ni DSS05 debido a que esta, tiene un enfoque para los proveedores de servicios, mas no para la gestión de TI por parte de las empresas, por esta razón no se la puede considerar Actividad, ni práctica.
Fase: Diseño		
Proceso:	**2.1 Gestión del Catálogo de Servicios**	
Actividades	**Tipo de Limitación**	**Justificación**
2.1.1 Definición de las familias principales de servicios a prestar	Sin Acción	No se considera esta actividad para los procesos DSS01, ni DSS05 debido a que esta, tiene un enfoque para los proveedores de servicios, mas no para la gestión de TI por parte de las empresas, por esta razón no se la puede considerar Actividad, ni práctica.
2.1.2 Mantenimiento y actualización del Catálogo de Servicios	Sin Acción	No se considera esta actividad para los procesos DSS01, ni DSS05 debido a que esta, tiene un enfoque para los proveedores de servicios, mas no para la gestión de TI por parte de las empresas, por esta razón no se la puede considerar Actividad, ni práctica.

Cuadro 13. (Continuación)

Fase: Diseño		
Proceso:	**2.2 Gestión de Niveles de Servicio**	
Actividades	**Tipo de Limitación**	**Justificación**
2.2.1 Planificación de los Niveles de Servicio	Actividad	Como se puede observar en el **Anexo A** la actividad **2.2.1** del proceso de **ITIL V3:2011,** cumple en parte con actividades **(1, 2)** de la práctica **DSS01.02 "Gestionar los servicios de TI externalizados**" que propone COBIT 5, por ello se considera crear una actividad para llevar a cabo planificación de los niveles de servicio mediante la elaboración de los requisitos, hojas de especificación para determinar las necesidades de externalización de las empresas
2.2.2 Implementación de los Acuerdos de Niveles de Servicio	Actividad	Como se puede observar en el **Anexo A** la actividad **2.2.2** del proceso de **ITIL V3:2011,** cumple en parte con actividades **(1, 2)** de la práctica **DSS01.02 "Gestionar los servicios de TI externalizados**" que propone COBIT 5, por ello se considera crear una actividad para llevar a cabo el proceso de contratación o elaboración de los contratos y acuerdos de nivel de servicio y operación.
2.2.3 Supervisión y revisión de los Acuerdos de Nivel de Servicio	Sin acción	Como se puede observar en el **Anexo A** la cumple con actividades **(3, 4)** de la práctica **DSS01.02 "Gestionar los servicios de TI externalizados**" que propone COBIT 5, por esta razón no se la puede considerar Actividad, ni práctica.

Cuadro 13. (Continuación)

Fase: Diseño		
Proceso:	**2.3 Gestión de la Capacidad**	
Actividades	**Tipo de Limitación**	**Justificación**
2.3.2 Monitorización de los recursos de la infraestructura TI	Enfoque	Como se puede observar en el **Anexo A** la actividad **2.3.2** del proceso de **ITIL V3:2011,** cumple en parte la actividad **(2)** de la práctica **DSS01.02 "Gestionar los servicios de TI externalizados**" que propone COBIT 5, por ello se considera crear una actividad para llevar a cabo la asignación de recursos adecuados para cada servicio y aplicación.
2.3.3 Supervisión de la capacidad	Sin acción	Como se puede observar en el **Anexo A** la actividad **2.3.3** del proceso de **ITIL V3:2011,** cumple con actividades **(2, 3)** de la práctica **DSS01.02 "Gestionar los servicios de TI externalizados"** que propone COBIT 5, por esta razón no se la puede considerar Actividad, ni práctica.
Proceso:	**2.4 Gestión de la Disponibilidad**	
Actividades	**Tipo de Limitación**	**Justificación**
2.4.1 Determinar cuáles son los requisitos de disponibilidad reales del negocio	Enfoque	Como se puede observar en el **Anexo A** la actividad **2.4.1** del proceso de **ITIL V3:2011,** cumple en parte la actividad **(2)** de la práctica **DSS01.02 "Gestionar los servicios de TI externalizados**" que propone COBIT 5, por ello se considera crear una actividad para cuantificar los requisitos de la disponibilidad para la correcta elaboración de los ANS manteniendo el balance entre las necesidades reales del negocio.

Cuadro 13. (Continuación)

Fase: Diseño		
Proceso:	**2.4 Gestión de la Disponibilidad**	
Actividades	**Tipo de Limitación**	**Justificación**
2.4.2 Desarrollar un plan de disponibilidad donde se estime el futuro a corto y medio plazo	Enfoque	Como se puede observar en el **Anexo A** la actividad **2.4.2** del proceso **2.4** de **ITIL V3:2011,** tiene relación con una de las actividades (2) de las práctica DSS01.02, por lo cual se considera mejorar su enfoque para establecer los niveles de disponibilidad adecuados según la necesidades reales de la empresa y determinar los intervalos de interrupción de los servicios dependiendo de su impacto.
2.4.3Mantenimiento del servicio en operación y recuperación del mismo en caso de fallo	Actividad	Como se puede observar en el **Anexo 1** la actividad **2.4.3** del proceso de **ITIL V3:2011,** cumple con el contexto de la práctica **DSS01.01 "Realizar procedimientos operacionales",** que propone **COBIT 5**, por ello se considera crear una actividad para recuperar el servicio en el menor tiempo posible en el caso de interrupciones del servicio por incidencias o por tareas planificadas de mantenimiento.
Proceso:	**2.5 Gestión de la Continuidad de los servicios TI**	
Actividades	**Tipo de Limitación**	**Justificación**
2.5.1 Establecer las políticas y alcance de la ITSCM	Sin Acción	Como se puede observar en el **Anexo A** la actividad **2.5.1** del proceso **2.5** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** ni con el contexto de las mismas.

Cuadro 13. (Continuación)

Fase: Diseño		
Proceso:	**2.5 Gestión de la Continuidad de los servicios TI**	
Actividades	**Tipo de Limitación**	**Justificación**
2.5.2 Evaluar el impacto en el negocio de una interrupción de los servicios TI	Sin Acción	Como se puede observar en el **Anexo A** la actividad **2.5.2** del proceso **2.5** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** ni con el contexto de las mismas.
2.5.3 Analizar y prever los riesgos a los que está expuesto la infraestructura TI	Sin Acción	Como se puede observar en el **Anexo A** la actividad **2.5.3** del proceso **2.5** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** ni con el contexto de las mismas.
2.5.4 Establecer las estrategias de continuidad del servicio TI	Sin Acción	Como se puede observar en el **Anexo A** la actividad **2.5.4** del proceso **2.5** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** ni con el contexto de las mismas.
2.5.5 Desarrollar los planes de contingencia	Sin Acción	Como se puede observar en el **Anexo A** la actividad **2.5.4** del proceso **2.5** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** ni con el contexto de las mismas.
2.5.6 Poner a prueba dichos planes	Sin Acción	Como se puede observar en el **Anexo A** la actividad **2.5.6** del proceso de **ITIL V3:2011,** cumple con la actividad **(3)** de la práctica **DSS01.02 "Gestionar los servicios de TI externalizados"** que propone COBIT 5, por esta razón no se la puede considerar actividad, ni práctica.

Cuadro 13. (Continuación)

Fase: Diseño		
Proceso:	**2.5 Gestión de la Continuidad de los servicios TI**	
Actividades	**Tipo de Limitación**	**Justificación**
2.5.8 Revisar periódicamente los planes para adaptarlos a las necesidades reales del negocio	Sin Acción	Como se puede observar en el **Anexo A** la actividad **2.5.8** del proceso de **ITIL V3:2011,** cumple con la actividad **(6)** de la práctica **DSS01.04 "Gestionar el medio ambiente"** que propone COBIT 5, por ello se considera crear una actividad para actualizar periódicamente los planes para asegurar que responden a los requisitos de la organización en su conjunto.
Proceso:	**2.6 Gestión de la Seguridad de la Información**	
Actividades	**Tipo de Limitación**	**Justificación**
2.6.1 Constituya política de seguridad que oriente a la empresa	Práctica	Como se puede observar en el **Anexo A** la actividad **2.6.1** del proceso **2.6** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** pero se considera crear una práctica para el proceso **DSS05** para formar establecer una política global y clara sobre la seguridad, en donde se fijen aspectos tales como los objetivos, responsabilidades y recursos.

Cuadro 13. (Continuación)

Fase: Diseño		
Proceso:	**2.6 Gestión de la Seguridad de la Información**	
Actividades	**Tipo de Limitación**	**Justificación**
2.6.2 Realizar un Plan de Seguridad que integre los límites de seguridad adecuados descritos en los acuerdos de servicio firmados con proveedores internos y externo.	Práctica	Como se puede observar en el **Anexo A** la actividad **2.6.2** del proceso **2.6** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** pero se considera crear una práctica para el proceso **DSS05** para fijar los niveles de seguridad que serán incluidos como parte de los Acuerdos de niveles de seguridad (ANS), acuerdos de nivel de operación (OLAs) y contratos de apoyo (UC), incluyendo métricas o indicadores para evaluar los niveles de seguridad.
2.6.3 Supervisión proactiva de los límites de seguridad analizando tendencias, nuevos riesgos y vulnerabilidades.	Sin Acción	Como se puede observar en el **Anexo A** existen varias actividades que cumplen en parte con la función de la actividad **2.6.3** propuesta por el proceso **2.6** de **ITIL V3:2011**, tal es así que en, la actividad (1) del proceso **DSS01.02 "Gestionar los servicios de TI externalizados"** y las actividades **(1, 4, 6)** de **DSS05.01 "Proteger contra el malware"** que propone COBIT 5, permiten cumplir totalmente con la función de la actividad **2.6.5**, por esta razón no se la puede considerar actividad, ni práctica.

Cuadro 13. (Continuación)

Fase: Diseño		
Proceso:	**2.7 Gestión de Proveedores**	
Actividades	**Tipo de Limitación**	**Justificación**
2.7.1 Los requisitos de contratación que se van a exigir a los proveedores	Actividad	Como se puede observar en el **Anexo A** la actividad **2.7.1** del proceso de **ITIL V3:2011,** cumple con el contexto de la práctica **DSS01.02 "Gestionar los servicios de TI externalizados",** que propone COBIT 5, por ello se considera crear una actividad para analizar las estrategias generales de la organización y los servicios que presta, para definir sus necesidades de contratación.
2.7.2 Los procesos de evaluación y selección de proveedores	Práctica	Como se puede observar en el **Anexo A** la actividad **2.6.6** del proceso **2.6** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** pero se considera crear una práctica para el proceso **DSS01** para elegir un proveedor acorde con los requisitos de la empresa, tomando en cuenta sus referencias, capacidad, disponibilidad y el financiamiento del cual dispone la empresa.
2.7.3 La clasificación y documentación de la relación con los proveedores	Práctica	Como se puede observar en el **Anexo A** la actividad **2.7.3** del proceso **2.7** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** pero se considera crear una práctica para el proceso **DSS01** para crear una base de datos que reúna información de los proveedores, contratos, nivel de atención y su relación con otros procesos de gestión.

Cuadro 13. (Continuación)

Fase: Diseño		
Proceso:	**2.7 Gestión de Proveedores**	
Actividades	**Tipo de Limitación**	**Justificación**
2.7.4 Gestión del Rendimiento de los proveedores	Sin Acción	Como se puede observar en el **Anexo A** existe una actividad que cumplen en parte con la función de la actividad **2.7.4** propuesta por el proceso **2.7** de **ITIL V3:2011**, la actividad (3) del proceso **DSS01.02 "Gestionar los servicios de TI externalizados"** que propone COBIT 5, por esta razón no se la puede considerar actividad, ni práctica.
2.7.5 Renovación o terminación	Práctica	Como se puede observar en el **Anexo A** la actividad **2.7.5** del proceso **2.7** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** pero se considera crear una práctica para asesorar a los directivos sobre la renovación o terminación de contratos de los proveedores, considerando su rendimiento, perspectivas de crecimiento de la empresa y cumplimiento de contrato.
Fase: Transición		
Proceso:	**3.1 Planificación y soporte a la Transición**	
Actividades	**Tipo de Limitación**	**Justificación**
3.1.1 Estrategia de transición	Sin Acción	No se considera esta actividad para los procesos DSS01, ni DSS05 debido a que esta tiene un enfoque para los proveedores de servicios, mas no para la gestión de TI por parte de las empresas, por esta razón no se la puede considerar Actividad, ni práctica.

Cuadro 13. (Continuación)

Fase: Transición		
Proceso:	**3.1 Planificación y soporte a la Transición**	
Actividades	**Tipo de Limitación**	**Justificación**
3.1.2 Preparación de transición	Sin Acción	No se considera esta actividad para los procesos DSS01, ni DSS05 debido a que esta tiene un enfoque para los proveedores de servicios, mas no para la gestión de TI por parte de las empresas, por esta razón no se la puede considerar Actividad, ni práctica.
3.1.3 Planificación de la transición	Sin Acción	No se considera esta actividad para los procesos DSS01, ni DSS05 debido a que esta tiene un enfoque para los proveedores de servicios, mas no para la gestión de TI por parte de las empresas, por esta razón no se la puede considerar Actividad, ni práctica.
Proceso:	**3.2 Gestión de Cambios**	
Actividades	**Tipo de Limitación**	**Justificación**
3.2.1 Registro de peticiones	Sin acción	Como se puede observar en el **Anexo A** la actividad **3.2.1** del proceso **3.2** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** ni con el contexto de las mismas.
3.2.2 Aceptación y Clasificación del cambio	Sin acción	Como se puede observar en el **Anexo A** la actividad **3.2.2** del proceso **3.2** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** ni con el contexto de las mismas.

Cuadro 13. (Continuación)

Fase: Transición		
Proceso:	**3.2 Gestión de Cambios**	
Actividades	**Tipo de Limitación**	**Justificación**
3.2.3 Aprobación y Planificación del cambio	Sin acción	Como se puede observar en el **Anexo A** la actividad **3.2.3** del proceso **3.2** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** ni con el contexto de las mismas.
3.2.4 Implementación del cambio	Sin acción	Como se puede observar en el **Anexo A** la actividad **3.2.4** del proceso **3.2** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** ni con el contexto de las mismas.
3.2.5 Evaluación del cambio	Sin acción	Como se puede observar en el **Anexo A** la actividad **3.2.5** del proceso **3.2** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** ni con el contexto de las mismas.
3.2.6 Cambios de emergencia	Sin acción	Como se puede observar en el **Anexo A** la actividad **3.2.6** del proceso **3.2** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** ni con el contexto de las mismas.

Cuadro 13. (Continuación)

Fase: Transición		
Proceso:	**3.3 Gestión de la Configuración y Activos del Servicio**	
Actividades	**Tipo de Limitación**	**Justificación**
3.3.1 Planificación de la Configuración	Sin acción	Como se puede observar en el **Anexo A** la actividad **3.3.1** del proceso **3.3** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** ni con el contexto de las mismas.
3.3.2 Clasificación y registro de los Elementos de Configuración	Sin acción	Como se puede observar en el **Anexo A** existe una actividad que cumple con la función de la actividad **3.3.2** propuesta por el proceso **3.3** de **ITIL V3:2011**, siendo esta la actividad (2) del proceso **DSS01.03 "Supervisar la Infraestructura de TI",** que propone COBIT 5, por esta razón no se la puede considerar actividad, ni práctica.
3.3.3 Monitorización y Control	Sin acción	Como se puede observar en el **Anexo A** la actividad **3.3.3** del proceso de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** ni con el contexto de las mismas.
3.3.4 Realización de auditorías	Sin acción	Como se puede observar en el **Anexo A** la actividad **3.3.4** del proceso de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** ni con el contexto de las mismas.

Cuadro 13. (Continuación)

Fase: Transición		
Proceso:	**3.4 Gestión de entrega y despliegues**	
Actividades	**Tipo de Limitación**	**Justificación**
3.4.1 Planificación de entregas 3.4.2 Desarrollo del despliegue 3.4.3 Implementación de la entrega 3.4.4 Comunicación y formación al cliente	Sin Acción	No se considera al proceso 3.4 de **ITIL V3:2011** para los procesos DSS01, ni DSS05 debido a que esta tiene un enfoque para los proveedores de servicios, mas no para la gestión de TI por parte de las empresas, por esta razón sus actividades no se las puede considerar como una nueva actividad o práctica.
Proceso:	**3.5 Validación y pruebas**	
Actividades	**Tipo de Limitación**	**Justificación**
3.5.1 Validación, planificación y verificación de tests 3.5.2 Construcción de tests 3.5.3 Pruebas de Validación 3.5.4 Aceptación y reporte 3.5.5 Limpieza y cierre	Sin Acción	No se considera al proceso 3.5 de **ITIL V3:2011** para los procesos DSS01, ni DSS05 debido a que esta tiene un enfoque para los proveedores de servicios, mas no para la gestión de TI por parte de las empresas, por esta razón sus actividades no se las puede considerar como una nueva actividad o práctica.

Cuadro 13. (Continuación)

Fase: Transición		
Proceso:	**3.6 Evaluación**	
Actividades	**Tipo de Limitación**	**Justificación**
3.6.1 Planificación de la evaluación. 3.6.2 Evaluación del rendimiento previsto. 3.6.3 Evaluación del rendimiento real.	Sin Acción	No se considera al proceso 3.6 de **ITIL V3:2011** para los procesos DSS01, ni DSS05 debido a que esta tiene un enfoque para los proveedores de servicios, mas no para la gestión de TI por parte de las empresas, por esta razón sus actividades no se las puede considerar como una nueva actividad o práctica.
Proceso:	**3.7 Gestión del Conocimiento**	
Actividades	**Tipo de Limitación**	**Justificación**
3.7.1 Puntualizar una estrategia de Gestión del Conocimiento y divulgarla a toda la empresa	Práctica	Como se puede observar en el cuadro 15la actividad **3.7.1** del proceso **3.7** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** pero se considera crear un práctica para definir, desarrollar y difundir una estrategia de conocimiento en la que se reflejen las condiciones de administración, roles, procedimientos de registro y validación de información.

Cuadro 13. (Continuación)

Fase: Transición		
Proceso:	**3.7 Gestión del Conocimiento**	
Actividades	**Tipo de Limitación**	**Justificación**
3.7.2 Mejora la transmisión de conocimiento entre personas, equipos y departamentos	Práctica	Como se puede observar en el **Anexo A** la actividad **3.7.2** del proceso **3.7** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** pero se considera crear un práctica para transferir los conocimientos entre los miembros de la empresa, inculcando el registro de la información con el propósito de mejorar la cultura de aprendizaje del personal y mejorar el conocimiento de la posesión y propietarios de la información.
3.7.3 Gestionar la información para certificar su calidad y utilidad.	Sin Acción	Como se puede observar en el **Anexo 1** existe una actividad que cumple con la función de la actividad **3.7.3** propuesta por el proceso **3.7** de **ITIL V3:2011**, la actividad (3) del proceso **DSS01.01 "Realizar procedimientos operacionales"** que propone COBIT 5, por esta razón no se la puede considerar actividad, ni práctica.
3.7.4 Uso del Sistema de Gestión del Conocimiento del Servicio (SKMS)	Práctica	Como se puede observar en el **Anexo A** la actividad **3.7.4** del proceso **3.7** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** pero se considera crear un práctica para mantener en un repositorio de todos los documentos generados por los demás procesos.

Cuadro 13. (Continuación)

Fase: Operación		
Proceso:	**4.1 Gestión de Eventos**	
Actividades	**Tipo de Limitación**	**Justificación**
4.1.1 Notificación de eventos	Sin Acción	Como se puede observar en el **Anexo A** la cumple con la actividad **(1)** de la práctica **DSS05.07 "Supervisar la infraestructura para eventos relacionados con la seguridad",** que propone COBIT 5, por esta razón no se la puede considerar actividad, ni práctica.
4.1.2 Detección y filtrado de eventos	Sin Acción	Como se puede observar en el **Anexo A** la cumple con la actividad **(1)** de la práctica **DSS01.03 "Supervisar la infraestructura de TI"** que propone COBIT 5, por esta razón no se la puede considerar actividad, ni práctica.
4.1.3 Clasificación de eventos	Sin Acción	Como se puede observar en el **Anexo A** la actividad **4.1.3** del proceso de **ITIL V3:2011,** cumple en parte la actividad **(1)** de la práctica **DSS01.03 "Supervisar la infraestructura de TI"**, que propone COBIT 5, pero no es considerada como actividad, porque la actividad **4.1.4** del proceso de **ITIL V3:2011** tienen un mayor alcance.
4.1.4 Correlación	Actividad	Como se puede observar en el **Anexo A** la actividad **4.1.4** del proceso de **ITIL V3:2011,** cumple con el contexto de la práctica **DSS01.03 "Supervisar la infraestructura de TI"**, que propone COBIT 5, por ello se considera crear una actividad para dimensionar la importancia del evento y establecer conexiones con otros con el fin de ahorrar tiempo en la búsqueda de soluciones.

Cuadro 13. (Continuation)

Fase:	Operación	
Proceso:	**4.1 Gestión de Eventos**	
4.1.5 Disparadores	Sin Acción	Como se puede observar en el **Anexo A** cumple con la actividad **(1)** de la práctica **DSS01.03 "Supervisar la infraestructura de TI"** que propone COBIT 5, por esta razón no se la puede considerar actividad, ni práctica.
Proceso:	**4.2 Gestión de Incidencias**	
Actividades	**Tipo de Limitación**	**Justificación**
4.2.1 Registro y clasificación	Sin Acción	Como se puede observar en el **Anexo A** cumple con la actividad **(6)** de la práctica **DSS01.03 "Supervisar la infraestructura de TI" y** la actividad **(5)** de la práctica **DSS05.07 "Supervisar la infraestructura para eventos relacionados con la seguridad"** que propone COBIT 5, por esta razón no se la puede considerar actividad, ni práctica.
4.2.2 Análisis, resolución y cierre	Sin Acción	Como se puede observar en el **Anexo A** cumple con la actividad **(9)** de la práctica **DSS01.05 "Manejo de las instalaciones"** que propone COBIT 5, por esta razón no se la puede considerar actividad, ni práctica.

Cuadro 13. (Continuación)

Fase: Operación		
Proceso:	**4.3 Gestión de Peticiones**	
Actividades	**Tipo de Limitación**	**Justificación**
4.3.1 Selección de Peticiones	Sin Acción	Como se puede observar en el **Anexo A** cumple con la actividad **(3)** de la práctica **DSS01.03 "Supervisar la infraestructura de TI" y** la actividad **(1)** de la práctica **DSS05.05 "Administrar el acceso físico a los activos de TI."** que propone COBIT 5, por esta razón no se la puede considerar actividad, ni práctica.
4.3.2 Aprobación financiera	Práctica	Como se puede observar en el **Anexo A** la actividad **4.3.2** del proceso **4.3** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** pero se considera costos para aquellas peticiones que requieran de algún gasto fuera del curso normal financiero; permitiendo decidir si se tramita la petición o no. Se pueden establecer costos fijos para peticiones estándar predefinidas, la cual no cumple con el contexto analizado en los procesos DSS01 y DSS05 que propone COBIT 5; esto se debe a que el contenido general de este marco de referencia en ninguna de sus prácticas propone una aprobación financiera.
4.3.3 Tramitación y cierre	Sin Acción	Como se puede observar en el **Anexo A** la actividad **4.3.3** del proceso **4.3** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** ni con el contexto de las mismas.

Cuadro 13. (Continuación)

Fase: Operación		
Proceso: **4.4 Gestión de Problemas**		
Actividades	**Tipo de Limitación**	**Justificación**
4.4.1 Control de Problemas	Sin Acción	Como se puede observar en el **Anexo A**, la actividad **4.4.1** del proceso **4.4** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** ni con el contexto de las mismas.
4.4.2 Control de Errores	Sin Acción	Como se puede observar en el **Anexo A**, la actividad **4.4.2** del proceso **4.4** de **ITIL V3:2011,** no tiene relación con ninguna de actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** ni con el contexto de las mismas.
Proceso: **4.5 Gestión de Acceso a los Servicios TI**		
Actividades	**Tipo de Limitación**	**Justificación**
4.5.1 Verificación	Sin Acción	Como se puede observar en el **Anexo A** cumple con la actividad **(1, 2, 6 ,7)** de la práctica **DSS05.04 "Manejo de la identidad del usuario y el acceso lógico"** y con la actividad **(2)** la práctica **DSS05.05 Administrar el acceso físico a los activos de TI** que propone COBIT 5, por esta razón no se la puede considerar actividad, ni práctica.
4.5.2 Monitorización de identidad	Sin Acción	Como se puede observar en el **Anexo A** cumple con la actividad **(4)** de la práctica **DSS05.04 "Manejo de la identidad del usuario y el acceso lógico** que propone COBIT 5, por esta razón no se la puede considerar actividad, ni práctica.

Cuadro 13. (Continuación)

Fase: Operación		
Proceso:	**4.5 Gestión de Acceso a los Servicios TI**	
4.5.3 Registro y monitorización de acceso	Sin Acción	Como se puede observar en el **Anexo A** cumple con la actividad **(8)** de la práctica **DSS05.04 "Manejo de la identidad del usuario y el acceso lógico** que propone COBIT 5, por esta razón no se la puede considerar actividad, ni práctica.
4.5.4 Eliminación y restricción de derechos	Sin Acción	Como se puede observar en el **Anexo A** cumple con la actividad **(4)** de la práctica **DSS05.04 "Manejo de la identidad del usuario y el acceso lógico** que propone COBIT 5, por esta razón no se la puede considerar actividad, ni práctica.
Fase: Mejora		
Proceso:	**4.1 Gestión de Eventos**	
Actividades	**Tipo de Limitación**	**Justificación**
5.1 Proceso de mejorar CSI	Sin Acción	No se considera al proceso 5.1 de **ITIL V3:2011** para los procesos DSS01, ni DSS05 debido a que estas actividades no entran en el contexto de los procesos DSS01 y DSS06 que propone COBIT 5, por esta razón sus actividades no se las puede considerar como una nueva actividad o práctica.
5.2 Proceso de mejorar CSI	Sin Acción	No se considera al proceso 5.2 de **ITIL V3:2011** para los procesos DSS01, ni DSS05 debido a que estas actividades no entran en el contexto de los procesos DSS01 y DSS06 que propone COBIT 5, por esta razón sus actividades no se las puede considerar como una nueva actividad o práctica.

Fuente: Elaboración Propia

Cuadro 14. Limitaciones de los controles de ISO 27001:2005 hacia el marco de referencia COBIT 5.

Objetivo: A.10 Gestión de las comunicaciones y las operaciones		
Controles	**Tipo de Limitación**	**Justificación**
A.10.1.1 Procedimientos de operación documentados	Enfoque	Como se puede observar en el **Anexo B** el control **A.10.1.1** de ISO 27001:2005**,** cumple en parte la actividad **(1)** de la práctica **DSS01.01 "Realizar procedimientos operacionales"**, que propone COBIT 5, por ello se considera crear una actividad para documentar las operaciones y mantener dicha información disponible a los usuarios que lo necesiten [14].
A.10.1.3 Segregación de deberes.	Actividad	Como se puede observar en el **Anexo B** el control **A.10.1.3** de **ISO 27001:2005,** cumple en parte la actividad **(1)** de la práctica **DSS01.01 "Realizar procedimientos operacionales"**, que propone COBIT 5, por ello se considera crear una actividad para separar las tareas y áreas de responsabilidad entre los usuarios involucrados en las operaciones [14].
A.10.10.2 Uso del sistema de monitoreo	Enfoque	Como se puede observar en el **Anexo B** el control **A.10.1.3** de **ISO 27001:2005**, cumple en parte la actividad **(1)** de la práctica **DSS01.01 "Realizar procedimientos operacionales"**, que propone **COBIT 5,** esta actividad se refiere a desarrollar y mantener procedimientos y actividades de apoyo a los servicios, por lo que su función queda muy generalizada, por esta razón se considera mejorar el enfoque, aquejando el enfoque del control **A.10.10.2** de **ISO 27001:2005,** que trata establecer procedimientos para

		monitorear el uso de los sistemas de procesamiento [14].
Objetivo: A.11 Control de Acceso		
Controles	**Tipo de Limitación**	**Justificación**
A.11.2.1 Inscripción del usuario	Enfoque	Como se puede observar en el **Anexo B** el control **A.11.2.1** de **ISO 27001:2005**, cumple en parte la actividad **(7)** de la práctica **DSS05.05 "Administrar el acceso físico a los activos de TI."**, que propone **COBIT 5,** esta actividad se refiere a regular la conducta de los usuarios mediante una formación de conciencia de seguridad física, por lo que su función queda muy generalizada, por esta razón se considera mejorar el enfoque, aquejando el enfoque del control **A.11.2.1** de **ISO 27001:2005,** que trata establecer procedimientos formales de la inscripción y des-inscripción para conceder acceso a todos los sistemas de información [14].
A.11.3.1 Uso de clave	Enfoque	Como se puede observar en el **Anexo B** el control **A.11.3.1** de **ISO 27001:2005**, cumple en parte la actividad **(1)** de la práctica **DSS01.01 "Realizar procedimientos operacionales"**, que propone **COBIT 5,** esta actividad se refiere a desarrollar y mantener procedimientos y actividades de apoyo a los servicios, por lo que su función queda muy generalizada, por esta razón se considera mejorar el enfoque, aquejando el enfoque del control **A.11.3.1** de **ISO 27001:2005,** que trata de requerir a los usuarios seguir con buenas prácticas para la selección y uso de claves [14].

Cuadro 14. (Continuación)

Objetivo: A.11 Control de Acceso		
Controles	**Tipo de Limitación**	**Justificación**
A.11.3.2 Equipo de usuario desatendido	Enfoque	Como se puede observar en el **Anexo B** el control **A.11.3.2** de **ISO 27001:2005**, cumple en parte la actividad **(1)** de la práctica **DSS01.01 "Realizar procedimientos operacionales"**, que propone **COBIT 5,** esta actividad se refiere a desarrollar y mantener procedimientos y actividades de apoyo a los servicios, por lo que su función queda muy generalizada, por esta razón se considera mejorar el enfoque, aquejando el enfoque del control **A.11.3.2** de **ISO 27001:2005,** que trata de requerir a los usuarios se aseguren de dar protección al equipo desatendido [14].
A.11.5.5 Sesión inactiva	Enfoque	Como se puede observar en el **Anexo B** el control **A.11.5.5** de **ISO 27001:2005**, cumple en parte la actividad **(2)** de la práctica **DSS01.01 "Realizar procedimientos operacionales"**, que propone **COBIT 5,** esta actividad se refiere mantener horarios de las actividades operacionales, por esta razón se considera mejorar el enfoque, aquejando el enfoque del control **A.11.5.5** de **ISO 27001:2005,** que trata de establecer el cierre a las sesiones inactivas en un periodo determinado [14].

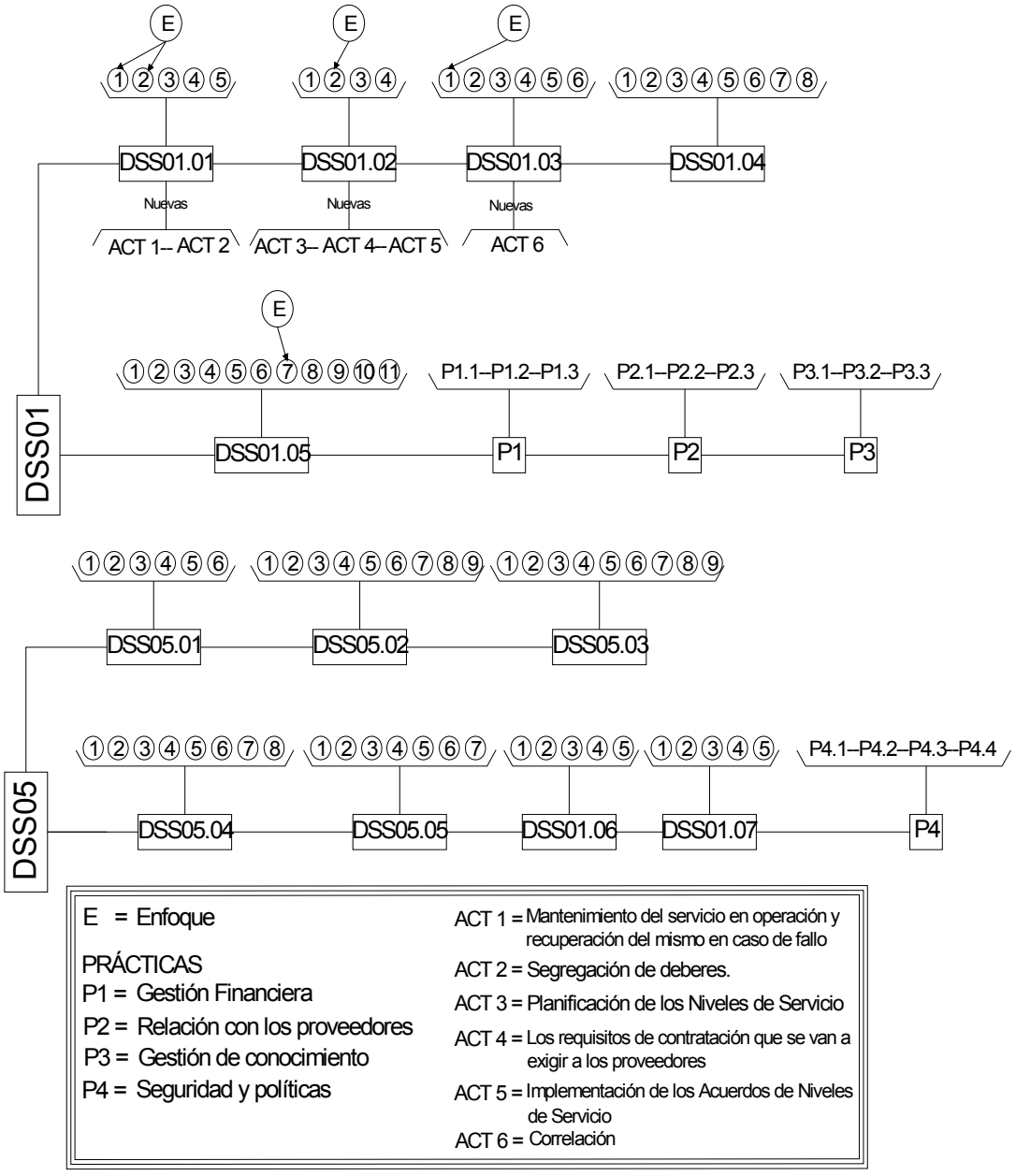
Cuadro 14. (Continuación)

Objetivo: A.11 Control de Acceso		
Controles	**Tipo de Limitación**	**Justificación**
A.11.5.6 Limitación de tiempo de conexión	Enfoque	Como se puede observar en el **Anexo B** el control **A.11.5.5** de **ISO 27001:2005**, cumple en parte la actividad **(2)** de la práctica **DSS01.01 "Realizar procedimientos operacionales"**, que propone **COBIT 5,** esta actividad se refiere mantener horarios de las actividades operacionales, por esta razón se considera mejorar el enfoque, aquejando el enfoque del control **A.11.5.5** de **ISO 27001:2005,** que trata de establecer restricciones de tiempos de conexión a las aplicaciones de alto riesgo [14].
A.11.7.1 Computación móvil y comunicaciones	Práctica	Como se puede observar en el **Anexo B** el control **A.11.7.1** de **ISO 27001:2005,** no tiene relación con ninguna de la actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** pero se considera crear una práctica para el proceso **DSS05** para establecer políticas formales sobre el riesgo del uso de medios de computación y comunicación móviles [14].
A.11.7.2 Tele-trabajo	Práctica	Como se puede observar en el **Anexo B** el control **A.11.7.2** de **ISO 27001:2005,** no tiene relación con ninguna de la actividades de las prácticas de los procesos **DSS01 y DSS05** que propone **COBIT 5,** pero se considera crear una práctica para el proceso **DSS05** para establecer políticas formales sobre para procedimientos de actividades de tele-trabajo [14].

Fuente: Elaboración Propia

2.4.1 Diseño del modelo de Gestión de Operaciones y Servicios de Seguridad para tecnologías de información integrando COBIT 5, ITILV3:2011 E ISO 27001:2005

Figura 12. Modelo de Gestión de Operaciones y Servicios de Seguridad



Fuente: Elaboración Propia

2.4.2 Explicación del modelo de Gestión de Operaciones y Servicios de Seguridad para tecnologías de información integrando COBIT 5, ITILV3:2011 E ISO 27001:2005

Para objeto de este trabajo se considera la siguiente terminología:

- *Proceso.-* es el ámbito en que se concentra el modelo, en este caso es la Gestión de Operaciones y la Gestión de Servicios de Seguridad.
- *Practica.-* es un conjunto de actividades que se enfocan a proteger o dar solución a una determinada área.
- *Enfoque.-* se refiere a la propuesta de actividades que pueden ser usadas por una actividad de COBIT 5, que posee un cierto grado de ambigüedad.

PROCESO.- DSS01 Gestión de Operaciones

Para este proceso de COBIT 5, se han agregado ciertos enfoques, actividades y prácticas para reforzar el proceso de gestión de operaciones en las empresas.

→ **Enfoque**

Práctica.- DSS01.01 Realizar procedimientos operacionales.

- *1 Desarrollar y mantener procedimientos de funcionamiento y actividades relacionadas con el apoyo de todos los servicios prestados.-* Se considera mejorar el enfoque de esta práctica, tomando en consideración actividades existentes en ITILV3:2011 e ISO 27001:2005 esclarecer su propósito, puesto que su contexto posee un cierto grado de ambigüedad; dichas actividades pueden ser las siguientes:

  A.10.1.1 Procedimientos de operación documentados

  A.10.10.2 Uso del sistema de monitoreo

  A.11.3.1 Uso de clave

  A.11.3.2 Equipo de usuario desatendido

Práctica.- DSS01.01 Realizar procedimientos operacionales.

- *2 Mantener un horario de las actividades operacionales, lleve a cabo las actividades y gestionar el rendimiento y el rendimiento de las actividades programadas.-* Se considera mejorar el enfoque de esta práctica, tomando en consideración actividades existentes en ITILV3:2011 e ISO 27001:2005 esclarecer su propósito, puesto que su contexto posee un cierto grado de ambigüedad; dichas actividades pueden ser las siguientes:

A.11.5.5 Sesión inactiva

A.11.5.6 Limitación de tiempo de conexión

→ **Actividades**

Se ha analizado agregar actividades a cada una de las siguientes prácticas:

Práctica.- DSS01.01 Realizar procedimientos operacionales.

ACT 1. 2.4.3 *Mantenimiento del servicio en operación y recuperación del mismo en caso de fallo*.- Se ha considerado que esta actividad, perteneciente a ITILV3:2011 debido a que la práctica de COBIT 5 se refiere a llevar a cabo procedimientos y tareas operativas, de forma fiable y confiable, por lo cual al incorporar esta actividad en la práctica DSS01.01 se refuerza su propósito, y por ende, permitir la recuperación de los servicios en un corto periodo de tiempo minimizando sus interrupciones por incidencias o tareas de mantenimiento proyectadas.

ACT 2. *A.10.1.3 Segregación de deberes.-* Se ha considerado que esta actividad, perteneciente a ISO 27001:2005 debido a que la práctica de COBIT 5 se refiere a llevar a cabo procedimientos y tareas operativas, de forma fiable y confiable, por lo cual al implementar esta actividad en la práctica DSS01.01, con el propósito de reforzar las actividades existentes y por ende, permitir la repartición de las tareas y áreas de responsabilidad entre los usuarios involucrados en las operaciones.

Práctica.- DSS01.02 Gestionar los servicios de TI externalizados.

ACT 3. *2.2.1 Planificación de los Niveles de Servicio.-* Se ha considerado que esta actividad, perteneciente a ITILV3:2011 debido a que la práctica de COBIT 5 se refiere al manejo de la gestión de servicios externalizados, asegurando la protección de la información y confiabilidad de la prestación de servicios, por lo cual al incorporar esta actividad en la práctica DSS01.02, se refuerza su propósito, y por ende, permite proyectar los requisitos de los niveles de servicio, en base a las necesidades y expectativas de nivel de servicio de la empresa, mediante la elaboración de hojas de

especificación, que ayuden a determinar a las empresas los procesos que pueden ser externalizados.

ACT 4. 2.7.1 Los requisitos de contratación que se van a exigir a los proveedores.- Se ha considerado que esta actividad, perteneciente a ITILV3:2011 debido a que la práctica de COBIT 5 se refiere al manejo de la gestión de servicios externalizados, asegurando la protección de la información y confiabilidad de la prestación de servicios, por lo cual al incorporar esta actividad en la práctica DSS01.02, se refuerza su propósito, y por ende, permita analizar las estrategias generales de la organización y los servicios que presta, para definir sus necesidades de contratación.

ACT 5. 2.2.2 Implementación de los Acuerdos de Niveles de Servicio.- Se ha considerado que esta actividad, perteneciente a ITILV3:2011 debido a que la práctica de COBIT 5 se refiere al manejo de la gestión de servicios externalizados, asegurando la protección de la información y confiabilidad de la prestación de servicios, por lo cual al incorporar esta actividad en la práctica DSS01.02, se refuerza su propósito, y por ende, permita llevar a cabo el proceso de negociación, elaboración de acuerdos y contratos.

Práctica.- DSS01.03 Supervisar la infraestructura TI.

ACT 6. 1.1.4 Correlación.- Implementación de los Acuerdos de Niveles de Servicio.- Se ha considerado que esta actividad, perteneciente a ITILV3:2011 debido a que la práctica de COBIT 5 se refiere a la supervisión de la infraestructura TI, y el almacenamiento de la información sobre las operaciones para su posterior revisión y análisis de sus secuencias de tiempo de las operaciones, por lo cual al incorporar esta actividad en la práctica DSS01.03, se refuerza su propósito, y por ende, permita dimensionar la importancia del evento y establecer conexiones con otros con el fin de ahorrar tiempo en la búsqueda de soluciones.

→ **Creación de Prácticas.**

Se ha determinado agregar las siguientes prácticas con sus respectivas actividades.

- Se considera crear una práctica para la Gestión Financiera, puesto que, en ninguno de los procesos analizado de COBIT 5 se plantea actividades referentes a la administración financiera para llevar a cabo las operaciones, tal y como se describe a continuación:

Cuadro 15. Práctica P1. Gestión financiera

P1.	**Gestión financiera**
P1.1	1.1.1 Presupuesto
P1.2	1.1.2 Contabilidad
P1.3	4.3.2 Aprobación financiera
Fuente: ITIL V3:2011 [5]	

Las actividades que se consideraron para esta nueva práctica fueron tomadas de ITILV3:2011; cada una de ellas cumplen una tarea específica.

P1.1 Consiste en llevar a cabo presupuestos para las tecnologías de información que serán aplicadas a las operaciones de la empresa.

P1.2 Consiste en realizar el control de la contabilidad en base a coste reales de TI.

P1.3 Se encarga del análisis de costos para aquellas peticiones de cambio que requieran de algún gasto fuera del presupuestado; permitiendo decidir si se tramita la petición o no. Se pueden establecer costos fijos para peticiones estándar predefinidas o de mayor ocurrencia.

- Se considera crear una práctica para la Relación con los proveedores, puesto que, en ninguno de los procesos analizados de COBIT 5 en este trabajo se plantea el registro de las actividades y comunicación, entre las empresas y proveedores de servicios a cabo las operaciones tal y como se describe a continuación:

Cuadro 16. Práctica P2.Relación con los proveedores

P2.	**Relación con los proveedores**
P2.1	2.7.2 Los procesos de evaluación y selección de proveedores
P2.2	2.7.3 La clasificación y documentación de la relación con los proveedores
P2.3	2.7.5 Renovación o terminación
Fuente: Basado en ITIL V3:2011 [5]	

Las actividades que se consideraron para esta nueva práctica fueron tomadas de ITILV3:2011; cada una de ellas cumplen una tarea específica.

P2.1 consiste en el proceso que deben realizar las empresas para la elección de un proveedor acorde con los requisitos de la empresa, tomando en cuenta sus referencias, capacidad, disponibilidad y el financiamiento del cual dispone actualmente la empresa**.**

P2.2 consiste en crear una base de datos que reúna información de los proveedores, contratos, nivel de atención y su relación con otros procesos de gestión.

P2.3 Se encarga de asesorar a los directivos sobre la renovación o terminación de contratos de los proveedores, considerando su rendimiento, perspectivas de crecimiento de la empresa y cumplimiento de contrato

- Se considera crear una práctica para la Gestión de conocimiento, puesto que, en ninguno de los procesos analizados de COBIT 5 en este trabajo se plantea actividades estratégicas para la trasferencia y organización de conocimiento entre los miembros de la empresa, tal y como se describe a continuación:

Cuadro 17. Práctica P3.Gestión de conocimiento

P3.	**Gestión de conocimiento**
P3.1	3.7.1 Puntualizar una estrategia de Gestión del Conocimiento y divulgarla a toda la empresa [5].
P3.2	3.7.2 Mejora la transmisión de conocimiento entre personas, equipos y departamentos [5].
P3.3	3.7.4 Uso del Sistema de Gestión del Conocimiento del Servicio (SKMS)
Fuente: Basado en ITIL V3:2011 [5]	

Las actividades que se consideraron para esta nueva práctica fueron tomadas de ITILV3:2011; cada una de ellas cumplen una tarea específica.

P3.1 consiste en definir, desarrollar y difundir una estrategia de conocimiento en la que se reflejen las, roles, procedimientos de registro y validación de información.

P3.2 consiste en transferir los conocimientos entre los miembros de la empresa, inculcando el registro de la información con el propósito de mejorar la cultura de aprendizaje del personal y mejorar el conocimiento de la posesión y propietarios de la información, poniendo en práctica la estrategia del conocimiento.

P3.3 consiste en establecer un repositorio de todos los documentos generados por las demás prácticas.

PROCESO.- DSS01 Gestión de Servicios de Seguridad

Para este proceso de COBIT 5, una práctica para reforzar el proceso de gestión de servicios de seguridad en las empresas.

→ **Creación de Práctica**

Se ha determinado agregar la siguiente práctica con sus respectivas actividades.

- Se considera crear una práctica para la Gestión Financiera, puesto que, en ninguno de los procesos analizado de COBIT 5 se plantea actividades referentes a la administración financiera para llevar a cabo las operaciones, tal y como se describe a continuación:

Cuadro 18. Práctica P4.Seguridad y Políticas

P4.	**Seguridad y Políticas**
P4.1	2.6.1 Constituya política de seguridad que oriente a la empresa
P4.2	2.6.2 Realizar un Plan de Seguridad que integre los límites de seguridad adecuados descritos en los acuerdos de servicio firmados con proveedores internos y externo.
P4.3	A.11.7.1 Computación móvil y comunicaciones
P4.4	A.11.7.2 Tele-trabajo
Fuente: Basado en ITIL V3:2011 [5] e ISO 27001:2005 [14]	

Las actividades que se consideraron para esta nueva práctica fueron tomadas de ITILV3:2011 e ISO 27001:2005; cada una de ellas cumplen una tarea específica.

P4.1 Consiste en establecer una política global y clara sobre la seguridad, en donde se fijen aspectos tales como los objetivos, responsabilidades y recursos.

P4.2 Consiste en fijar los niveles de seguridad que han de ser incluidos como parte de los ANS, OLAs y UCs, incluyendo métricas o indicadores para evaluar los niveles de seguridad

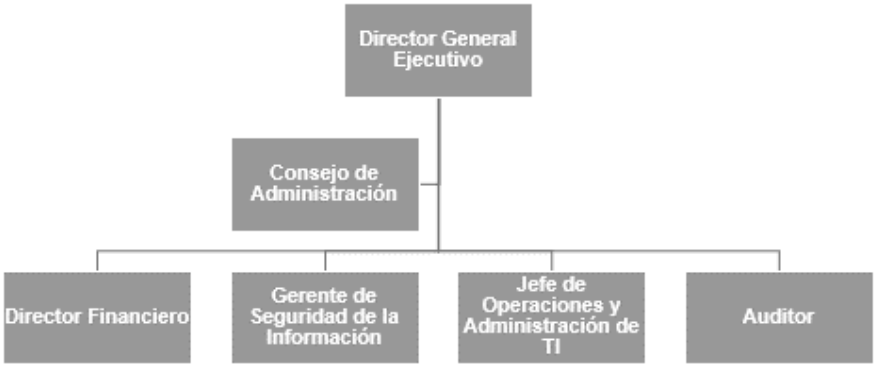
P4.3 Consiste en establecer políticas formales sobre el peligro de la utilización de medios de computación y comunicación móviles[14].

P4.4 Consiste en establecer políticas formales sobre procedimientos de actividades de tele-trabajo [14].

2.5 **Ejecución y/o ensamblaje del prototipo.**

Para el ensamblaje del modelo de gestión se crea una estructura organizativa basada en roles aplicados por COBIT 5.

Figura 13. Estructura organizativa basada en roles propuestos por COBIT 5



Fuente: ISACA, [53]

2.5.1 Descripción de los roles de la estructura

Director General Ejecutivo.- Es el ejecutivo con más alto rango encargado de la gestión y dirección administrativa, cuyas responsabilices son informar a los agentes internos y externos los objetivos y logros de la empresa, organizar, dirigir, controlar, motivar y contratar al personal adecuado para cada una de las áreas de la empresa.

Consejo de administración.- Consiste en un grupo de personas que tienen el control total de los recursos entre ellos se encuentran ejecutivos de un alto cargo, incluyendo a directores no ejecutivos, consultores y representantes de los proveedores de servicios.

Director Financiero (CFO).- Es la persona a cargo de la gestión financiera, cuya responsabilidad consiste en planificar, ejecutar e informar el estado financiero de la empresa.

Jefe de operaciones y administración TI.- Es el ejecutivo responsable de la infraestructura y administración de las tecnologías de información, además de llevar el registro de las actividades diarias de la TI, cuyos reportes presenta directamente al director ejecutivo.

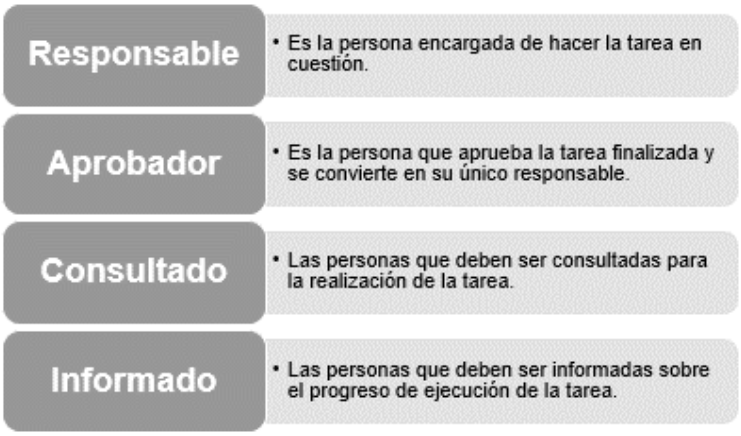
Gerente de Seguridad de la Información.- Es el ejecutivo encargado de gestionar, diseñar, supervisar y/o evaluar la seguridad de la información de la empresa.

Auditor.- Es el responsable de proveer auditorías internas al área de tecnologías de Información y servicios de TI.

2.5.2 Asignación de responsabilidades

ITIL facilita un modelo de asignación de responsabilidades, mejorando la organización de las tareas o actividades para que se realicen con éxito, este modelo llamado RACI (también llamado matriz de asignación de responsabilidades) es el acrónimo de [58]:

Figura 14: Responsabilidades propuestas por ITIL



Fuente: Elaboración Propia, basada en [58]

En cada tarea debe haber un único R y A. Si esto no fuera así la tarea se subdividirá hasta que así sea. Por supuesto una persona puede ser, a priori, R o A en múltiples tareas [58].

2.5.3 *Matriz RACI.-* Para que exista una gestión organizada de las operaciones de deben asigna las responsabilidades de los miembros de una empresa, de este modo se evitan confusiones sobre quiénes son los encargados, responsables, consultados e informados, dentro de la pirámide estructural de una empresa. La realización de esta asignación de responsabilidades es tomada de la matriz de asignaciones sugerida por ITIL denominada RACI.

Cuadro 19. Relación entre los roles y actividades

	Actividades / Roles	Director General Ejecutivo	Consejo de Administración	Director Financiero	Gerente de Seguridad de la Información	Jefe de Operaciones y Administración de TI	Auditor
1	Mantenimiento del servicio en operación y recuperación del mismo en caso de fallo	A	C/I	I	C	R	I
2	Segregación de deberes.	A/C	C/I	I	C	R	I
3	Planificación de los Niveles de Servicio	A	C/I	I	C	R	I
4	Los requisitos de contratación que se van a exigir a los proveedores	A/C	C/I	C	C	R	I
5	Implementación de los Acuerdos de Niveles de Servicio	A	I	C	C	R	i
6	Correlación	A	I	C	C	R/A	I
7	Presupuesto	A/I	I	R	C	C/I	I
8	Contabilidad	A/I	I	R	C	C	I
9	Aprobación financiera	C/I	C/I	R/A	C	C	I
10	Los procesos de evaluación y selección de proveedores	A/C	I	C	I	R	C
11	La clasificación y documentación de la relación con los proveedores	A/I	C/I	C	C	R	I
12	Renovación o terminación	R/A	C/I	C	C	C/I	I
13	Puntualizar una estrategia de Gestión del Conocimiento y divulgarla a toda la empresa	I/A	C/I	I	C	R	C/I
14	Mejora la transmisión de conocimiento entre personas, equipos y departamentos	I	I	I	C	R/A	I
15	Uso del Sistema de Gestión del Conocimiento del Servicio (SKMS)	I	C/I	C	C	R/A	C/I
16	Constituya política de seguridad que oriente a la empresa	A/I	C/I	I	R	C	C/I
17	Realizar un Plan de Seguridad que integre los límites de seguridad adecuados descritos en los acuerdos de servicio firmados con proveedores internos y externo	A	C/I	I	R	C/I	C
18	Computación móvil y comunicaciones	A/C	C/I	I	R	C/I	C/I
19	Tele-trabajo	A/C	C/I	I	R	C/I	C/I

Fuente: Elaboración Propia

Justificación de la Matriz RACI.- Las actividades anteriormente mencionadas se encuentran divididas entre las prácticas propuestas por COBIT 5 y las nuevas prácticas planteadas en este trabajo. A continuación se detallan las responsabilidades de cada uno de los roles de la estructura organizativa en las nuevas actividades:

En la actividad 1 **"Mantenimiento del servicio en operación y recuperación del mismo en caso de fallo".**-Se asigna como responsable (R) al Jefe de Operaciones y Administración de TI, quien será el encargado de ejecutar esta actividad y recibirá apoyo del Gerente de Seguridad de la Información (C) y Consejo de Administración (C/I), en el caso de necesitar información, pueden ser consultados sobre los horarios de en los que se puede realizar esta actividad, con el propósito de evitar la interrupción de las actividades diarias de la empresa, luego se pedirá la aprobación al Director General Ejecutivo (A); una vez aprobada la actividad se procederá a informar al Director Financiero, Consejo de Administración y Auditor, con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

En la actividad 2 **"Segregación de deberes".-**Se asigna como responsable (R) al Jefe de Operaciones y Administración de TI, quien será el encargado de ejecutar esta actividad y recibirá apoyo del Gerente de Seguridad de la Información (C), Consejo de Administración (C/I) y Director General Ejecutivo (A/C), en el caso de necesitar información, pueden ser consultados sobre la contratación de nuevo personal, objetivos de la empresa o cambio de proveedores de servicios; luego se pedirá la aprobación al Director General Ejecutivo (A/C); una vez aprobada la actividad se procederá a informar al Director Financiero, Consejo de Administración y Auditor, con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

En la actividad 3 **"Planificación de los Niveles de Servicio"**.-Se asigna como responsable (R) al Jefe de Operaciones y Administración de TI, quien será el encargado de ejecutar esta actividad y recibirá apoyo del Gerente de Seguridad de la Información (C) y el Consejo de Administración (C/I, en el caso de necesitar información, pueden ser consultados sobre el resguardo de recursos sensibles para el funcionamiento normal de la empresa y que actividades requieren externalización; luego se pedirá la aprobación al Director General Ejecutivo (A); una vez aprobada la actividad se procederá a informar al Director Financiero, Consejo de Administración y Auditor, con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

En la actividad 4 **“Los requisitos de contratación que se van a exigir a los proveedores”.-**Se asigna como responsable (R) al Jefe de Operaciones y Administración de TI, quien será el encargado de ejecutar esta actividad y recibirá apoyo del Gerente de Seguridad de la Información (C), Consejo de Administración (C/I), Director Financiero (C) y Director General Ejecutivo (A/C), en el caso de necesitar información, pueden ser consultados sobre las estrategias generales de la empresa; luego se pedirá la aprobación al Director General Ejecutivo (A); una vez aprobada la actividad se procederá a informar al Consejo de Administración y Auditor, con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

En la actividad 5 **“Implementación de los Acuerdos de Niveles de Servicio”.-**Se asigna como responsable (R) al Jefe de Operaciones y Administración de TI, quien será el encargado de ejecutar esta actividad y recibirá apoyo del Gerente de Seguridad de la Información (C) y el Director Financiero (C), en el caso de necesitar información, pueden ser consultados sobre el presupuesto destinado a las TI, políticas de seguridad y el manejo diario de los recursos; luego se pedirá la aprobación al Director General Ejecutivo (A); una vez aprobada la actividad se procederá a informar al Consejo de Administración y Auditor, con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

En la actividad 6 **“Correlación”.-**Se asigna como responsable (R/A) al Jefe de Operaciones y Administración de TI, quien será el encargado de ejecutar esta actividad, aprobar y recibirá apoyo del Gerente de Seguridad de la Información (C) y el Director Financiero (C), en el caso de necesitar información, pueden ser consultados sobre el presupuesto destinado a las TI, políticas de seguridad, el manejo diario de los recursos y eventos suscitados con anterioridad, para determinar qué soluciones fueron aplicadas anteriormente; luego se pedirá la aprobación al Director General Ejecutivo (A); una vez aprobada la actividad se procederá a informar al Consejo de Administración y Auditor, con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

En la actividad 7 **“Presupuesto”.-**Se asigna como responsable (R) al Director Financiero, quien será el encargado de ejecutar esta actividad y recibirá apoyo del Gerente de Seguridad de la Información (C) y el Jefe de Operaciones y Administración de TI (C), en el caso de necesitar información, pueden ser consultados sobre los precios para la implementación herramientas o mecanismos para la seguridad y el manejo diario de los recursos; luego se pedirá la aprobación al Director General Ejecutivo (A/i); una

vez aprobada la actividad se procederá a informar al Consejo de Administración y Auditor, con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

En la actividad 8 **"Contabilidad".-**Se asigna como responsable (R) al Director Financiero, quien será el encargado de ejecutar esta actividad y recibirá apoyo del Gerente de Seguridad de la Información (C), el Director General Ejecutivo (C/I), el Jefe de Operaciones y Administración de TI (C) y el Consejo de Administración (C/I) en el caso de necesitar información, pueden ser consultados sobre los precios para la implementación herramientas o mecanismos para la seguridad, costos de servicios TI implementados en la empresa; luego se pedirá la aprobación al Director General Ejecutivo (A/I); una vez aprobada la actividad se procederá a informar al Consejo de Administración y Auditor, con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

En la actividad 9 **"Aprobación Financiera".-**Se asigna como responsable (R) al Director Financiero, quien será el encargado de ejecutar esta actividad y recibirá apoyo del Gerente de Seguridad de la Información (C), el Director General Ejecutivo (C/I), el Jefe de Operaciones y Administración de TI (C) y el Consejo de Administración (C/I) en el caso de necesitar información, pueden ser consultados sobre los precios para la implementación herramientas o mecanismos para la seguridad, costos de servicios TI implementados en la empresa; luego se pedirá la aprobación al Director General Ejecutivo (C/I); una vez aprobada la actividad se procederá a informar al Consejo de Administración y Auditor, con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

En la actividad 10 **"Los procesos de evaluación y selección de proveedores".-**Se asigna como responsable (R) al Director Financiero, quien será el encargado de ejecutar esta actividad y recibirá apoyo del Director General Ejecutivo (A/C), el Jefe de Operaciones y Administración de TI (C) y el Auditor (C) en el caso de necesitar información, pueden ser consultados sobre; luego se pedirá la aprobación al Director General Ejecutivo (A/C); una vez aprobada la actividad se procederá a informar al Consejo de Administración y al Gerente de Seguridad de la Información con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

En la actividad 11 **"La clasificación y documentación de la relación con los proveedores".-**Se asigna como responsable (R) al Jefe de Operaciones y Administración de TI, quien será el encargado de ejecutar esta actividad y recibirá apoyo

del Gerente de Seguridad de la Información (C), el Director Financiero (C) y el Consejo de Administración (C/I) en el caso de necesitar información, pueden ser consultados sobre, incidencias de seguridad, interrupción del servicio, contratos o costos de servicios TI implementados en la empresa; luego se pedirá la aprobación al Director General Ejecutivo (A/I); una vez aprobada la actividad se procederá a informar al Director General Ejecutivo (A/I), al Consejo de Administración (C/I) y al Auditor (I) con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

En la actividad 12 "**Renovación o terminación**".-Se asigna como responsable (R/A) al Director General Ejecutivo, quien será el encargado de ejecutar esta actividad y recibirá apoyo del Gerente de Seguridad de la Información (C), el Director Financiero (C), al Jefe de Operaciones y Administración de TI (C) y el Consejo de Administración (C/I) en el caso de necesitar información, pueden ser consultados sobre, incidencias de seguridad, interrupción del servicio (rendimiento), contratos o costos de servicios TI implementados en la empresa, condiciones de crecimiento empresarial, condiciones de renovación; luego se pedirá la aprobación al Director general Ejecutivo (A/I); una vez aprobada la actividad se procederá a informar al Consejo de Administración (C/I) y al Auditor (I) con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

En la actividad 13 "**Puntualizar una estrategia de Gestión del Conocimiento y divulgarla a toda la empresa**".-Se asigna como responsable (R) al Jefe de Operaciones y Administración de TI, quien será el encargado de ejecutar esta actividad y recibirá apoyo del Gerente de Seguridad de la Información (C/I), del Auditor (C/I) y del Consejo de Administración (C/I) en el caso de necesitar información, pueden ser consultados sobre, roles, procedimientos de registro y validación de información; luego se pedirá la aprobación al Director general Ejecutivo (I/A); una vez aprobada la actividad se procederá a informar al Consejo de Administración (C/I), Director Financiero (I) y al Auditor (C/I) con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

En la actividad 14 "**Mejora la transmisión de conocimiento entre personas, equipos y departamentos**".-Se asigna como responsable (R/A) al Jefe de Operaciones y Administración de TI, quien será el encargado de ejecutar y aprobar esta actividad; recibirá apoyo del Gerente de Seguridad de la Información (C), en el caso de necesitar información, pueden ser consultados sobre, roles, e información manejada por cada miembro de la empresa; luego se procederá a informar al Director general Ejecutivo (I),

Consejo de Administración (I), Director Financiero (I) y al Auditor (I) con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

En la actividad 15 "**Uso del Sistema de Gestión del Conocimiento del Servicio (SKMS)**".-Se asigna como responsable (R/A) al Jefe de Operaciones y Administración de TI, quien será el encargado de ejecutar y aprobar esta actividad; recibirá apoyo del Gerente de Seguridad de la Información (C), Consejo de Administración (C/I), Director Financiero (C) en el caso de necesitar información, pueden ser consultados sobre los informes e información manejada por cada miembro de la empresa; luego se procederá a informar al Director general Ejecutivo (I), Consejo de Administración (C/I) y al Auditor (C/I) con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

En la actividad 16 "**Constituya política de seguridad que oriente a la empresa**".-Se asigna como responsable (R) al Gerente de Seguridad de la Información, quien será el encargado de ejecutar esta actividad; recibirá apoyo del Jefe de Operaciones y Administración de TI (C), Consejo de Administración (C/I) y el Auditor (C/I) en el caso de necesitar información u opinión sobre la elaboración de la misma, con el propósito de no omitir, responsables ni funciones de seguridad; luego se procederá a informar al Director general Ejecutivo (A/I) quien será el encadado de la aprobación de la política de seguridad, al Consejo de Administración (C/I), Director Financiero (I) y al Auditor (C/I) con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

En la actividad 17 "**Realizar un Plan de Seguridad que integre los límites de seguridad adecuados descritos en los acuerdos de servicio firmados con proveedores internos y externo**".-Se asigna como responsable (R) al Gerente de Seguridad de la Información, quien será el encargado de ejecutar y esta actividad; recibirá apoyo del Jefe de Operaciones y Administración de TI (C/I), al Auditor (C) y al Consejo de Administración (C/I), en el caso de necesitar información, pueden ser consultados sobre los acuerdos de seguridad y contratos de servicios con los proveedores para la inclusión de medidas e indicadores de evaluación; luego se procederá a informar al Director general Ejecutivo (A) quien será el encargado de la aprobación, al Consejo de Administración (C/I) y Director Financiero (I) con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

En la actividad 18 “**Computación móvil y comunicaciones.**”.-Se asigna como responsable (R) al Gerente de Seguridad de la Información, quien será el encargado de ejecutar y aprobar esta actividad; recibirá apoyo del Jefe de Operaciones y Administración de TI (C/I), Consejo de Administración (C/I), al Auditor (C) y al Director general Ejecutivo (A/C) en el caso de necesitar información u opinión sobre la elaboración de políticas o normas que involucren el uso de computación móvil y comunicaciones. El Director general Ejecutivo (A/C) será el encargado de aprobar esta actividad, luego se procederá a informar al Consejo de Administración (C/I), al Director Financiero (I) al Jefe de Operaciones y Administración de TI (C/I) y al Auditor (C/I) con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

En la actividad 19 “**Tele-trabajo.**”.- Se asigna como responsable (R) al Gerente de Seguridad de la Información, quien será el encargado de ejecutar y aprobar esta actividad; recibirá apoyo del Jefe de Operaciones y Administración de TI (C/I), Consejo de Administración (C/I), al Auditor (C) y al Director general Ejecutivo (A/C) en el caso de necesitar información u opinión sobre la elaboración de políticas o normas que involucren el Tele-trabajo. El Director general Ejecutivo (A/C) será el encargado de aprobar esta actividad, luego se procederá a informar al Consejo de Administración (C/I), al Director Financiero (I) al Jefe de Operaciones y Administración de TI (C/I) y al Auditor (C/I) con el propósito de mantener una buena comunicación entre los miembros de la estructura organizativa sobre las actividades de la empresa.

3 EVALUACIÓN DEL PROTOTIPO

3.4 Plan de evaluación

Para llevar a cabo el proceso de evaluación del prototipo se estableció una técnica de recolección de datos y se seleccionó una muestra a la cual será aplicada dicha técnica.

3.2.1 Establecimiento de Técnica.- Para el levantamiento de la información se estableció como técnica de recolección de datos a la encuesta, por su facilidad de empleo, recolección y análisis de datos, además de ser considerada como una de las modalidades más utilizadas para sondear opiniones y la mayoría de las veces asociadas al proceso de muestreo [59].

3.2.2 Selección de la población y muestra.- Para la selección de la muestra se utilizó un método no probabilístico, ya que la elección de los elementos es arbitraria y basada en suposiciones sobre la población [60]; generalmente este método es usado cuando el objeto de estudio es de tipo cualitativo y existen limitantes de presupuesto, tiempo y mano de obra. De la técnica del método no probabilístico se escogió el muestreo de selección experta, el cual le permite al investigador realizar la selección de una muestra representativa, enfocándose en sus características y accesibilidad.

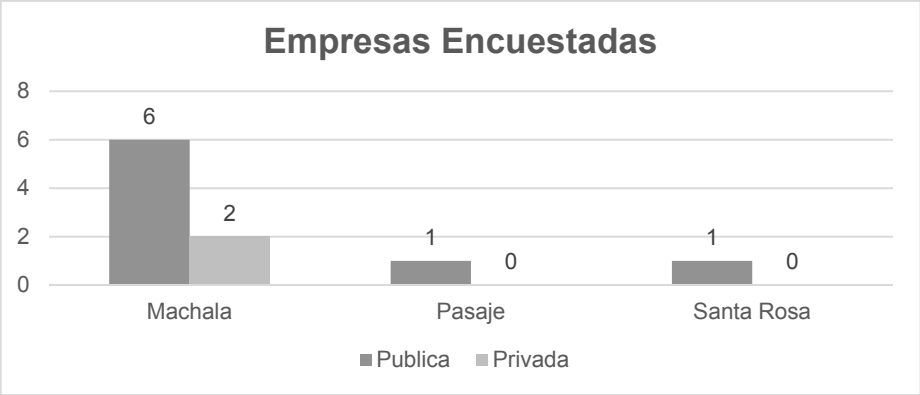
Tomando en cuenta el método de muestreo seleccionado es establece como población a las empresas, que cuenten con estructuras organizacionales, implementación de políticas, normas, estándares de seguridad, marcos de gobierno o gestión de las TI y constituidas legalmente en las ciudades de Machala, Pasaje y Santa Rosa pertenecientes a la Provincia de El Oro, por su cercanía y facilidad de acceso a los 10 expertos que se requieren para la evaluación de la propuesta.

Tabla 1. Empresas Encuestadas

	Pública	**Privada**	**Total**
Machala	6	2	8
Pasaje	1	0	1
Santa Rosa	1	0	1
Total	8	2	10

Fuente: Resultados de la Encuesta

Gráfico 1. Empresas Encuestadas



Fuente: Resultados de la Encuesta

*De las empresas seleccionadas en las ciudades de Machala, Pasaje y Santa Rosa, se puede determinar que 6 son públicas y 2 son privadas en la ciudad de Machala; y en las ciudades de Pasaje y Santa Rosa de analizó 1 empresa pública respectivamente.

3.2.3 Instrumento de Evaluación

El instrumento de evaluación presentara 10 preguntas con una serie de alternativas de respuestas extraídas de la escala clásica de Licker (5 opciones), por su rapidez y sencillez de aplicación, permitiendo la evaluación de la propuesta en base a los criterios de conformidad de la escala elegida (Ver Anexo 1). Para verificar que la encuesta es realizada a un experto; el instrumento cuenta con una sección en donde se solicita al encuestado su nombre, cargo, nombre de la empresa en la cual labora y el tipo de empresa.

3.3 Resultados de la evaluación

3.3.1 Análisis y presentación de resultados.

Después de la recolección de la información a través de la encuesta realizada a los expertos de las 10 empresas seleccionadas, se tabularon y analizaron las respuestas seleccionadas de cada una de las preguntas mediante tablas y gráficos estadísticos, con ayuda de la hoja de cálculo Microsoft Excel. A continuación se muestran los resultados:

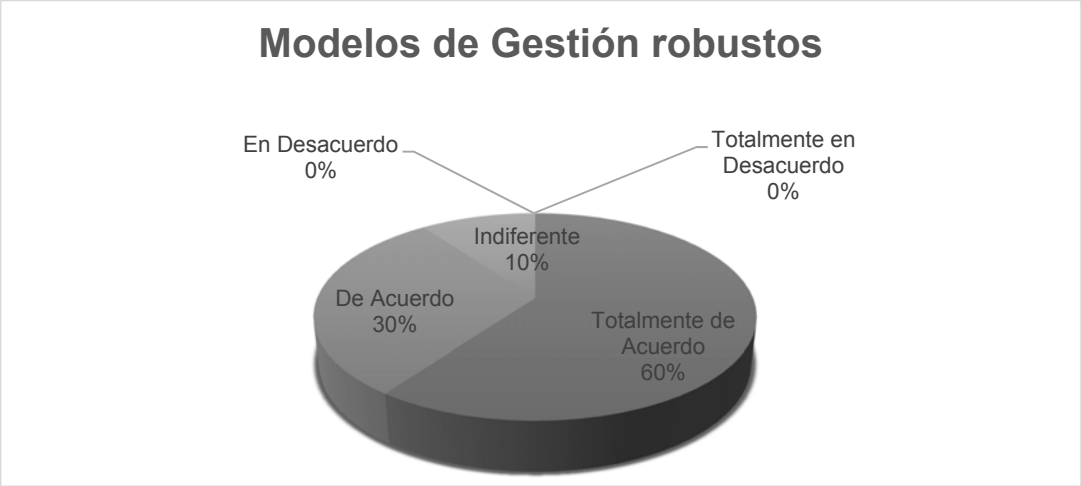
Pregunta 1: Considera usted que actualmente no existen modelos de gestión robustos para las operaciones y servicios de seguridad de las tecnologías de información?

Tabla 2. Modelos de Gestión robustos

Totalmente de Acuerdo	De Acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo	Total
60%	30%	10%	0%	0%	100%

Fuente: Resultados de la Encuesta

Gráfico 2. Modelos de Gestión robustos



Fuente: Resultados de la Encuesta

En lo que se refiere a esta pregunta, los resultados reflejan que el 60% de los expertos se encuentran totalmente de acuerdo, el 30% se consideran de acuerdo con respecto a que no existen modelos de gestión robustos para las operaciones y servicios de seguridad de las tecnologías de información, mientras que un 10% se muestra indiferente.

Por lo tanto de acuerdo a la opinión de los expertos, se considera importante robustecer los modelos de gestión de TI existentes.

Pregunta 2: Dentro de los procesos de Gestión de Operaciones y Servicios de Seguridad pertenecientes a COBIT 5, considera usted que existen actividades con cierto grado de ambigüedad.

Tabla 3. Existen actividades con cierto grado de ambigüedad

Totalmente de Acuerdo	De Acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo	Total
90%	10%	0%	0%	0%	100%

Fuente: Resultados de la Encuesta

Gráfico 3. Existen actividades con cierto grado de ambigüedad

Fuente: Resultados de la Encuesta

En lo que se refiere a esta pregunta, los resultados reflejan que el 90% de los expertos se encuentran totalmente de acuerdo con respecto a que existen actividades con cierto grado de ambigüedad, mientras que el 10% restante se muestra indiferente.

Por lo tanto de acuerdo a la opinión de los expertos, se considera mejorar el enfoque de las actividades que se consideran ambiguas.

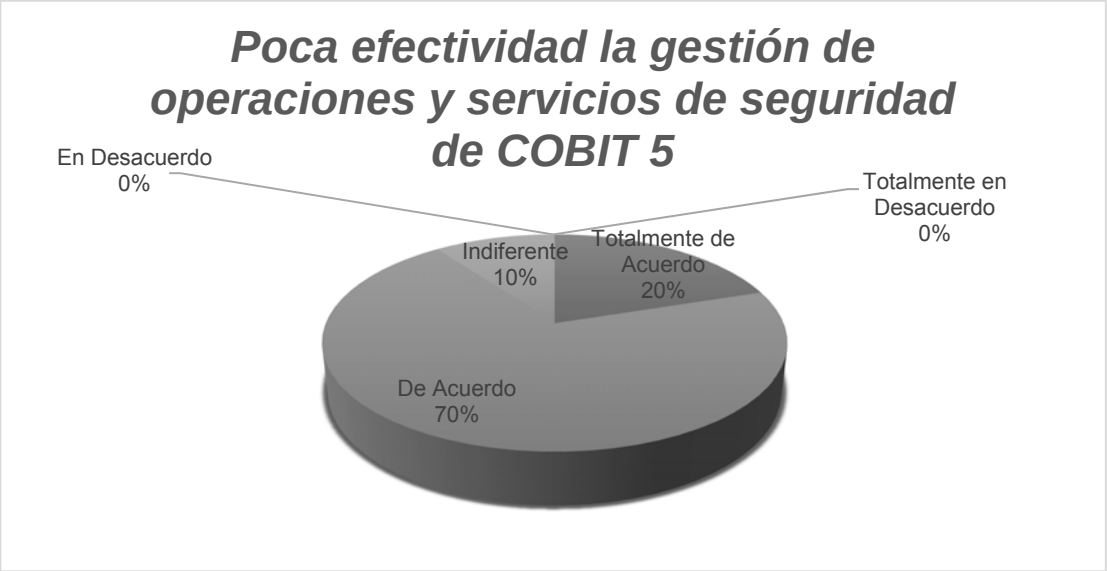
Pregunta 3: Considera poco efectiva la gestión de operaciones y servicios de seguridad que propone COBIT 5?

Tabla 4. Poca efectividad la gestión de operaciones y servicios de seguridad de COBIT 5

Totalmente de Acuerdo	De Acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo	Total
20%	70%	10%	0%	0%	100%

Fuente: Resultados de la Encuesta

Gráfico 4. Poca efectividad la gestión de operaciones y servicios de seguridad de COBIT 5



Fuente: Resultados de la Encuesta

En lo que se refiere a esta pregunta, los resultados reflejan que el 90% de los expertos se encuentran de acuerdo, con respecto a que COBIT 5, es poco efectivo para la gestión de las operaciones y servicios de seguridad, mientras que el 10% se muestra indiferente.

Por lo tanto de acuerdo a la opinión de los expertos, se considera mejorar los procesos de gestión de operaciones y servicios de seguridad que propone COBIT 5**.**

.

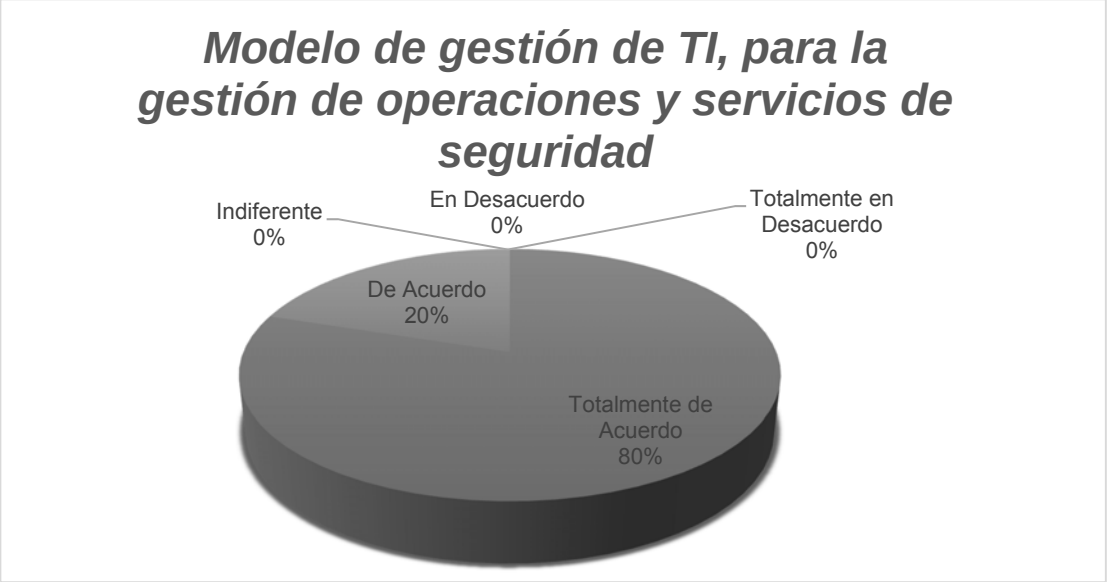
Pregunta 4: Considera usted que actualmente se requiere de un modelo de gestión de tecnologías de información enfocado en la gestión de operaciones y servicios de seguridad.

Tabla 5. Modelo de gestión de TI, enfocado en la gestión de operaciones y servicios de seguridad

Totalmente de Acuerdo	De Acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo	Total
80%	20%	0%	0%	0%	100%

Fuente: Resultados de la Encuesta

Gráfico 5. Modelo de gestión de TI, para la gestión de operaciones y servicios de seguridad



Fuente: Resultados de la Encuesta

En lo que se refiere a esta pregunta, los resultados reflejan que el 100% de los expertos se encuentran de acuerdo, con respecto a que COBIT 5, es poco efectivo para la gestión de las operaciones y servicios de seguridad.

Por lo tanto de acuerdo a la opinión de los expertos, se considera factible el diseño de un modelo gestión de operaciones y servicios de seguridad que propone COBIT 5.

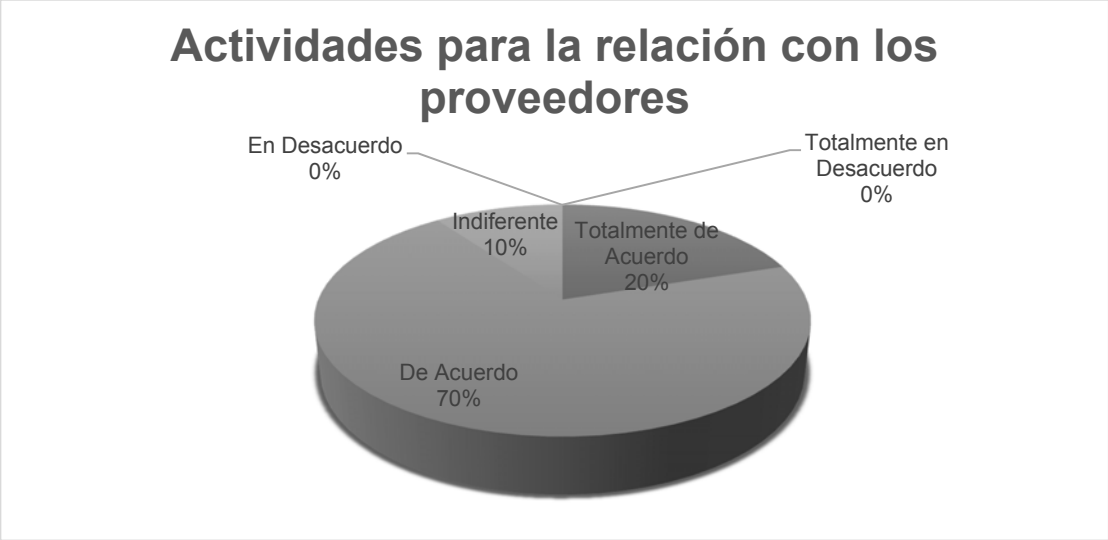
Pregunta 5: Está usted de acuerdo con incorporar a los procesos de COBIT 5, actividades para la relación con los proveedores.

Tabla 6. Actividades para la relación con los proveedores.

Totalmente de Acuerdo	De Acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo	Total
20%	70%	10%	0%	0%	100%

Fuente: Resultados de la Encuesta / Autor

Gráfico 6. Actividades para la relación con los proveedores.



Fuente: Resultados de la Encuesta

En lo que se refiere a esta pregunta, los resultados reflejan que el 90% de los expertos se encuentran de acuerdo, con respecto a que COBIT 5, mientras que el 10% de los expertos con respecto a integrar nuevas actividades para la relación con los proveedores.

Por lo tanto de acuerdo a la opinión de los expertos, se considera factible agregar actividades de relación con los proveedores en la gestión de operaciones y servicios de seguridad que propone COBIT 5.

Pregunta 6: Cree usted que es necesario incorporar una práctica de Gestión Financiera a los procesos de gestión de operaciones y servicios de seguridad que propone COBIT 5.

Tabla 7. Incorporar una práctica de Gestión Financiera.

Totalmente de Acuerdo	De Acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo	Total
70%	30%	0%	0%	0%	100%

Fuente: Resultados de la Encuesta

Gráfico 7. Incorporar una práctica de Gestión Financiera.

Fuente: Resultados de la Encuesta

En lo que se refiere a esta pregunta, los resultados reflejan que el 100% de los expertos se encuentran de acuerdo, con respecto a integrar una nueva practica para la gestión a que COBIT 5.

Por lo tanto de acuerdo a la opinión de los expertos, se considera agregar una nueva práctica para la gestión financiera en la gestión de operaciones y servicios de seguridad que propone COBIT 5.

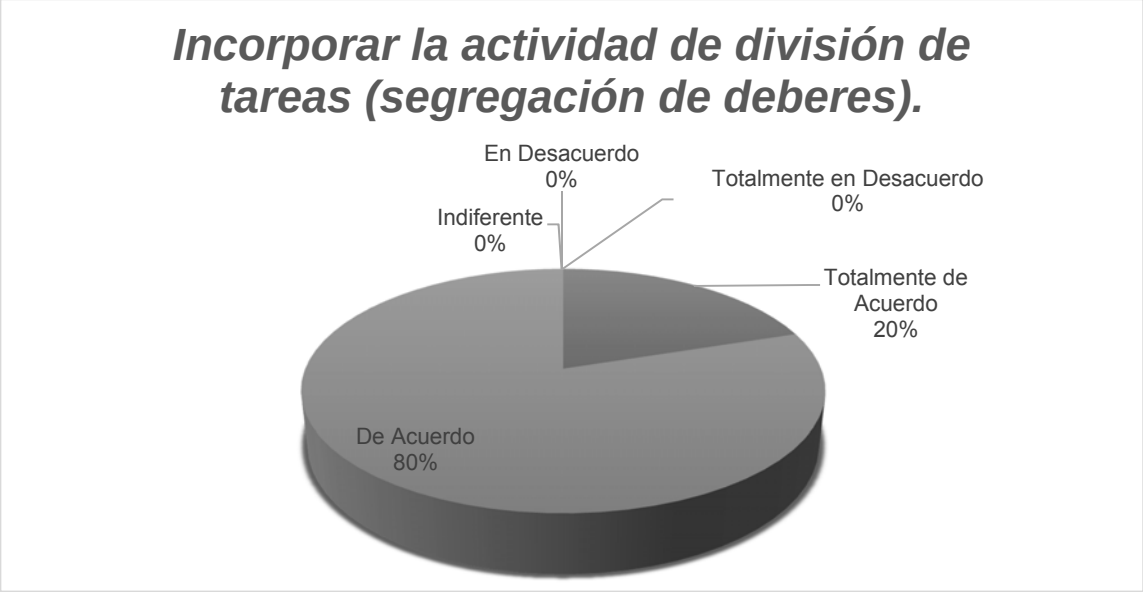
Pregunta 7: Dentro de la administración de tecnologías de información, cree usted necesario incorporar a la división de tareas (segregación de deberes) como una actividad.

Tabla 8. Incorporar la actividad de división de tareas (segregación de deberes).

Totalmente de Acuerdo	De Acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo	Total
20%	80%	0%	0%	0%	100%

Fuente: Resultados de la Encuesta

Gráfico 8. Incorporar la actividad de división de tareas (segregación de deberes).



Fuente: Resultados de la Encuesta

En lo que se refiere a esta pregunta, los resultados reflejan que el 100% de los expertos se encuentran de acuerdo, con respecto a integrar una nueva actividad para la segregación de deberes.

Por lo tanto de acuerdo a la opinión de los expertos, se considera factible agregar una nueva actividad para la división de tareas en la gestión de operaciones y servicios de seguridad que propone COBIT 5.

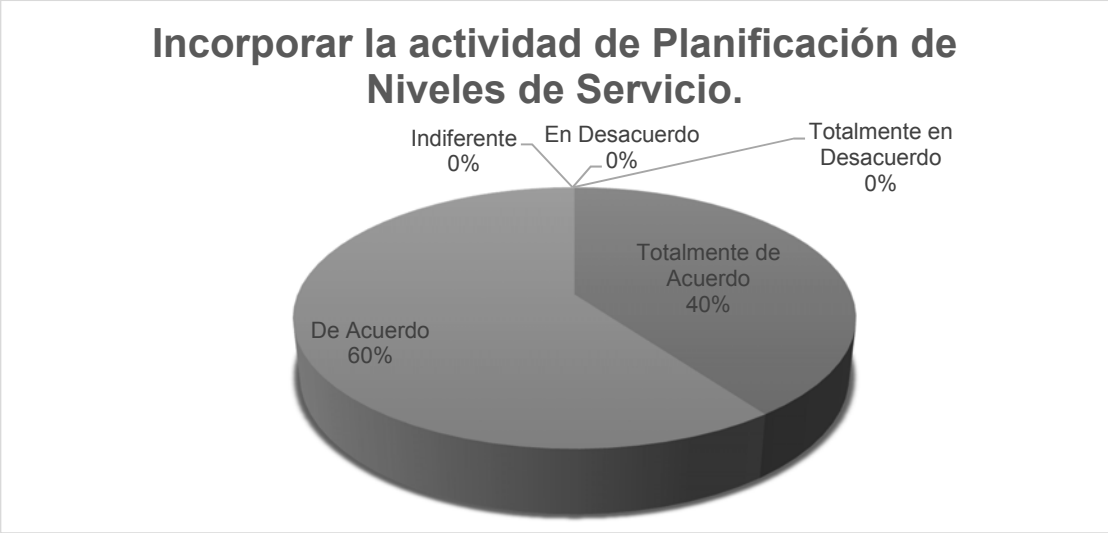
Pregunta 8: Cree usted conveniente considerar a la Planificación de Niveles de Servicio para reforzar las actividades de la práctica de Gestionar los servicios de TI externalizados, que propone COBIT 5?

Tabla 9. Incorporar la actividad de Planificación de Niveles de Servicio

Totalmente de Acuerdo	De Acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo	Total
40%	60%	0%	0%	0%	100%

Fuente: Resultados de la Encuesta

Gráfico 9. Incorporar la actividad de Planificación de Niveles de Servicio.



Fuente: Resultados de la Encuesta

En lo que se refiere a esta pregunta, los resultados reflejan que el 100% de los expertos se encuentran de acuerdo, con respecto a integrar una nueva actividad para la segregación de deberes.

Por lo tanto de acuerdo a la opinión de los expertos, se considera agregar una nueva actividad para la división de tareas en la gestión de operaciones y servicios de seguridad que propone COBIT 5.

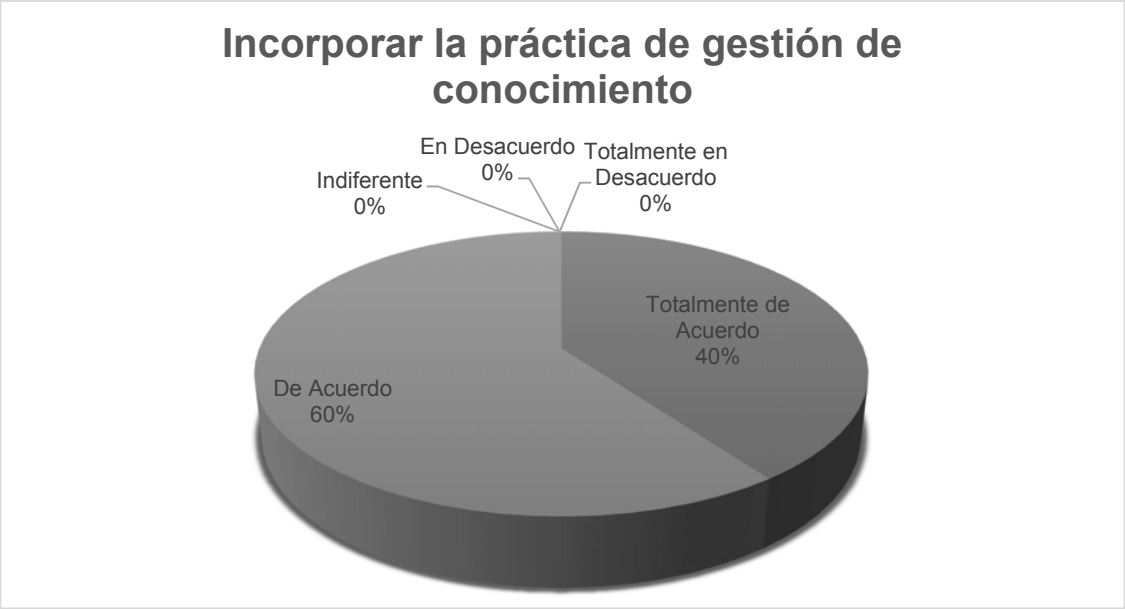
Pregunta 9: Usted considera necesario incorporar la gestión de conocimiento como una práctica que complemente a las propuestas por COBIT 5 en la Gestión de Operaciones.

Tabla 10. Incorporar la práctica de gestión de conocimiento

Totalmente de Acuerdo	De Acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo	Total
40%	60%	0%	0%	0%	100%

Fuente: Resultados de la Encuesta

Gráfico 10. Incorporar la práctica de gestión de conocimiento



Fuente: Resultados de la Encuesta

En lo que se refiere a esta pregunta, los resultados reflejan que el 100% de los expertos se encuentran de acuerdo, con respecto a integrar una nueva práctica de gestión de conocimiento.

Por lo tanto de acuerdo a la opinión de los expertos, se considera factible agregar una nueva práctica para la gestión de conocimiento en la gestión de operaciones y servicios de seguridad que propone COBIT 5.

Pregunta 10: Está usted de acuerdo en incorporar una actividad en COBIT 5, que permita la correlación de los eventos para ahorrar tiempo en la seguridad de soluciones.

Tabla 11. Incorporar una actividad para la correlación de eventos

Totalmente de Acuerdo	De Acuerdo	Indiferente	En Desacuerdo	Totalmente en Desacuerdo	Total
20%	70%	10%	0%	0%	100%

Fuente: Resultados de la Encuesta

Gráfico 11. Incorporar una actividad para la correlación de eventos

Fuente: Resultados de la Encuesta

En lo que se refiere a esta pregunta, los resultados reflejan que el 90% de los expertos se encuentran de acuerdo, con respecto a integrar una nueva actividad para la correlación de eventos, mientras que el 10% de los expertos se presentan indiferentes.

Por lo tanto de acuerdo a la opinión de los expertos, se considera agregar una nueva actividad para la correlación de eventos en la gestión de operaciones y servicios de seguridad que propone COBIT 5.

3.4 Conclusiones

- A lo largo de la presente investigación se logró integrar actividades extraídas de los procesos de ITIL V3:2011 y controles de ISO 27001:2005 a los procesos de Gestión de Operaciones y Gestión de los Servicios de Seguridad propuestos por COBIT 5 para la elaboración del modelo propuesto, el cual servirá como una opción de prevención a las perturbaciones de las operaciones y protección de las tecnologías que gestionan la información.
- La inclusión de nuevas actividades a las prácticas de propuestas por COBIT 5, se realizó en el proceso DSS01 – Gestión de las Operaciones y DSS05 Gestión de los Servicios de Seguridad, puesto que se detectaron falencias, mediante el análisis comparativo de sus actividades con el marco de trabajo ITIL V3:2011 y el Estándar ISO 27001:2005; además de la creación de nuevas prácticas, que se consideró importante integrar para complementar el contexto de acción de los procesos.
- Durante el desarrollo del mapeo se descubrieron ambigüedad en algunas de las actividades de los procesos de Gestión de Operaciones y Gestión de los Servicios de Seguridad COBIT 5, por esto se planteó actividades pertenecientes al marco de trabajo ITIL V3:2011 y controles del Estándar ISO 27001:2005, con el propósito de mejorar su enfoque.
- Mediante la opinión obtenida por medio de la encuesta aplicada a expertos de distintas empresas constituidas legalmente en la ciudades seleccionadas para el estudio, ubicadas en la Provincia de El Oro, se concluyó que el modelo propuesto permite solventar falencias y ambigüedades de los procesos de Gestión de las Operaciones y Gestión de los Servicios de Seguridad propuestos por COBIT 5, además de proporcionar apoyo a las operaciones y servicios de seguridad de las empresa.

3.5 Recomendaciones

- Implementar modelos de gestión de Tecnologías de Información en las empresas para mejorar el rendimiento de sus operaciones y servicios TI con la prevención a las perturbaciones de las operaciones y protección de las tecnologías que gestionan la información.
- Antes de integrar nuevas actividades o prácticas a los procesos de Gestión de Operaciones y Servicios de Seguridad pertenecientes a COBIT 5, se recomienda conocer el contexto de estos, para no cometer errores o malas interpretaciones de sus actividades.
- Determinar las condiciones que deben cumplir las actividades de los procesos de ITIL V3:2011 y controles de ISO 27001:2005, para ser consideradas como una nueva actividad, práctica o si es considera para cambiar el enfoque de aquellas actividades de COBIT 5 que tienen cierto grado de ambigüedad.
- Establecer instrumentos claros y bien redactados para la recolección de la opinión de los encuestados con el fin de evitar confusiones con respecto a la perspectiva que se quiere abarcar con cada pregunta, además de seleccionar como muestra a aquellas empresas de fácil acceso y de las que el investigador tiene conocimiento sobre sus actividades, de forma que se permita obtener datos reales y con un alto grado de compromiso por los expertos.
- Como trabajo posterior a este modelo, se recomienda el diseño de instrumentos, plantillas, aplicaciones web o de escritorio que permitan la gestión del conocimiento de forma automatizada.

Referencias

[1] Kaspersky Lab, “Kaspersky Lab: 68% de empresas en América Latina ha sufrido un ataque de malware en los últimos 12 meses,” *http://latam.kaspersky.com/*, 2013. [Online]. Available: http://latam.kaspersky.com/mx/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/kaspersky-lab-68-de-empresas-en-américa-latin. [Accessed: 18-Jul-2016].

[2] Kaspersky Lab, “Kaspersky Lab echa un vistazo hacia atrás: repaso los principales incidentes de seguridad de 2015,” *http://latam.kaspersky.com/*, 2015. [Online]. Available: http://latam.kaspersky.com/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/2015/repaso-los-principales-incidentes-de-seguridad-de-2015. [Accessed: 18-Jul-2016].

[3] ESET, “ESET informa que el 40% de las empresas sufrió un ataque de malware,” *http://www.eset-la.com/*, 2016. [Online]. Available: http://www.eset-la.com/centro-prensa/articulo/2016/40-empresas-sufrio-ataque-malware-eset-security-report/4290. [Accessed: 18-Jul-2016].

[4] R. Tecnura, “Model for implementation of IT corporate governance,” *Tecnura*, no. c, pp. 159–169, 2015.

[5] OSIATIS S.A., “El ciclo de vida de los servicios TI,” *http://itilv3.osiatis.es*, 2011. [Online]. Available: http://itilv3.osiatis.es/ciclo_vida_servicios_TI.php. [Accessed: 16-May-2016].

[6] M. I. Ladino A., P. A. Villa S., and A. L. E. María, “Fundamentos de iso 27001 y su aplicación en las empresas,” *Sci. Tech.*, vol. 1, pp. 334 – 339, 2011.

[7] D. Radovanovic, M. Sarac, D. Radovanović, M. Šarac, S. Adamovic, and D. Lučić, “Necessity of IT Service management and IT Governance,” *… , 2011 Proc. …*, pp. 1430–1433, 2011.

[8] F. Doelitzscher, C. Reich, and A. Sulistio, “Designing cloud services adhering to government privacy laws,” *Proc. - 10th IEEE Int. Conf. Comput. Inf. Technol. CIT-2010, 7th IEEE Int. Conf. Embed. Softw. Syst. ICESS-2010, ScalCom-2010*, no. Cit, pp. 930–935, 2010.

[9] Z. Yao and X. Wang, “An ITIL based ITSM practice: A case study of steel manufacturing enterprise,” *2010 7th Int. Conf. Serv. Syst. Serv. Manag. Proc. ICSSSM’ 10*, pp. 423–427, 2010.

[10] P. Kusumah, S. Sutikno, and Y. Rosmansyah, “Model design of information security governance assessment with collaborative integration of COBIT 5 and ITIL (case study: INTRAC),” *IEEE Syst. Journal, Proc. - 2014 Int. Conf. ICT Smart Soc. “Smart Syst. Platf. Dev. City Soc. GoeSmart 2014”, ICISS 2014*, pp. 1–6, 2014.

[11] J. M. Fan, Y. H. Xiao, X. Y. Shun, and P. Ji, “A unified framework for outsourcing governance,” *Proc. - 9th IEEE Int. Conf. E-Commerce Technol. 4th IEEE Int. Conf. Enterp. Comput. E-Commerce E-Services, CEC/EEE 2007*, pp. 367–374, 2007.

[12] S. Saetang and A. Haider, “IT governance implementation in corporate environments: A case study of an international hospital in Thailand,” *2013 Proc. PICMET 2013 Technol. Manag. IT-Driven Serv.*, pp. 2460–2467, 2013.

[13] L. Merchán, A. Urrea, and R. Rebollar, “Definición de una metodología ágil de ingeniería de requerimientos para empresas emergentes de desarrollo de software del sur-occidente colombiano,” *Rev. Científica Guillermo Ockham*, vol. 6, no. 1, pp. 37–50, 2008.

[14] O. I. para la Estandarización and Comisión Electrotécnica Internacional, “Estándar Internacional Iso / Iec 27001:2005,” vol. 2005. ISO/IEC, 2005.

[15] A. S. Hashim and W. F. W. Ahmad, “The Development of New Conceptual Model for MobileSchool,” *IEEE Syst. Journal, 2012 Sixth UKSim/AMSS Eur. Symp. Comput. Model. Simul.*, vol. 3, pp. 517–522, 2012.

[16] R. M. Argent, R. S. Sojda, C. Guipponi, B. McIntosh, A. A. Voinov, and H. R. Maier, “Best practices for conceptual modelling in environmental planning and management,” *Environ. Model. Softw.*, vol. 80, pp. 113–121, 2016.

[17] ISACA, “COBIT 5 Implementation,” *http://www.isaca.org/*, 2012. [Online]. Available: http://www.isaca.org/COBIT/Pages/COBIT-5-Implementation-product-page.aspx. [Accessed: 22-Jun-2016].

[18] J. Cristóbal, C. Romaní, and J. C. Cobo, “El concepto de tecnologías de la información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento,” *Zer*, vol. 14, no. 27, pp. 1137–1102, 2009.

[19] E. Sánchez-Duarte, “Las tecnologías de información y comunicación (TIC) desde una perspectiva social,” *Rev. Electrónica Educ.*, vol. XII, pp. 155–162, 2008.

[20] R. Ramírez, F. Villao, and H. Ramírez, “Planeación estrategica de tecnologías de la informacion y comunicacion,” *Rev. Cienc. y Tecnol. UTEG*, vol. N° 5, pp. 53–65, 2013.

[21] C. E. Dickerson and D. Mavris, “A brief history of models and model based systems engineering and the case for relational orientation,” *IEEE Syst. J.*, vol. 7, no. 4, pp. 581–592, 2013.

[22] Asociación de Academias de la Lengua Española (ASALE)., “Diccionario de la lengua española - Modelo,” 2016.

[23] M. Aguilera, “Los distintos Modelos Científicos,” UOC - Universitat Oberta de Catalunya, España, 2000.

[24] F. Scheiber, H. B. Motra, D. Legatiuk, and F. Werner, “Uncertainty-based evaluation and coupling of mathematical and physical models,” Elsevier, 2016.

[25] K. Ogata, *Dinámica de Sistemas*, Primera. México: PRENTICE-HALL HISPANOAMERICANA, S.A., 1987.

[26] REDUE ALCUE, “El Salvador: UFG crea un centro de modelaje matemático,” 2016.

[27] J. T. Ulloa Ibarra and J. A. Rodríguez Carrillo, “La modelación matemática como puente entre el conocimiento científico y el matemático,” *Rev. Electron. Vet.*, vol. 14, no. 2, 2013.

[28] M. A. Pignataro, G. Lobaccaro, and G. Zani, “Digital and physical models for the validation of sustainable design strategies,” *Autom. Constr.*, vol. 39, pp. 1–14, 2014.

[29] S.-G. María Fernanda, P. R. Diego Darío, G. A. Diego Alejandro, and F. S. Juan Carlos, “Modelo Físico de Acuífero: su implementación para un curso de aguas subterráneas,” *Cienc. docencia tecnol.*, vol. XXV, pp. 209–223, 2014.

[30] H. Hu, C. He, and Z. Li, “An AOP Framework and Its Implementation Based on Conceptual Model,” *IEEE Syst. J.*, pp. 233–236, 2009.

[31] E. M. Fergusson, “Importancia de los modelos conceptuales y teorías de

enfermería: experiencia de la Facultad de Enfermería de la Universidad de La Sabana," *Rev. Aquichan*, vol. 5, pp. 44–55, 2005.

[32] M. Pereda and J. M. Zamarreño, "Modelado Basado en Agentes: un Enfoque desde la Ingeniería de Sistemas," *RIAI - Rev. Iberoam. Autom. e Inform. Ind.*, vol. 12, no. 3, pp. 304–312, 2015.

[33] M. Nemiche, R. Pla-López, and V. Cavero, "Un Modelo Teórico Basado en Agentes para Simular la Evolución de los Comportamientos Sociales en un Mundo Artificial," *Rev. Int. Sist.*, vol. 18, pp. 19–28, 2013.

[34] P. Sr and F. Cid, "Formulación de un modelo Multi-agente para el análisis de la generación de energía eléctrica a base de biomasa forestal , en una comunidad rural de la Región de los Ríos , Chile .," Universidad Austral de Chile, 2012.

[35] M. J. González, E. Martín, G. Buiza, M. Hidalgo, and J. Beltrán, "Implementation of an Operations Management System in eight Spanish SMEs," *IEEE Syst. J.*, no. October, 2015.

[36] H. Zhang and Q. Li, "Research on the Application of Comprehensive Budget Management in China Based on Operation : Problems and Countermeasures," *IEEE Syst. J.*, pp. 1416–1419, 2011.

[37] S. Jing, Z. Wang, Y. Liu, J. Kou, and S. Han, "The practice of hospital operation management in the era of new healthcare reform," *IEEE Syst. J.*, pp. 197–199, 2013.

[38] GRUPO NETPC S.A., "Servicios de Seguridad," *http://www.gruponetpc.com*, 2015. [Online]. Available: http://www.gruponetpc.com/Seguridad.html. [Accessed: 23-Jun-2016].

[39] G. Yee, "Personalized security for e-services," *IEEE, Proc. - First Int. Conf. Availability, Reliab. Secur. ARES 2006*, vol. 2006, pp. 140–147, 2006.

[40] BITCompany, "COBIT 5: el mejor aliado para la seguridad de la información en TI," *bitcompany.biz*, 2015. [Online]. Available: http://www.bitcompany.biz/cobit-5-gestion-de-seguridad/#.V15SKrt97IW. [Accessed: 13-Jun-2016].

[41] OSIATIS S.A., "Gestión de la Seguridad de la Información - Introducción y Objetivos," *http://itilv3.osiatis.es/*, 2011. [Online]. Available: http://itilv3.osiatis.es/diseno_servicios_TI/gestion_seguridad_informacion/introduccion_objetivos.php. [Accessed: 13-Jun-2016].

[42] OSIATIS S.A., "Gestión de la Seguridad de la Información," *http://itilv3.osiatis.es/*, 2011. [Online]. Available: http://itilv3.osiatis.es/diseno_servicios_TI/gestion_seguridad_informacion.php. [Accessed: 13-Jun-2016].

[43] G. Paola, M. Góngora, and W. N. Bernal, "Factores Clave en la Gestión de Tecnología de Información para Sistemas de Gobierno Inteligente," *J. Technol. Manag. Innov.*, vol. 10, no. 4, pp. 109–117, 2015.

[44] M. Cochran, "Proposal of an operations department model to provide IT governance in organizations that don't have IT C-level executives," *IEEE Syst. Journal, Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 1–10, 2010.

[45] OSIATIS S.A., "Centro de Servicios - Introducción y Objetivos," *http://itilv3.osiatis.es*, 2011. [Online]. Available: http://itilv3.osiatis.es/operacion_servicios_TI/centro_servicios/introduccion_objetivos.php. [Accessed: 15-May-2016].

[46] E. Oscar, Orlando and R. Sofía, Paola, “Análisis Y Diseño De La Solución ‘ Centro De Servicios (Service Desk)’, Basados En El Marco De Trabajo Itil Versión 3,” ESCUELA POLITÉCNICA DEL EJÉRCITO - ESPE, 2012.

[47] OSIATIS S.A., “Operación de los Servicios TI - Procesos,” *http://itilv3.osiatis.es*, 2011. [Online]. Available: http://itilv3.osiatis.es/operacion_servicios_TI/procesos.php. [Accessed: 16-May-2016].

[48] T. Lucio-Nieto and R. Colomo-Palacios, “ITIL and the creation of a Service Management Office (SMO): A new challenge for IT professionals - An exploratory study of Latin American companies,” *Iber. Conf. Inf. Syst. Technol. Cist.*, pp. 1–6, 2012.

[49] M. Valencia, “Propuesta de Estrategias de Marketing para la prestación de servicios de outsourcing administrativo-financiero orientado al mercado de las PYMES en la ciudad de Cuenca,” UNIVERSIDAD DEL AZUAY, 2014.

[50] S. Sieber, J. Valor, and V. Porta, “Los Sistemas de Información en la Empresa Actual,” in *IESE*, vol. 3, McGraw-Hill, Ed. Madrid, 2007, pp. 0–31.

[51] E. Rodríguez and P. Robaina, “¿ Qué Actividades Deberían Externalizar Las Empresas ? Una Aproximación Bajo La Perspectiv a De,” *Investig. Eur. Dir. y Econ. la Empres.*, vol. 10, pp. 209–230, 2004.

[52] E. Valenciana, “El Outsourcing TIC y de procesos como herramienta de innovación y competitividad en las empresas de la Comunidad Valenciana,” *everis/IE*, Valencia, p. 99, 2011.

[53] P. C. Mercado, “COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.” ISACA, Estados Unidos, p. 90, 2015.

[54] Q. Lin, “Operation maintenance and management model on informationization system of small and medium enterprises,” *IEEE Syst. Journal, 2011 2nd Int. Conf. Artif. Intell. Manag. Sci. Electron. Commer.*, pp. 6700–6703, 2011.

[55] J. J. Sánchez Peña, E. Fernández Vicente, and A. M. Ocaña, “ITIL, COBIT and EFQM: Can They Work Together?,” *Int. J. Comb. Optim. Probl. Informatics*, vol. 4, no. 1, pp. 54–64, 2013.

[56] M. A. V. Vitoriano and J. S. Neto, “Information technology service management processes maturity in the Brazilian Federal direct administration,” *J. Inf. Syst. Technol. Manag.*, vol. 12, no. 3, pp. 663–686, 2016.

[57] A. L. Mesquida, A. Mas, E. Amengual, and I. Cabestrero, “Sistema de Gestión Integrado según las normas ISO 9001 ISO IEC 20000 e ISO IEC 27001,” *Rev. Española Innovación, Calid. e Ing. del Softw.*, vol. 6, no. 3, pp. 25–34, 2010.

[58] OSIATIS S.A, “RACI,” 2011. [Online]. Available: http://itilv3.osiatis.es/diseno_servicios_TI/modelo_RACI.php. [Accessed: 01-Jun-2016].

[59] H. Cerda, “Medios, Instrumentos, Técnicas y Métodos en la Recolección de Datos e Información,” in *Los elementos de la Investigación.*, Caracas, 2011, p. 106.

[60] R. Pimienta Lastra, “Encuestas probabilísticas vs . no probabilísticas,” *Política y Cultura*, no. 13, Mexico, pp. 263–276, 2000.

ÍNDICE COMPLEMENTARIO

Anexo A. Mapeo de los procesos de Gestión de Operaciones y Gestión de Servicios de Seguridad de COBIT 5 con los procesos de ITIL V3:2011

COBIT 5 / ITIL V3:2011	DSS01.01 Realizar procedimientos operacionales.					DSS01.02 Gestionar los servicios de TI externalizados.				DSS01.03 Supervisar la infraestructura de TI.						Proceso DSS01: Gestión de			
	Desarrollar y mantener procedimientos operativos y actividades relacionadas para dar apoyo a todos los servicios entregados.	Mantener una programación de actividades operativas, ejecutar las actividades y supervisar el desempeño conforme a lo programado (incluyendo el mantenimiento preventivo) de las actividades programadas.	Asegurar que se cumple con los estándares de seguridad aplicables para la recepción, procesamiento, almacenamiento y salida de datos de forma tal que se satisfagan los objetivos empresariales, la política de seguridad de la empresa y los requerimientos regulatorios.	Verificar que todos los datos esperados para su procesamiento son recibidos y procesados por completo y de una forma precisa y oportuna. Entregar los resultados de acuerdo con los requisitos de la empresa. Dar soporte a las necesidades de reinicio y reprocesamiento necesarias para asegurar que se reciben los resultados adecuados de una forma segura y oportuna.	Programar, realizar y registrar las copias de respaldo, según lo definido por las políticas y procedimientos establecidos.	Asegurar que los procesos de información se adhieren a los requerimientos de seguridad de la empresa y que se cumplen los términos y ANS con terceros que alojan o proveen servicios.	Asegurar que los requerimientos operativos del negocio y de procesamiento de TI, así como a las prioridades en la entrega del servicio se adhieren y son conformes a los términos y ANS con terceros que alojan o proveen servicios.	Integrar los procesos críticos de TI con los de los proveedores de servicios externalizados, por ejemplo, la planificación de la capacidad y el rendimiento, la gestión de cambio, la gestión de configuración, la gestión de peticiones de servicio y de incidentes, la gestión de problemas, la gestión de seguridad, la continuidad de negocio y la monitorización y notificación del desempeño de procesos.	Planificar la realización de auditorías y aseguramientos independiente de los proveedores de servicios externalizados de externalización (outsourcing) para confirmar que los requerimientos acordados están recibiendo el tratamiento adecuado.	Registrar eventos, identificando el nivel de información a ser grabada sobre la base de una consideración del riesgo y el rendimiento.	Identificar y mantener una lista de los activos de infraestructura que necesitan ser monitorizados en base a la criticidad del servicio y la relación entre los elementos de configuración y los servicios que de ellos dependen.	Definir e implementar reglas que identifican condiciones de eventos, para ayudar a reconocer la significación de eventos, Encontrar un equilibrio entre la generación de eventos falsos menores y eventos significativos, de forma tal que los registros de eventos no se llenen innecesaria.	Producir registros de eventos y reteneños por un período apropiado para asistir en investigaciones futuras.	Establecer procedimientos para supervisar los registros de eventos y llevar a cabo revisiones periódicas.	Asegurar que se crean oportunamente los tiques de incidente cuando la monitorización identifica desviaciones de los umbrales definidos.	Identificar desastres naturales y causados por el ser humano que puedan ocurrir en el área donde se encuentran las instalaciones de TI. Evaluar el efecto potencial en las instalaciones de TI.	Identificar de qué manera el equipamiento de TI, incluyendo el equipamiento móvil y el propiedad conectado a la empresa, está protegido contra las amenazas del entorno. Asegurar que la política limite o impida comer, beber y fumar en áreas sensibles y que se prohíba almacenamiento de material de oficina susceptible de combustión espontánea. Asegurar que el personal conoce el modo de reportar problemas relativos a los centros de procesamiento de datos.	Ubicar y construir las instalaciones de TI para minimizar y mitigar la susceptibilidad ante las amenazas del entorno.	Supervisar y mantener de forma periódica a los dispositivos que detectan proactivamente las amenazas del entorno (p. ej. Fuego, agua, humo, humedad)
Procesos - Actividades	1	2	3	4	5	1	2	3	4	1	2	3	4	5	6	1	2	3	4
1 Fase de Estrategia																			
1.1. Gestión Financiera																			
1.1.1 Presupuesto	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
1.1.2 Contabilidad	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
1.2. Gestión del Portfolio de Servicios																			
1.2.1 Definicion del Negocio	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
1.2.2 Desarrollo de la Oferta	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
1.3. Gestión de la Demanda																			
1.3.1 Análisis de actividad	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
1.3.2 Desarrollo de la oferta	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2 Fase de Diseño																			
2.1. Gestión del Catálogo de Servicios																			
2.1.1 Definición de las familias principales de servicios a prestar, registro de los servicios en activo y de la documentación asociada a los mismos.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2.1.2 Mantenimiento y actualización del Catálogo de Servicios	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2.2. Gestión de Niveles de Servicio																			
2.2.1. Planificación de los Niveles de Servicio	x	x	x	x	x	◑	◑	x	x	x	x	x	x	x	x	x	x	x	x
2.2.2. Implementación de los Acuerdos de Niveles de Servicio	x	x	x	x	x	◑	◑	x	x	x	x	x	x	x	x	x	x	x	x
2.2.3. Supervisión y revisión de los Acuerdos de Nivel de Servicio	x	x	x	x	x	x	x	◑	◑	x	x	x	x	x	x	x	x	x	x
2.3. Gestión de la Capacidad																			
2.3.2 Monitorización de los recursos de la infraestructura TI.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2.3.3 Supervisión de la capacidad	x	x	x	x	x	x	◑	◑	x	x	x	x	x	x	x	x	x	x	x
2.4. Gestión de la Disponibilidad																			
2.4.1 Determinar cuáles son los requisitos de disponibilidad reales del negocio.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2.4.2 Desarrollar un plan de disponibilidad donde se estime el futuro a corto y medio plazo.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2.4.3 Mantenimiento del servicio en operación y recuperación del mismo en caso de fallo.	◑	◑	◑	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2.5. Gestión de la Continuidad de los Servicios TI																			
2.5.1 Establecer las políticas y alcance de la ITSCM.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2.5.2 Evaluar el impacto en el negocio de una interrupción de los servicios TI.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2.5.3 Analizar y prever los riesgos a los que esta expuesto la infraestructura TI.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2.5.4 Establecer las estrategias de continuidad del servicio TI.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2.5.5 Desarrollar los planes de contingencia.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2.5.6 Poner a prueba dichos planes.	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	x	x	x
2.5.8 Revisar periódicamente los planes para adaptarlos a las necesidades reales del negocio.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2.6. Gestión de la Seguridad de la Información																			
2.6.1 Establezca una clara y definida política de seguridad que sirva de guía a todos los otros procesos.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2.6.2 Elabore un Plan de Seguridad que incluya los niveles de seguridad adecuados tanto en los servicios prestados a los clientes como en los acuerdos de servicio firmados con proveedores internos y externos.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

2.6.3	Supervise proactivamente los niveles de seguridad analizando tendencias, nuevos riesgos y vulnerabilidades.	x	x	x	x	x	◑	x	x	x	x	x	x	x	x	x	x	x	x	x
2.7.	**Gestión de Proveedores**																			
2.7.1	Los requisitos de contratación que se van a exigir a los proveedores.	x	x	x	x	x	◑	x	x	x	x	x	x	x	x	x	x	x	x	x
2.7.2	Los procesos de evaluación y selección de proveedores.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2.7.3	La clasificación y documentación de la relación con los proveedores.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2.7.4	Gestión del Rendimiento de los proveedores	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2.7.5	Renovación o terminación.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3	**Fase de Transición**																			
3.1.	**Planificación y soporte a la Transición**																			
3.1.1.	Estrategia de transición	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.1.2.	Preparación de transición	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.1.3.	Planificación de la transición	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.2.	**Gestión de Cambios**																			
3.2.1	Registro de peticiones	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.2.2	Aceptación y Clasificación del cambio	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.2.3	Aprobación y Planificación del cambio	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.2.4	Implementación del cambio	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.2.5	Evaluación del cambio	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.2.6	Cambios de emergencia	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.3	**Gestión de la Configuración y Activos del Servicio**																			
3.3.1	Planificación de la Configuración	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.3.2	Clasificación y registro de los Elementos de Configuración	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x
3.3.3	Monitorización y Control de los Elementos de Configuración	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.3.4	Realización de auditorías	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.4.	**Gestión de Entregas y Despliegues**																			
3.4.1.	Planificación de entregas	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.4.2.	Desarrollo del despliegue	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.4.3.	Implementación de la entrega	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.4.4.	Comunicación y formación al cliente	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.5.	**Validación y pruebas**																			
3.5.1	Validación, planificación y verificación de tests	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.5.2	Construcción de tests	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.5.3	Pruebas de Validación	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.5.4	Aceptación y reporte	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.5.5	Limpieza y cierre	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.6.	**Evaluación**																			
3.6.1.	Planificación de la evaluación.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.6.2.	Evaluación del rendimiento previsto.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.6.3.	Evaluación del rendimiento real.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.7.	**Gestión del Conocimiento**																			
3.7.1.	Definir una estrategia de Gestión del Conocimiento y difundirla a toda la organización TI.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.7.2.	Ayudar a la transferencia de conocimiento entre personas, equipos y departamentos.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.7.3.	Gestionar la información y los datos para garantizar su calidad y utilidad.	x	x	✓	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3.7.4.	Uso del Sistema de Gestión del Conocimiento del Servicio (SKMS).	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4	**Fase de Operación**																			
4.1.	**Gestión de Eventos**																			
4.1.1	Notificación de eventos	x	x	✓	x	x	x	x	x	x	◑	x	x	x	x	x	x	x	x	x
4.1.2	Detección y filtrado de eventos	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	x
4.1.3	Clasificación de eventos	x	x	x	x	x	x	x	x	x	◑	x	x	x	x	x	x	x	x	x
4.1.4	Correlación	x	x	x	x	x	x	x	x	x	x	x	x	x	◑	x	x	x	x	x
4.1.5	Disparadores	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4.2.	**Gestión de Incidencias**																			
4.2.1	Registro y clasificación	x	x	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	x
4.2.2	Análisis, resolución y cierre	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4.3.	**Gestión de Peticiones**																			
4.3.1	Selección de peticiones	x	x	✓	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4.3.2	Aprobación financiera	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4.3.3	Tramitación y cierre	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4.4.	**Gestión de Problemas**																			
4.5.1	Control de Problemas	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4.5.2	Control de Errores	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4.5.	**Gestión de Acceso a los Servicios TI**																			
4.5.1	Verificación.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

4.5.2	Monitorización de identidad.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4.5.3	Registro y monitorización de accesos.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4.5.4	Eliminación y restricción de derechos.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
5	**Fase de Mejora**																			
5.1.	**Proceso de Mejora**	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
5.2.	**Informes de Servicios TI**	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

Operaciones.																				
tionar el medio ambiente.				DSS01.05 Manejo de las instalaciones.											DSS05.01 Proteger contra el malware.					
Responder a las alarmas y otras notificaciones del entorno. Documentar y probar los procedimientos, lo que debería incluir la priorización de alarmas y el contacto con las autoridades locales de respuesta ante emergencias y entrenar al personal en estos procedimientos.	Comparar medidas y planes de contingencia respecto a los requerimientos de las pólizas de seguros e informar de los resultados. Atender a los puntos de no-conformidad de manera oportuna.	Asegurar que los sitios de TI están construidos y diseñados para minimizar el impacto del riesgo del entorno (p. ej. Robo, aire, fuego, humo, agua, vibración, terrorismo, vandalismo, productos químicos, explosivos). Considerar zonas específicas de seguridad o celdas a prueba de incendio (p. ej. ubicando los entornos/servicios de producción y de desarrollo alejados entre si).	Mantener en todo momento a los sitios de TI y las salas de servidores limpias y en una condición segura (es decir, sin desorden, sin papel ni cajas de cartón, sin papeleras llenas, sin productos químicos o materiales inflamables).	Examinar los requerimientos de las instalaciones de TI respecto a la protección frente a la fluctuación y cortes de la energía eléctrica, en relación con otros requerimientos de la planificación de la continuidad del negocio. Disponer de equipamiento adecuado de alimentación interrumpida (p. ej. baterías, generadores) para dar soporte a la planificación de continuidad de negocio.	Probar periódicamente los mecanismos del sistema de alimentación interrumpida (SAI) y asegurar que la electricidad puede ser conmutada al sistema sin efectos significativos en las operaciones del negocio.	Asegurar que las instalaciones que alojan los sistemas de TI tienen más de un proveedor para los servicios públicos indispensables (p. ej. Electricidad, telecomunicaciones, agua, gas). Separar la acometida de cada servicio.	Confirmar que el cableado externo al sitio TI está bajo tierra o que tiene una protección alternativa adecuada. Determinar que el cableado en el sitio TI está contenido en productos asegurados y que los armarios de cableado tienen su acceso restringido al personal autorizado. Proteger adecuadamente al cableado contra el daño causado por fuego, humo, agua, interceptación e interferencia.	Asegurar que el cableado y el patching físico (datos y telefonía) están estructurados y organizados. Las estructuras de cableado y de conductos debieran estar documentadas (p. ej. Olano del edificio y diagramas de cableado).	Analizar las instalaciones que alojan los sistemas de alta disponibilidad para verificar el cumplimiento de los requerimientos de cableado (externo e interno) en cuanto a redundancia y tolerancia a fallos.	Asegurar que los sitios e instalaciones de TI cumplen de manera sistemática con la legislación, regulaciones, directrices y especificaciones relevantes de salud y seguridad en el trabajo.	Proporcionar periódicamente formación al personal en la legislación, regulaciones y directrices relevantes de salud y seguridad en el trabajo. Capacitar al personal en simulacros de incendio y rescate para asegurar el adecuado conocimiento y las acciones apropiadas a tomar en caso de incendio o incidentes similares.	Registrar, supervisar, gestionar y resolver incidentes en las instalaciones siguiendo los procesos de gestión de incidentes de TI. Poner a disposición proveedor. El mantenimiento debe ser realizado únicamente por personal autorizado.	Asegurar que los sitios y el equipamiento de TI son mantenidos de acuerdo con los intervalos de servicio y las especificaciones recomendados por el proveedor. El mantenimiento debe ser realizado únicamente por personal autorizado.	Analizar las alteraciones físicas a los sitios o localizaciones de TI para reevaluar el riesgo del entorno (p. ej. Daño por fuego o agua). Informar los resultados de este análisis a los niveles directivos de comunidad de negocio y de gestión de edificios.	Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.	Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).	Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.	Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).	Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de pishing).	Realizar formación periódica sobre software malicioso en el uso del correo electrónico e internet. Formar a los usuarios para no instalarse software compartido o no autorizado.
5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	1	2	3	4	5	6
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	◑	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	◑	x	x	◑	x	◑
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

Proceso DSS05: Gestión de Servicios de Seguridad.

DSS05.02Gestión de la red y la seguridad de la conexión.									DSS05.03 Administrar la seguridad del punto final.									DSS05.04 Manejo de la identidad del usuario y el acceso lógico.								DSS05.05 Administrar el acceso físico a los acti				
Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones.	Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña.	Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.	Cifrar la información en tránsito de acuerdo con su clasificación.	Aplicar los protocolos de seguridad aprobados a las conexiones de red.	Configurar equipos de red de forma segura.	Establecer mecanismos de confianza para apoyar la transmisión segura y recepción de información.	Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.	Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.	Configurar los sistemas operativos de forma segura.	Implementar mecanismos de bloqueo del dispositivo.	Cifrar la información de almacenamiento de acuerdo con su clasificación.	Gestionar el acceso y control remoto.	Gestionar la configuración de la red de forma segura.	Implementar el filtrado del tráfico de la red en dispositivos de usuario final.	Proteger la integridad del sistema.	Proveer de protección física a los dispositivos de usuario final.	Deshacerse de los dispositivos de usuario final de forma segura.	Mantener los derechos de acceso de usuario de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer.	Identificar unívocamente todas las actividades de proceso de la información de roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos por el propio negocio en las aplicaciones de procesos de negocio.	Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación con aplicaciones usadas en procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.	Administrar todos los cambios de derecho de acceso (creación, modificación, eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas po los gestores individuales designados.	Segregar y gestionar cuentas de usuarios privilegiadas.	Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.	Asegúrese de que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocios, infraestructura de TI, las operaciones del sistema, desarrollo y mantenimiento) son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información po usuario.	Mantener una pista de auditoría de accesos a la información clasificada como altamente sensible.	Gestionar las peticiones y concesión de acceso a las instalaciones de procesamiento. Las peticiones formales de acceso deben ser completadas y autorizadas por la dirección de la ubicación de TI, y guardado el registro de petición. Los formularios deberían identificar específicamente las áreas a las que el individuo tiene acceso concebido.	Asegurarse de que todos los puntos de entrada están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en funciones de trabajo y responsabilidades.	Registrar y supervisar todos los puntos de entrada a los sitios de TI. Registrar a todos los visitantes de la ubicación, incluyendo contratistas y vendedores.	Instruir a todo el personal para mantener visible la identificación en todo momento. Prevenir la expedición de tarjetas o placas de identidad sin la autorización adecuada.	Escoltar a los visitantes en todo momento mientras esté en la ubicación. Si se encuentra a un individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, se deberá alertar al personal de seguridad.
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**1**	**2**	**3**	**4**	**5**
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	◑	x	x	x	x	x	✔	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	◑
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	✓	✓	x	x	x	✓	✓	x	x	✓	x	x	x

x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

vos de TI.		DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.					DSS05.07 Supervisar la infraestructura para eventos relacionados con la seguridad.				
Restringir el acceso a ubicaciones de TI sensibles, estableciendo perímetros físicos de seguridad, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores. Asegurar que los dispositivos registren el acceso y disparen alarmas ante accesos no autorizados. Ejemplos de estos dispositivos incluyen placas o tarjetas llave, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos.	Realizar regularmente formación de concienciación de seguridad física.	Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formas especiales y dispositivos de salida, dentro, en y fuera de la empresa.	Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basadas en el principio del menor privilegio, equilibrando riesgos y requisitos de negocio.	Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones.	Establecer salvaguardas físicas apropiadas sobre formularios especiales y dispositivos sensibles.	Destruir la información sensible y proteger dispositivos de salida (por ejemplo, la destrucción física de papel sensible, destruir físicamente dispositivos de memoria, poniendo trituradoras o papeleras cerradas disponibles para distribuir formularios especiales y otros documentos confidenciales).	Registrar los sucesos relacionados con la seguridad reportada por las herramientas de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en función a la consideración de riesgo. Retenerla por un período apropiado para asistir en futuras investigaciones.	Definir y comunicar la naturaleza y las características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta commensurada.	Revisar regularmente los registros de eventos para los incidentes potenciales.	Mantener un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales y asegurar que todos los empleados están conformados de los requerimientos.	Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.
6	7	1	2	3	4	5	1	2	3	4	5
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x

x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x

x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	✓	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	✓
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x

x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x

Anexo B. Mapeo de los procesos de Gestión de Operaciones y Gestión de Servicios de Seguridad de COBIT 5 con los controles de ISO 27001:2005

COBIT 5 / ISO 27001: 2005		Proceso DSS01: Gestión de Operaciones.																			
		DSS01.01 Realizar procedimientos operacionales.					DSS01.02 Gestionar los servicios de TI externalizados.				DSS01.03 Supervisar la infraestructura de TI.						DSS01.04 Gestionar el medio amb				
	OBJETIVOS DE CONTROL	Desarrollar y mantener procedimientos operativos y actividades relacionadas para dar apoyo a todos los servicios entregados.	Mantener una programación de actividades operativas, ejecutar las actividades y gestionar el desempeño y rendimiento (throughput) de las actividades programadas.	Asegurar que se cumple con los estándares de seguridad aplicables para la recepción, procesamiento, almacenamiento y salida de datos de forma tal que se satisfagan los objetivos empresariales, la política de seguridad de la empresa y los requerimientos regulatorios.	Verificar que todos los datos esperados para su procesamiento sean recibidos y procesados por completo y de una forma precisa y oportuna. Entregar los resultados de acuerdo con los requisitos de la empresa. Dar soporte a las necesidades de reinicio y reprocesamiento. Asegurar que los usuarios reciben los resultados adecuados de una forma segura y oportuna.	Programar, realizar y registrar las copias de respaldo de acuerdo con las políticas y procedimientos establecidos.	Asegurar que los procesos de información se adhieren a los requerimientos de inseguridad de la información, definidos en los acuerdos y ANS con terceros que alojan o proveen servicios.	Asegurar que los requerimientos operativos del negocio y de procesamiento de TI, así como a las prioridades en la entrega del servicio se adhieren y son conformes a los contratos y ANS con terceros que alojan o proveen servicios.	Integrar los procesos críticos de TI con los de los proveedores de servicios externalizados cubriendo, por ejemplo, la planificación de la capacidad y el rendimiento, la gestión de cambio, peticiones de servicio y de incidentes, la gestión de problemas, la gestión de la seguridad, la continuidad de negocio y la monitorización y notificación del desempeño de procesos.	Planificar la realización de auditorías y aseguramientos independiente de los entornos basados en la externalización (outsourcing) para confirmar que los requerimientos acordados están recibiendo el tratamiento adecuado.	Registrar eventos, identificando el nivel de información a ser grabada sobre la base de una consideración del riesgo y el rendimiento.	Identificar y mantener una lista de los activos de infraestructura que son críticos para dar soporte a la criticidad del servicio y la relación entre los elementos de configuración y los servicios que de ellos dependen.	Definir e implementar reglas que identifican y registren violaciones de umbral y condiciones de eventos. Encontrar un equilibrio entre la generación de eventos falsos menores y eventos significativos que no generan suficientes alertas (eventos no existentes) sobrecargados con información innecesaria.	Producir registros de eventos y retenerlos por un período apropiado para asistir en investigaciones futuras.	Establecer procedimientos para supervisar los registros de eventos y llevar a cabo revisiones periódicas.	Asegurar que se crean oportunamente los tiques de incidente cuando la monitorización identifica desviaciones de los umbrales definidos.	Identificar desastres naturales y causados por el ser humano que puedan ocurrir en el área donde se encuentran las instalaciones de TI. Evaluar el efecto potencial en las instalaciones de TI.	Identificar de qué manera el equipamiento de TI, incluyendo el equipamiento móvil y el ubicado fuera de las instalaciones, se supervisa para las amenazas del entorno. Asegurar que la política límite o impida comer, beber y fumar en áreas sensibles y que se prohíba almacenamiento de material de oficina y otros suministros que puedan constituir un peligro de incendio en los centros de procesamiento de datos.	Ubicar y construir las instalaciones de TI para minimizar y mitigar la susceptibilidad ante las amenazas del entorno.	Supervisar y mantener de forma periódica a los dispositivos que detectan proactivamente las amenazas del entorno (p. ej. Fuego, agua, humo, humedad)	Responder a las alarmas y otras notificaciones del entorno. Documentar y probar los procedimientos, lo que debería incluir la priorización de alarmas y escalado de incidentes, contactos de respuesta ante emergencias y entrenar al personal en estos procedimientos.
		1	2	3	4	5	1	2	3	4	1	2	3	4	5	6	1	2	3	4	5
A.5	**Política de seguridad**																				
A.5.1	**Política de seguridad de información**																				
A.5.1.1	Documentar política de seguridad de información	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.5.1.2	Revisión de la política de seguridad de la información	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.6	**Organización de la seguridad de la información**																				
A.6.1	**Organización interna**																				
A.6.1.1	Compromiso de la gerencia con la seguridad de la información	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.6.1.2	Coordinación de la seguridad de información	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.6.1.3	Asignación de responsabilidades de la seguridad de la información	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.6.1.4	Proceso de autorización para los medios de procesamiento de información	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.6.1.5	Acuerdos de confidencialidad	X	X	X	X	X	✓	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.6.1.6	Contacto con autoridades	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.6.1.7	Contacto con grupos de interés especial	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.6.1.8	Revisión independiente de la seguridad de la información	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.6.2	Entidades externas																				
A.6.2.1	Identificación de riesgos relacionados con entidades externas	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.6.2.2	Tratamiento de la seguridad cuando se trabaja con clientes	X	X	X	X	X	✓	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.6.2.3	Tratamiento de la seguridad en contratos con terceras personas	X	X	X	X	X	✓	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.7	**Gestión de activos**																				
A.7.1	**Responsabilidad por los activos**																				
A.7.1.1	Inventarios de activos	X	X	X	X	X	X	X	X	X	X	✓	X	X	X	X	X	X	X	X	X
A.7.1.2	Propiedad de los activos	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.7.1.3	Uso aceptable de los activos	✓	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.7.2	**Clasificación de la información**																				
A.7.2.1	Lineamientos de clasificación	X	X	X	X	X	X	X	X	X	✓	X	X	X	X	X	X	X	X	X	X
A.7.2.2	Etiquetado y manejo de la información	✓	X	X	X	X	X	X	X	X	✓	X	X	X	X	X	X	X	X	X	X
A.8	**Seguridad de los recursos humanos**																				
A.8.1	**Antes del empleo**																				
A.8.1.1	Roles y responsabilidades	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.8.1.2	Selección	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.8.1.3	Términos y condiciones de empleo	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.8.2	**Durante el empleo**																				
A.8.2.1	Gestión de responsabilidades	X	X	X	X	X	✓	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.8.2.2	Capacitación y educación en seguridad de la información	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	✓
A.8.2.3	Proceso disciplinario	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.8.3	**Terminación o cambio del empleo**																				
A.8.3.1	Responsabilidades de terminación responsabilidades para realizar la terminación o cambio del empleo.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.8.3.2	Devolución de activos	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.8.3.3	Eliminación de derechos de acceso	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.9	**Seguridad física y ambiental**																				
A.7.1	**Áreas seguras**																				
A.9.1.1	Perímetro de seguridad física	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	✓	X	X
A.9.1.2	Controles de entrada físicos	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.9.1.3	Seguridad de oficinas, habitaciones y medios	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.9.1.4	Protección contra amenazas externas y ambientales	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	✓	X	X	X	X
A.9.1.5	Trabajo en áreas seguras	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.9.1.6	Áreas de acceso público, entrega y carga	X	X	✓	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.9.2	**Seguridad del equipo**																				
A.9.2.1	Ubicación y protección del equipo	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	✓	X	✓	X
A.9.2.2	Servicios públicos	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

A.9.2.3	Seguridad en el cableado	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.9.2.4	Mantenimiento de equipo	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.9.2.5	Seguridad del equipo fuera-dellocal	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	✓
A.9.2.6	Eliminación seguro o re-uso del equipo	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.9.2.7	Traslado de Propiedad	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10	**Gestión de las comunicaciones y operaciones**																			
A.10.1	**Procedimientos y responsabilidades operacionales**																			
A.10.1.1	Procedimientos de operación documentados	◑	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.1.2	Gestión de cambio Control	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.1.3	Segregación de deberes	◑	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.1.4	Separación de los medios de desarrollo y operacionales	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.2	**Gestión de la entrega del servicio de terceros**																			
A.10.2.1	Entrega del servicio revisión de los servicios de terceros	X	X	X	X	X	X	✓	X	X	X	X	X	X	X	X	X	X	X	X
A.10.2.2	Monitoreo y revisión de los servicios de terceros	X	X	X	X	X	X	✓	✓	X	X	X	X	X	X	X	X	X	X	X
A.10.2.3	Manejar los cambios en los servicios de terceros	X	X	X	X	X	X	X	✓	X	X	X	X	X	X	X	X	X	X	X
A.10.3	**Planeación y aceptación del sistema**																			
A.10.3.1	Gestión de capacidad	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.3.2	Aceptación del sistema	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.4	**Protección contra software malicioso y código móvil**																			
A.10.4.1	Controles contra software malicioso	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.4.2	Controles contra códigos móviles	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.5	**Respaldo (back-up)**																			
A.10.5.1	Back-up o respaldo de la información	X	X	X	X	✓	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.6	**Gestión de seguridad de redes**																			
A.10.6.1	Controles de red Control	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.6.2	Seguridad de los servicios de red	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.7	**Gestión de medios**																			
A.10.7.1	Gestión de los medios removibles	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.7.2	Eliminación de medios	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.7.3	Procedimientos de manejo de la información	X	X	X	✓	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.7.4	Seguridad de documentación del sistema no autorizado.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.8	**Intercambio de información**																			
A.10.8.1	Procedimientos y políticas de información y software	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.8.2	Acuerdos de intercambio	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.8.3	Medios físicos en tránsito	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.8.4	Mensajes electrónicos	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.8.5	Sistemas de información comercial	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.9	**Servicios de comercio electrónico**																			
A.10.9.1	Comercio electrónico	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.9.2	Transacciones en línea	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.9.3	Información Control disponible públicamente	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.10	**Monitoreo**																			
A.10.10.1	Registro de auditoria	X	X	X	X	X	X	X	X	X	X	X	X	✓	X	X	X	X	X	X
A.10.10.2	Uso del sistema de monitoreo	◑	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.10.3	Protección de la información del registro	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.10.4	Registros del administrador y operador	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.10.10.5	Registro de fallas	X	X	X	X	X	X	X	X	X	X	X	X	X	✓	X	X	X	X	X
A.10.10.6	Sincronización de relojes	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11	**Control de acceso**																			
A.11.1	**Requerimiento comercial para el control del acceso**																			
A.11.1.1	Política de control de acceso	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.2	**Gestión del acceso del usuario**																			
A.11.2.1	Inscripción del usuario	◑	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.2.2	Gestión de privilegios	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.2.3	Gestión de la clave del usuario	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.2.4	Revisión de los derechos de acceso del usuario	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.3	**Responsabilidades del usuario**																			
A.11.3.1	Uso de clave	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.3.2	Equipo de usuario desatendido	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.3.3	Política de pantalla y escritorio limpio	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.4	**Control de acceso a redes**																			
A.11.4.1	Política sobre el uso de servicios en red	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.4.2	Autenticación del usuario para conexiones externas	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.4.3	Identificación del equipo en red	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

A.11.4.4	Protección del puerto de diagnóstico remoto	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.4.5	Segregación en redes	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.4.6	Control de conexión de redes	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.4.7	Control de 'routing' de redes	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.5	**Control de acceso al sistema de operación**																			
A.11.5.1	Procedimientos de registro en el terminal	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.5.2	Identificación y autenticación del usuario	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.5.3	Sistema de gestión de claves	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.5.4	Uso de utilidades del sistema	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.5.5	Sesión inactiva Control	X	◑	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.5.6	Limitación de tiempo de conexión	X	◑	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.6	**Control de acceso a la aplicación e información**																			
A.11.6.1	Restricción al acceso a la información	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.6.2	Aislamiento del sistema sensible	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.7	**Computación móvil y tele-trabajo**																			
A.11.7.1	Computación móvil y comunicaciones	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.11.7.2	Tele-trabajo Control	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.12	**Adquisición, desarrollo y mantenimiento de los sistemas de información**																			
A.12.1	**Requerimientos de seguridad de los sistemas**																			
A.12.1.1	Análisis y especificación de los requerimientos de seguridad	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.12.2	**Procesamiento correcto en las aplicaciones**																			
A.12.2.1	Validación de data de Insumo	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.12.2.2	Control de procesamiento interno	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.12.2.3	Integridad del mensaje	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.12.2.4	Validación de data de output	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.12.3	**Controles criptográficos**																			
A.12.3.1	Política sobre el uso de controles criptográficos	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.12.3.2	Gestión clave Control	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.12.4	**Seguridad de los archivos del sistema**																			
A.12.4.1	Control de software operacional	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.12.4.2	Protección de la data de prueba del sistema	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.12.4.3	Control de acceso al código fuente del programa	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.12.5	**Seguridad en los procesos de desarrollo y soporte**																			
A.12.5.1	Procedimientos de control de cambio	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.12.5.2	Revisión técnica de las aplicaciones después de cambios en el sistema operativo	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.12.5.3	Restricciones sobre los cambios en los paquetes de software	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.12.5.4	Filtración de información	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.12.5.5	Desarrollo de outsourced software organización.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.12.6	**Gestión de vulnerabilidad técnica**																			
A.12.6.1	Control de vulnerabilidades técnicas	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A. 13	**Gestión de incidentes en la seguridad de la información**																			
A.13.1	**Reporte de eventos y debilidades en la seguridad de la información**																			
A.13.1.1	Reporte de eventos en la seguridad de la información	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.13.1.2	Reporte de debilidades en la seguridad	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.13.2	**Gestión de incidentes y mejoras en la seguridad de la información**																			
A.13.2.1	Responsabilidades y procedimientos	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.13.2.2	Aprendizaje de los incidentes en la seguridad de la información	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.13.2.3	Recolección de evidencia	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.14	**Gestión de la continuidad comercial**																			
A.14.1	**Aspectos de la seguridad de la información de la gestión de la continuidad comercial**																			
A.14.1.1	Incluir seguridad de la información en el proceso de gestión de	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.14.1.2	Continuidad comercial y evaluación del riesgo	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.14.1.3	Desarrollar e implementar planes de continuidad incluyendo seguridad de la información	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.14.1.4	Marco referencial para la planeación de la continuidad comercial	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.14.1.5	Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.15	**Cumplimiento**																			
A.15.1	**Cumplimiento con requerimientos legales**																			
A.15.1.1	Identificación de legislación aplicable	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.15.1.2	Derechos de propiedad intelectual (IPR)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.15.1.3	Protección los registros organizacionales	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.15.1.4	Protección de data y privacidad de información personal	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

A.15.1.5	Prevención de mal uso de medios de procesamiento de información	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.15.1.6	Regulación de controles criptográficos	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.15.2	**Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico**																					
A.15.2.1	Cumplimiento con las políticas y estándares de seguridad	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.15.2.2	Chequeo de cumplimiento técnico	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.15.3.1	Controles de auditoria de sistemas de información	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.15.3.2	Protección de las herramientas de auditoria de los sistemas de información	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

piente.			DSS01.05 Manejo de las instalaciones.											DSS05.01 Proteger contra el malware.						DSS05.02Gestión de la red y la seguridad de la cone						
Comparar medidas y planes de contingencia respecto a los requerimientos de las pólizas de seguros e informar de los resultados. Atender a los puntos de no-conformidad de manera oportuna.	Asegurar que los sitios de TI están construidos y diseñados para minimizar el impacto del riesgo del entorno (p. ej. Robo, aire, fuego, humo, agua, vibración, terrorismo, vandalismo, productos químicos, explosivos). Considerar zonas específicas de seguridad o celdas a prueba de incendio (p. ej. ubicando los entornos/servicios de producción y de desarrollo alejados entre si).	Mantener en todo momento a los sitios de TI y las salas de servidores limpias y en una condición segura (es decir, sin desorden, sin papel ni cajas de cartón, sin papeleras llenas, sin productos químicos o materiales inflamables).	Examinar los requerimientos de las instalaciones de TI respecto a la protección frente a la fluctuación y cortes de la energía eléctrica, en relación con otros requerimientos de la planificación de la continuidad del negocio. Disponer de equipamiento adecuado de alimentación interrumpida (p. ej. baterías, generadores) para dar soporte a la planificación de continuidad de negocio.	Probar periódicamente los mecanismos del sistema de alimentación interrumpida (SAI) y asegurar que la electricidad puede ser conmutada al sistema sin efectos significativos en las operaciones del negocio.	Asegurar que las instalaciones que alojan los sistemas de TI tienen más de un proveedor para los servicios públicos indispensables (p. ej. Electricidad, telecomunicaciones, agua, gas). Separar la acometida de cada servicio.	Confirmar que el cableado externo al sitio TI está bajo tierra o que tiene una protección alternativa adecuada. Determinar que el cableado en el sitio TI está contenido en productos asegurados y que los armarios de cableado tienen su acceso restringido al personal autorizado. Proteger adecuadamente al cableado contra el daño causado por fuego, humo, agua, interceptación e interferencia.	Asegurar que el cableado y el patching físico (datos y telefonía) están estructurados y organizados. Las estructuras de cableado y de conductos debieran estar documentadas (p. ej. Olano del edificio y diagramas de cableado).	Analizar las instalaciones que alojan los sistemas de alta disponibilidad para verificar el cumplimiento de los requerimientos de cableado (externo e interno) en cuanto a redundancia y tolerancia a fallos.	Asegurar que los sitios e instalaciones de TI cumplen de manera sistemática con la legislación, regulaciones, directrices y especificaciones relevantes de salud y seguridad en el trabajo.	Proporcionar periódicamente formación al personal en la legislación, regulaciones y directrices relevantes de salud y seguridad en el trabajo. Capacitar al personal en simulacros de incendio y rescate para asegurar el adecuado conocimiento y las acciones apropiadas a tomar en caso de incendio o incidentes similares.	Registrar, supervisar, gestionar y resolver incidentes en las instalaciones siguiendo los procesos de gestión de incidentes de TI. Poner a disposición proveedor. El mantenimiento debe ser realizado únicamente por personal autorizado.	Asegurar que los sitios y el equipamiento de TI son mantenidos de acuerdo con los intervalos de servicio y las especificaciones recomendados por el proveedor. El mantenimiento debe ser realizado únicamente por personal autorizado.	Analizar las alteraciones físicas a los sitios o localizaciones de TI para reevaluar el riesgo del entorno (p. ej. Daño por fuego o agua). Informar los resultados de este análisis a los niveles directivos de comunidad de negocio y de gestión de edificios.	Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.	Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).	Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.	Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).	Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de pishing).	Realizar formación periódica sobre software malicioso en el uso del correo electrónico e internet. Formar a los usuarios para no instalarse software compartido o no autorizado.	Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones.	Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña.	Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.	Cifrar la información en tránsito de acuerdo con su clasificación.	Aplicar los protocolos de seguridad aprobados a las conexiones de red.	Configurar equipos de red de forma segura.	Establecer mecanismos de confianza para apoyar la transmisión segura y recepción de información.
6	7	8	1	2	3	4	5	6	7	8	9	10	11	1	2	3	4	5	6	1	2	3	4	5	6	7
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	✓	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	✓	✓	x	x	✓	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
[redacted]																										
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
[redacted]																										
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
[redacted]																										
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
[redacted]																										
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

Proceso DSS05: Gestión de Servicios de Seguridad.

exión.		DSS05.03 Administrar la seguridad del punto final.									DSS05.04 Manejo de la identidad del usuario y el acceso lógico.								DSS05.05 Administrar el acceso físico a los activos de TI.							DSS05.06 Manejo de documentos confidenciales y los dispositivos de salida.				
Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.	Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.	Configurar los sistemas operativos de forma segura.	Implementar mecanismos de bloqueo del dispositivo.	Cifrar la información de almacenamiento de acuerdo con su clasificación.	Gestionar el acceso y control remoto.	Gestionar la configuración de la red de forma segura.	Implementar el filtrado del tráfico de la red en dispositivos de usuario final.	Proteger la integridad del sistema.	Proveer de protección física a los dispositivos de usuario final.	Deshacerse de los dispositivos de usuario final de forma segura.	Mantener los derechos de acceso de usuario de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer.	Identificar unívocamente todas las actividades de proceso de la información de roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos por el propio negocio en las aplicaciones de procesos de negocio.	Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación con aplicaciones usadas en procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.	Administrar todos los cambios de derecho de acceso (creación, modificación, eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.	Segregar y gestionar cuentas de usuarios privilegiadas.	Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.	Asegúrese de que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocios, infraestructura de TI, las operaciones del sistema, desarrollo y mantenimiento) son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información por usuario.	Mantener una pista de auditoría de accesos a la información clasificada como altamente sensible.	Gestionar las peticiones y concesión de acceso a las instalaciones de procesamiento. Las peticiones formales de acceso deben ser completadas y autorizadas por la dirección de la ubicación de TI, y guardado el registro de petición. Los formularios deberían identificar específicamente las áreas a las que el individuo tiene acceso concebido.	Asegurarse de que todos los puntos de entrada están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en funciones de trabajo y responsabilidades.	Registrar y supervisar todos los puntos de entrada a los sitios de TI. Registrar a todos los visitantes de la ubicación, incluyendo contratistas y vendedores.	Instruir a todo el personal para mantener visible la identificación en todo momento. Prevenir la expedición de tarjetas o placas de identidad sin la autorización adecuada.	Escoltar a los visitantes en todo momento mientras esté en la ubicación. Si se encuentra a un individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, se deberá alertar al personal de seguridad.	Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores. Asegurar que los dispositivos registren el acceso y disparen una alarma en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas llave, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos.	Realizar regularmente formación de concienciación de seguridad física.	Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formas especiales y dispositivos de salida, dentro, en y fuera de la empresa.	Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basadas en el principio del menor privilegio, equilibrando riesgos y requisitos de negocio.	Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones.	Establecer salvaguardas físicas apropiadas sobre formularios especiales y dispositivos sensibles.	Destruir la información sensible y proteger dispositivos de salida (por ejemplo, la desmagnetizando soportes magnéticos, destruir físicamente dispositivos de memoria, poniendo trituradoras o papeleras cerradas disponibles para distribuir formularios especiales y otros documentos confidenciales).
8	**9**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**1**	**2**	**3**	**4**	**5**
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	✓	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	✓	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x																														
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

DSS05.07 Supervisar la infraestructura para eventos relacionados con la seguridad.				
Registrar los sucesos relacionados con la seguridad reportada por las herramientas de la seguridad de la infraestructura, identificando el nivel de información necesario para realizar análisis basados en la consideración de riesgo. Retenerla por un período apropiado para asistir en futuras investigaciones.	Definir y comunicar la naturaleza y las características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta conmensurada.	Revisar regularmente los registros de eventos para los incidentes potenciales.	Mantener un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales, asegurar que todos los empleados están condenciados de los requerimientos.	Asegurar que los equipo de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.
1	2	3	4	5
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X
X	X	X	X	X

x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
✓	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
✓	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x

x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x

x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x

UNIVERSIDAD TÉCNICA DE MACHALA
UNIDAD ACADÉMICA DE INGENIERÍA CIVIL
CARRERA DE INGENIERÍA DE SISTEMAS

OBJETIVO: Evaluar el prototipo propuesto de Gestión de las Operaciones y Servicios de Seguridad por medio de la opinión de Expertos.

Nombre del encuestado: .....

Cargo: .....

Empresa: .....

Tipo de Empresa: .....

Nota: Señale con un visto según lo que Ud. Este de acuerdo

N°	Preguntas	Totalmente de Acuerdo	De Acuerdo	Indiferente	En Desacuerdo	Totalmente en desacuerdo
1	Considera usted que actualmente no existen modelos de gestión robustos para las operaciones y servicios de seguridad de las tecnologías de información?					
2	Dentro de los procesos de Gestión de Operaciones y Servicios de Seguridad pertenecientes a COBIT 5, considera usted que existen actividades con cierto grado de ambigüedad.					
3	Considera poco efectiva la gestión de operaciones y servicios de seguridad que propone COBIT 5?					
4	Considera usted que actualmente se requiere de un modelo de gestión de tecnologías de información enfocado en la gestión de operaciones y servicios de seguridad.					
5	Está usted de acuerdo con incorporar a los procesos de COBIT 5, actividades para la relación con los proveedores.					
6	Cree usted que es necesario incorporar una práctica de Gestión Financiera a los procesos de gestión de operaciones y servicios de seguridad que propone COBIT 5.					
7	Dentro de la administración de tecnologías de información, cree usted necesario incorporar a la división de tareas (segregación de deberes) como una actividad.					
8	Cree usted conveniente considerar a la Planificación de Niveles de Servicio para reforzar las actividades de la práctica de Gestionar los servicios de TI externalizados, que propone COBIT 5?					
9	Usted considera necesario incorporar la gestión de conocimiento como una práctica que complemente a las propuestas por COBIT 5 en la Gestión de Operaciones.					
10	Está usted de acuerdo en incorporar una actividad en COBIT 5, que permita la correlación de los eventos para ahorrar tiempo en la seguridad de soluciones.					

Firma del Experto