UNIVERSIDAD ANDINA DEL CUSCO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

PROPUESTA DE UN MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA SANTO DOMINGO DE GUZMÁN AGENCIA SICUANI BASADO EN EL MARCO DE REFERENCIA DE COBIT 5

TESIS PARA OPTAR EL TITULO DE INGENIERO DE SISTEMAS

Presentado por:
Jorge Luis Aguilar Inquel

Asesor: Mg. Luis Alberto Sota Orellana

Cusco – Perú

2019

ÍNDICE

Índice de Tablas ---- iv
Índice de Figuras ---- vi
Introducción ---- viii
Abstract ---- ix
CAPÍTULO 1 - Problema de investigación. ---- 1
1.1. Ámbito de influencia. ---- 1
1.1.1. Ámbito de influencia teórica. ---- 1
1.1.2. Área de dominio. ---- 1
1.1.3. Línea de investigación. ---- 2
1.2. Planteamiento del problema. ---- 2
1.2.1. Descripción de la situación actual del lugar de intervención. ---- 2
1.2.2. Descripción del problema. ---- 2
1.2.3. Formulación del problema. ---- 5
1.2.4. Objetivos. ---- 6
1.2.5. Justificación. ---- 6
1.2.6. Alcances y limitaciones. ---- 7
CAPÍTULO 2 - Marco Teórico. ---- 8
2.1. Antecedentes del desarrollo, implementación o transferencia tecnológica. ---- 8
2.2. Bases teórico – científicas. ---- 11
2.2.1 Modelo de gestión ---- 11
2.2.2 Dimensiones de los sistemas de información ---- 11
2.2.3 Seguridad ---- 12
2.2.4 Seguridad informática ---- 13
2.2.5 Seguridad de información ---- 15
2.2.6 Modelo de gobierno de la protección de los datos informáticos ---- 15
2.2.7 Importancia de la seguridad informática ---- 17
2.2.8 COBIT 5 ---- 17
2.2.9 COBIT 5 y la seguridad ---- 24
2.2.10 MAGERIT ---- 26
2.2.11 Matriz de riesgos ---- 26
CAPÍTULO 3 –Desarrollo de la propuesta del modelo de gestión de seguridad de la información. ---- 27
3.1 Diagnostico e identificación de las metas relacionadas de COBIT 5 ---- 27

3.2 Selección de los procesos de COBIT 5---------- 31
3.3 Identificación de los Activos de información.---------- 48
3.4 Identificación de amenazas por activo de información a través de la metodología MAGERIT ---------- 49
3.5 Evaluación de riesgos de los Activos de información---------- 59
3.6 Evaluación de las amenazas de los activos de información con los procesos de COBIT 5.---------- 79
3.7 Selección de las buenas practicas COBIT 5 ---------- 96
3.7.1 Gestionar el riesgo (APO12) ---------- 96
3.7.2 Gestionar la seguridad (APO13) ----------106
3.7.3 Gestionar la continuidad (DSS04) ----------112
3.7.4 Gestionar los servicios de seguridad (DSS05) ----------127
CAPÍTULO 4 – Resultados ----------144
4.1 Comprobación de la prospectiva. ----------144
4.2 Cumplimiento de objetivos.----------145
4.3 Contribuciones (impacto).----------146
Glosario----------147
Conclusiones----------148
Recomendaciones ----------149
Referencias----------150
Bibliografía ----------150
Anexos----------152
Anexo 1----------152
Anexo 2----------166
Anexo 3----------180
Anexo 4----------191
Anexo 5----------197
Anexo 6----------204

Índice de Tablas

Tabla 1 Objetivos corporativos de COBIT 5 con los objetivos de TI 28
Tabla 2 Objetivos relacionados con TI y procesos de Evaluar, Orientar y Supervisar (EDM)..... 32
Tabla 3 Objetivos relacionados con TI y procesos de Alinear, planear y organizar (APO) 35
Tabla 4 Objetivos relacionados con TI y procesos de Construir, adquirir e implementar (BAI)..... 38
Tabla 5 Objetivos relacionados con TI y procesos de Entregar, dar servicio y soporte (DSS) 41
Tabla 6 Objetivos relacionados con TI y procesos de Supervisar, evaluar y valorar (MEA) 44
Tabla 7 Resumen procesos COBIT 5 y Objetivos relacionados con TI..... 47
Tabla 8 Descripción de los activos de información..... 48
Tabla 9 Identificación de amenazas del activo de información-Equipos Informáticos.. 49
Tabla 10 Identificación de amenazas del activo de información-Servidores 50
Tabla 11 Identificación de amenazas del activo de información-Equipos de red local . 51
Tabla 12 Identificación de amenazas del activo de información-Periféricos y pendrives 52
Tabla 13 Identificación de amenazas del activo de información-Portátiles, tabletas y móviles 53
Tabla 14 Identificación de amenazas del activo de información-Oficinas..... 54
Tabla 15 Identificación de amenazas del activo de información-Personal propio 55
Tabla 16 Identificación de amenazas del activo de información-Apps Informáticas..... 56
Tabla 17 Identificación de amenazas del activo de información- Gestores de base de datos 57
Tabla 18 Identificación de amenazas del activo de información-Sistemas externos 58
Tabla 19 Valoración de los activos de información 59
Tabla 20 Parámetros de degradación. 59
Tabla 21 Degradación de la amenaza 60
Tabla 22 Valores del impacto..... 60
Tabla 23 Matriz de valoración de riesgos..... 60
Tabla 24 Evaluación de las amenazas y riesgos del activo de información – Equipos informáticos 61
Tabla 25 Evaluación de las amenazas y riesgos del activo de información – Servidores 63
Tabla 26 Evaluación de las amenazas y riesgos del activo de información – Equipos de red local 65
Tabla 27 Evaluación de las amenazas y riesgos del activo de información – Periféricos y pendrives..... 67
Tabla 28 Evaluación de las amenazas y riesgos del activo de información – Portátiles, tabletas y móviles 69
Tabla 29 Evaluación de las amenazas y riesgos del activo de información – Oficinas . 71
Tabla 30 Evaluación de las amenazas y riesgos del activo de información – Personal propio..... 73

Tabla 31 Evaluación de las amenazas y riesgos del activo de información – Aplicaciones informáticas 74
Tabla 32 Evaluación de las amenazas y riesgos del activo de información – Gestores de base de datos 76
Tabla 33 Evaluación de las amenazas y riesgos del activo de información – Sistemas externos 78
Tabla 34 Amenazas, riesgos y procesos de COBIT 5 - Equipos informáticos 79
Tabla 35 Amenazas, riesgos y procesos de COBIT 5 - Servidores 80
Tabla 36 Amenazas, riesgos y procesos de COBIT 5 - Equipos de red local 82
Tabla 37 Amenazas, riesgos y procesos de COBIT 5 - Periféricos y pendrives 84
Tabla 38 Amenazas, riesgos y procesos de COBIT 5 - Portátiles, tablets y móviles 85
Tabla 39 Amenazas, riesgos y procesos de COBIT 5 - Oficinas 87
Tabla 40 Amenazas, riesgos y procesos de COBIT 5 - Personal propio 89
Tabla 41 Amenazas, riesgos y procesos de COBIT 5 - Aplicaciones informáticas 90
Tabla 42 Amenazas, riesgos y procesos de COBIT 5 - Gestores de base de datos 92
Tabla 43 Amenazas, riesgos y procesos de COBIT 5 - Sistemas externos 94

Índice de Figuras

Ilustración 1 Mapa de ubicación de la Cooperativa Santo Domingo de Guzmán agencia Sicuani 1
Ilustración 2 Tarifario Plazo Fijo..... 3
Ilustración 3 Tarifario Ahorro libre 3
Ilustración 4 Tarifario Coopekids..... 4
Ilustración 5 Tipos de créditos..... 4
Ilustración 6 Dimensiones de los sistemas de información..... 12
Ilustración 7 El Objetivo de Gobierno: Creación de Valor. 18
Ilustración 8 Visión General de la Cascada de Metas de COBIT 5 19
Ilustración 9 Gobierno y Gestión de COBIT 5. 20
Ilustración 10 Marco de referencia Único e integrado de COBIT 5. 21
Ilustración 11 Catalizadores corporativos de COBIT 5..... 22
Ilustración 12 Las áreas claves de gobierno y gestión de COBIT 5. 23
Ilustración 13 Modelo de referencia de Procesos COBIT 5. 25
Ilustración 14 APO12.01 Recopilar datos - Buenas practicas..... 96
Ilustración 15 APO12.02 Analizar el riesgo - Buenas practicas 98
Ilustración 16 APO12.03 Mantener un perfil de riesgo - Buenas practicas 100
Ilustración 17 APO12.04 Expresar el riesgo - Buenas practicas..... 101
Ilustración 18 APO12.05 Definir un portafolio de acciones para la gestión de riesgos - Buenas practicas 102
Ilustración 19 APO12.06 Responder al riesgo - Buenas practicas..... 103
Ilustración 20 APO13.01 Establecer y mantener un SGSI - Buenas practicas 106
Ilustración 21 APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información - Buenas practicas 108
Ilustración 22 APO13.03 Supervisar y revisar el SGSI - Buenas practicas 110
Ilustración 23 DSS04.01 Definir la política de continuidad de negocio, objetivos y alcance - Buenas practicas..... 112
Ilustración 24 DSS04.02 Mantener una estrategia la continuidad - Buenas practicas . 114
Ilustración 25 DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio - Buenas practicas 116
Ilustración 26 DSS04.04 Ejercitar, probar y revisar el BCP - Buenas practicas..... 118
Ilustración 27 DSS04.05 Revisar, mantener y mejorar el plan de continuidad - Buenas practicas..... 119
Ilustración 28 DSS04.06 Proporcionar formación en el plan de continuidad - Buenas practicas..... 121
Ilustración 29 DSS04.07 Gestionar acuerdos de respaldo - Buenas practicas 123
Ilustración 30 DSS04.08 Ejecutar revisiones post reanudación - Buenas practicas..... 125
Ilustración 31 DSS05.01 Proteger contra software malicioso (software) - Buenas practicas 127
Ilustración 32 DSS05.02 Gestionar la seguridad de la red y las conexiones - Buenas practicas..... 129
Ilustración 33 DSS05.03 Gestionar la seguridad de los puestos de usuario final - Buenas practicas..... 131

Ilustración 34 DSS05.04 Gestionar la identidad del usuario y el acceso lógico - Buenas practicas 134
Ilustración 35 DSS05.05 Gestionar el acceso físico a los activos de TI - Buenas practicas 137
Ilustración 36 DSS05.06 Gestionar documentos sensibles y dispositivos de salida - Buenas practicas 139
Ilustración 37 DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad - Buenas practicas 141

Introducción

La tecnología y formas de comunicarse cambian permanente, por lo que las entidades financieras han hecho uso de herramientas tecnológicas que les permite gestionar las tecnologías de información tanto para el uso de sus trabajadores y el uso de sus clientes. Hoy en día la seguridad informática se ha convertido en unas las principales preocupaciones de las entidades financieras, ya que el más valioso activo que ellas tienen es la información.

La Cooperativa de Ahorro y Crédito Santo Domingo de Guzmán agencia Sicuani no cuenta con ningún modelo, plan, gestión, o cualquier tipo de sistema que proteja la información que esta posee. Al no contar con un modelo de gestión de seguridad de la información hace que dicha información, que es el activo más valioso para toda entidad, este vulnerable para todo tipo de ataques y amenazas, la seguridad informática se basa en resguardar el acceso a su confidencialidad, integridad y disponibilidad. La presente investigación propone un modelo de gestión de seguridad de la información para dicha entidad financiera, la cual se basa en el marco de referencia de COBIT 5, además de apoyarnos para la evaluación de las amenazas con la metodología de análisis y gestión de riesgos MAGERIT v3, la cual busca que contribuya al mejoramiento de la gestión, apoyando los procesos para alcanzar una mayor eficiencia y transparencia en su ejecución, que facilite la administración y el control de los recursos y que brinde información objetiva y oportuna para la toma de decisiones en todos los niveles, asimismo se espera poder reducir los riesgos de ocurrencia de las amenazas, y en caso ocurran saber cómo responder ante esas amenazas, se espera que con la propuesta del modelo de gestión de seguridad de la información la cooperativa pueda crecer y mejorar en la protección de sus datos además de hacer más competitiva entre las empresas de este rubro.

Abstract

En la presente investigación se desarrolla la propuesta de un modelo de gestión de seguridad de la información para la Cooperativa Santo Domingo de Guzmán agencia Sicuani basado en el marco de referencia de COBIT 5, para el desarrollo de esta propuesta se usó la cascada de metas que COBIT5 propone y el uso de sus procesos y sub procesos y también las buenas practicas que estas recomiendan.

Por lo cual en el Capítulo I- Problema de investigación, hacemos referencia al área de dominio de este estudio, y además de la línea de investigación, posteriormente planteamos la descripción del problema que se suscita en el área de investigación y vemos los objetivos a realizar en el presente estudio.

Además en el Capítulo II – Marco Teórico, se da las bases teóricas para la investigación y también se desarrolla los antecedentes nacionales e internacionales que se toman en cuenta para apoyar la presente investigación.

En el Capítulo III – Prospectiva Tecnológica, se describe cómo es que se hará y con qué materiales nos apoyaremos para la solución del estudio.

En el Capítulo IV – Resultados, se desarrolla cuáles fueron los resultados reflejados del estudio realizado la perspectiva tecnología y los objetivos realizados.

CAPÍTULO 1 - Problema de investigación.

1.1. Ámbito de influencia.

1.1.1. Ámbito de influencia teórica.

La seguridad de la información se encarga de proteger los sistemas implantados en las empresas a través de un cúmulo de habilidades y medidas que logran controlar todos los datos que se manipulan. Lo primordial en estos sistemas es que se justifican en nuevas tecnologías, por tanto esta se encarga de proteger la información que está disponible en el sistema, y de gestionar a los usuarios. Por otra parte no se podrá hacer ninguna modificación en los datos, si es que no son por usuarios autorizados.

La seguridad de la información tiene el trabajo de garantizar estas tres condiciones primordiales:

- Sensible
- Crítica
- Valiosa

Debe ser sensible, porque solo las personas con el nivel de autorización adecuado puedan ingresar. Debe ser crítica, porque gracias a ello las empresas pueden hacer sus operaciones sin demasiados riesgos. Debe ser valiosa, ya que estos gestionan la información y son importantes para la evolución de la empresa. La seguridad de la información tiene que resolver los riesgos, examinar, evitar y además descubrir soluciones inmediatas para eliminarlos si fuera el caso. (Universitat de Barcelona, 2019)

Existen diferentes tipos de modelos como: COBIT, ITIL, LEY SOX, COSO entre otros.

1.1.2. Área de dominio.

La Organización Empresarial y Gestión de Información, están dentro una de las áreas de dominio de la Escuela Profesional de Ingeniería de Sistemas.

De acuerdo a (Ramirez Vera, 2015) “La informática empresaria permite el procesamiento útil y necesario para el correcto funcionamiento de una empresa, con lleva también al orden adecuado de la información del interior de la organización, ayudando a procesar información de cómo conecta nuestra organización con las demás organizaciones y colaborar con la toma de decisiones.”

La organización empresarial es un conjunto de personas que trabajan coordinadamente y concertadamente con el objeto de lograr metas y producciones es la suma de esfuerzos y trabajo en equipo.

La gestión de la información comprende la obtención de la información adecuada, en la forma correcta, para la persona indicada, al coste adecuado, en el momento oportuno, en el lugar apropiado y articulando todas estas operaciones para el desarrollo de una acción correcta. Así mismo, comprende procesos relativos al registro, procesamiento, definición de la información.

La gestión de la información tiene como objetivos principales, agrandar la valoración y los beneficios precedentes de la utilización de la información, disminuir el coste de

compra, procesamiento y uso de la información, definir las responsabilidades para su uso, eficiente y económico de la información y asegurar un suministro continuo de la información. (Perez-Montoro, 2010).

1.1.3. Línea de investigación.

Sistemas de información.

Un sistema de información es un conjunto de datos que interactúan entre sí con la finalidad de satisfacer las demandas de información para una organización, y así poder enriquecer la sabiduría para apoyar la toma de decisiones y el desarrollo de sus acciones. (Dangel, 2010).

La seguridad de la información se basa en confidencialidad ya que a través de ella la seguridad de la información garantiza que los datos que están guardados en el sistema no se divulguen a otras entidades o individuos que no están autorizados para acceder a esa información. La disponibilidad que es toda la información que se encuentre recogida en el sistema tiene que estar siempre a disposición de los usuarios autorizados en cualquier momento que ellos necesiten acceder a ella. Y la integridad para que el sistema sea veraz los datos no deben manipularse. Así se garantiza que la información recogida sea exacta y no haya sido modificada a no ser que algún usuario autorizado lo haya hecho por orden expresa.

1.2. Planteamiento del problema.

1.2.1. Descripción de la situación actual del lugar de intervención.

En 1991 se creó el famoso WWW(World Wide Web) que a su vez dio paso a la creación del internet, y a su uso de nivel mundial, desde entonces las conectividades de red o las creaciones de redes fueron las más atacadas siendo así que nace la seguridad informática para poder mitigar estos ataques resguardando los servidores, equipos y otros activos de información accesibles públicamente desde el internet, inspeccionando de esta manera por cortafuegos (firewalls),y de esta manera poder robar información para luego exponerla y poner en riesgo al negocio.

La seguridad de la información con el pasar de los años ha estado tomando mucha importancia en todas las empresas ya que pueden contar con procedimientos de seguridad para poder mitigar los riesgos, minimizar la vulnerabilidad de su información, y evitar la manipulación de datos por usuarios no autorizados. Existen diferentes modelos de seguridad de información que permiten identificar, seleccionar, evaluar, identificar y gestionar las vulnerabilidades de las empresas, la información no se puede proteger al 100%, pero si se puede lograr disminuir o borrar las imperfecciones.

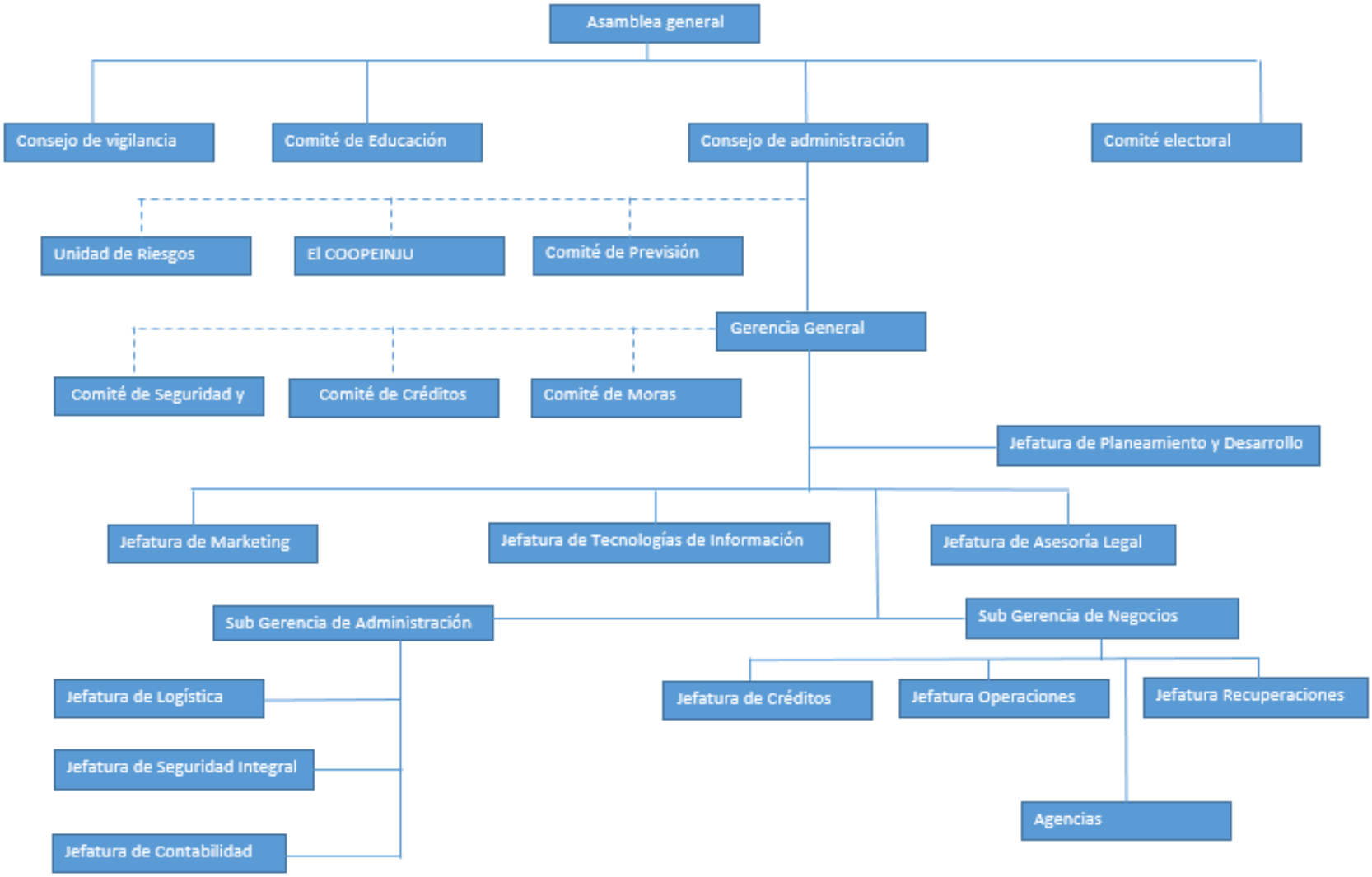
La vulnerabilidad en las empresas no discrimina ya que pueden ser atacadas todo tipo de ellas, grandes, pequeñas, privadas, públicas, las consecuencias que estos ataques tienen son el robo de información y el desprestigio de la empresa, estos ataques pueden ser cuantificados en pérdidas de millones de dólares. Con la finalidad de mitigar estos errores se han desarrollado diferentes modelos de ciberseguridad para diferentes sectores lo que les ha permitido minimizar los riesgos y asegurar el bien más preciado que es la información. (Gelbstein, 2011)

El 19 de noviembre de 1970 la tercera orden de Santo Domingo - Cusco se reunió y coordino mediante en el entonces líder el Reverendo Padre Manuel Alvarez Percca, para fundar la Cooperativa de Ahorro y Crédito Santo Domingo de Guzmán Ltda. N° 001 VII Cusco un 23 de enero de 1971, con la finalidad de promover el hábito del ahorro y la cooperación financiera entre sus socios.

La Cooperativa de Ahorro y Crédito "Santo Domingo de Guzmán" Ltda. Mediante un Fallo Directoral No. 1073-CAAE-ORAMNS-VII-Cusco. La cooperativa de Ahorro y Crédito "Santo Domingo de Guzmán" se encuentra inscrita Libro de Cooperativas de los Registros Públicos del Cusco, tomo 01, Folio 269, Asiento No. 05 del Registro de Cooperativas de los Registros Públicos del Cusco y con autorización de Inscripción en el Registro Oficial de Cooperativas de Ahorro y Crédito de la Superintendencia de Banca y Seguros, mediante la Resolución SBS No. 033-95 de fecha 10 de Enero de 1995.

La cooperativa gracias a la confianza de sus socios llego a posicionarse como una de las mejores del sur del Perú gracias a su desempeño laboral y a la entrega de toda la mancomunidad de oficinas, pretendiendo apegarnos siempre a los ideales y normas creadas por nuestro fundador y los que gobiernan nuestra cooperativa, logrando así posicionarnos en diferentes partes del Cusco y del Perú.

Organigrama de la Cooperativa Santo Domingo de Guzmán



En la jefatura de Tecnologías de Información, la oficina cuenta:

- Jefe de proyectos tecnológicos y desarrollo de software
- Jefe de infraestructura y operaciones
- Coordinador de desarrollo de software
- Coordinador de producción y mantenimiento
- Coordinador de infraestructuras
- Asistente de redes y comunicaciones
- Administrador de base de datos
- Analista de desarrollo de Software
- Programador
- Analista de calidad de software
- Asistente de soporte y producción
- Operador TI

La agencia de Sicuani se encuentra ubicada en el Jr. 28 de Julio N° 134-136 - Plaza de Armas.

Ilustración 1 Mapa de ubicación de la Cooperativa Santo Domingo de Guzmán agencia Sicuani
Fuente: Google Maps

La Cooperativa de Ahorro y Crédito Santo Domingo de Guzmán agencia Sicuani cuenta con 22 trabajadores y en su infraestructura tecnológica (Hardware y Software) cuenta con:

Hardware:

- 1 UPC
- 4 Canon Impresora Multifuncional Maxify MB-5410
- 2 EPSON TM-T20II - TICKETERA TERMICA USB - ARTEUS COMP SAC
- 6 Laptop 15.6" Aspire 3
- 8 Cámaras Full HD KIT-XVR-8C8CH Dahua
- 2 PC Desktop HP Prodesk 400 G4
- 2 Monitor Samsung LS22F350FHLX
- 2 Teclado Genius Alambrico Usb Km160 Negro
- 2 Mouse Genius Alambrico Usb Km160 Negro
- 1 Switch Cisco Gigabit Ethernet SG112-24

Software:

- BESTER – Software de gestión de operaciones de ventanilla.
- RENIEC – Software de control de ciudadanos.
- EXPERIAN y EQUIFAX - Software de evaluación crediticia de clientes.
- SUNARP- Software de información de bienes.

1.2.2. Descripción del problema.

Hoy en día las empresas están expuesta a la sustracción o extravió de información, siendo la información el recurso valioso de muchas empresas, si la información sustraída es expuesta la empresa tiende a tener una mala imagen y los clientes tienden a abandonar las empresas, una empresa sin clientes no genera ingresos, es por eso que las empresas están optando en poner en marcha modelos de gestión de seguridad para proteger el bien más valioso que es la información, en junio del 2017 la empresa Maersk Line fue atacada y filtraron un virus ramsonware con el cual lograron robar información de dicha empresa la cual le costó millones de dólares.(Sarabia, 2017)

La Cooperativa de Ahorro y Crédito Santo Domingo de Guzmán (CACSDG) agencia Sicuani genera ingresos como la mayoría de entidades financieras, a base de créditos siendo esta una de las cooperativas que entregan mayor intereses en:

Plazo fijo:

>> Moneda Nacional S/			>> Moneda Extranjera $		
Plan	**TEA**	**Importe Mín**	**Plan**	**TEA**	**Importe Mín**
30 Días	3.26%	S/ 300.00	30 Días	0.13%	$100.00
60 Días	4.51%	S/ 300.00	60 Días	0.13%	$100.00
90 Días	4.70%	S/ 300.00	90 Días	0.14%	$100.00
120 Días	5.06%	S/ 300.00	120 Días	0.15%	$100.00
180 Días	5.42%	S/ 300.00	180 Días	0.18%	$100.00
270 Días	5.78%	S/ 300.00	270 Días	0.20%	$100.00
360 Días	6.50%	S/ 300.00	360 Días	0.25%	$100.00
720 Días	7.23%	S/ 300.00	720 Días	0.31%	$100.00

Ilustración 2 Tarifario Plazo Fijo
Fuente: Cooperativa Santo Domingo de Guzmán

En ahorro libre:

Socio	TEA Soles S/	TEA Dólares $
Persona Natural	1.8%	0.10%
Persona Juridica	1.8%	0.10%

Ilustración 3 Tarifario Ahorro libre
Fuente: Cooperativa Santo Domingo de Guzmán

En sus cuentas Coopekids:

Socio	TEA Soles S/	TEA Dólares $
Persona Natural	4.00%	0.11%

Ilustración 4 Tarifario Coopekids
Fuente: Cooperativa Santo Domingo de Guzmán

Además en los diferentes tipos de créditos:

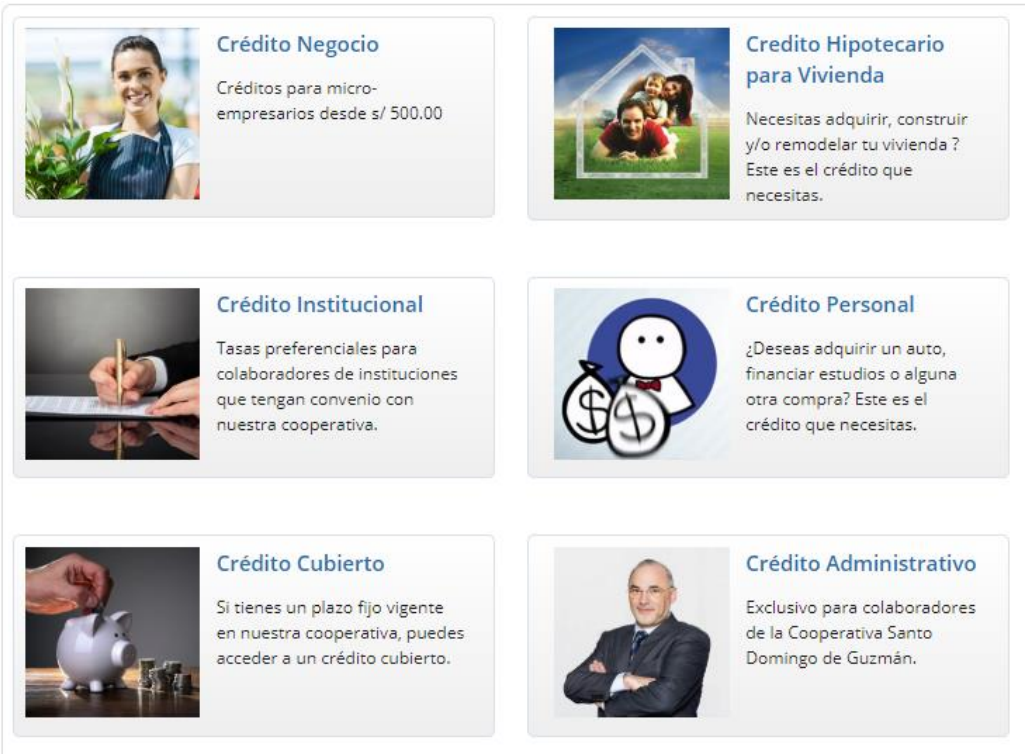


Ilustración 5 Tipos de créditos
Fuente: Cooperativa Santo Domingo de Guzmán

La CACSDG cuenta con las aportaciones de los clientes (que también para la cooperativa son considerados como socios), la CACSDG agencia Sicuani maneja gran cantidad de información de sus socios clientes, los cuales corren riesgo en la gestión de su información, porque mediante lo observado y vivido en la cooperativa ellos no cuenta con ningún modelo de gestión de seguridad de la información, no saben cómo actuar ante cualquier amenaza existente, por eso no pueden garantizar que la información este resguardada y además que no será filtrada por malos trabajadores, clientes insatisfechos, ex trabajadores, competencia y proveedores.

En la CACSDG agencia Sicuani tiene diferentes amenazas por cada activo de información, lo cual deben disminuir en su probabilidad de ocurrencia, la problemática es el no controlar el grado de exposición de información hacia los clientes y hacia los trabajadores, la gestión de usuarios es muy deficiente, las acciones correctivas de la CACSDG agencia Sicuani no cuentan con un modelo

de gestión, ni con ninguna estrategia de seguridad, estas amenazas desafían los modelos de gestión de seguridad de información y pueden causar perdida de información, pero ahora existen técnicas, modelos, estándares y diferentes maneras de gestionar la seguridad para estar precavidos ante las amenazas tecnológicas existentes.

Las empresas u organizaciones actualmente optaron por frameworks para así poder tener un control de la seguridad de su información, ya que este es un bien muy valioso, existen diferentes marcos de referencia como son: COBIT 5, ISO 27001, ITIL, entre otros, todos estos tienen practicas sugeridas y también su manera de cómo gestionar la seguridad de la información.

La alternativa de solución es proponer un modelo de gestión de seguridad de la información y usar lar buenas prácticas sugeridas por COBIT 5, ya que esta elabora un compendio de defensas que responsabilizaran de conducir todo el sistema, esta describe y establece los propósitos, directrices, objetivos, alcances, responsabilidades y políticas principales de los modelos de gestión de seguridad de la información. Así como mecanismos que garanticen de forma eficaz la planificación, operación y control en los procesos de la seguridad. También se realizan instrucciones para verificar las listas de control formularios que describen como realizar las tareas y actividades relacionadas con la seguridad. Adicionalmente se recomienda tener registros de la evidencia de que estos requisitos fueron cumplidos mediante el modelo de gestión por el que la empresa opto.

1.2.3. Formulación del problema.

¿Cómo afecta a la Cooperativa Santo Domingo de Guzmán agencia Sicuani no contar con un modelo de gestión de seguridad de la información?

1.2.4. Objetivos.

General.

Proponer un modelo de gestión para la seguridad de la información de la Cooperativa Santo Domingo de Guzmán agencia Sicuani usando el marco de referencia de COBIT 5.

Específicos.

1. Diagnosticar la situación actual de la Cooperativa Santo Domingo de Guzmán agencia Sicuani en cuanto a la seguridad de su información.
2. Reconocer los activos de información de la Cooperativa Santo Domingo de Guzmán agencia Sicuani, para poder mitigar las amenazas.
3. Identificar los procesos de COBIT 5 en la Cooperativa Santo Domingo de Guzmán agencia Sicuani, para proponer el modelo de la gestión de la seguridad de su información.
4. Seleccionar las buenas prácticas propuestas por COBIT 5, de acuerdo a los procesos que se ajusten a los requerimientos identificados en la Cooperativa Santo Domingo de Guzmán sede Sicuani.

1.2.5. Justificación.

Hoy en día las empresas están interesadas en la seguridad informática ya que de esta manera protegen sus activos de información, el presente estudio propone un modelo de gestión para la seguridad de la información que además estará basada en COBIT 5, este es un estándar internacional, que la direccionamos a la CACSDG agencia Sicuani, y además para cumplir con la resolución S.B.S. N° 2116 – 2009.

La empresa no cuenta con ningún modelo de este tipo como anteriormente se menciono. El uso de COBIT 5 representa un aporte importante a la CACSDG agencia Sicuani porque éste enfoque se basa en un modelo para seguir las buenas prácticas la cual nos permitirá minimizar los riesgos y además de saber actuar ante ellos cuando exista las amenazas en cuanto al robo, alteración o pérdida de información ya que estas empresas están expuestas a ataques, una adecuada gestión de riesgo nos permitirá saber actuar ante posibles eventos de riesgo.

La elaboración de este modelo de gestión para la seguridad de la información propuesto en este trabajo de investigación, se hace con el propósito de ser un marco de referencia para que en un futuro esta pueda ser implementada y además cuente con la seguridad para la información en la CACSDG agencia Sicuani y como grande beneficio es el resguardar su activo más valioso como es la información, minimizar los ataques contra este y crecer en su ámbito para que de esta manera mejore en cuanto a sus competencias.

1.2.6. Alcances y limitaciones.

El alcance de la presente investigación estará enfocada en desarrollar una propuesta de un modelo de gestión para la seguridad de la información en el ámbito exclusivamente de la CACSDG agencia Sicuani.

Limitaciones:

- Falta de interés y presupuesto para la capacitación de los trabajadores en el marco de trabajo de COBIT.
- Tiempo escaso en consultores en proyectos de COBIT.
- Bajo presupuesto para la adquisición de textos sobre COBIT.
- Falta de organización y tiempo del personal de TI para consultas o reuniones de trabajo.
- Escasa bibliografía sobre proyectos de entidades financieras con COBIT.

CAPÍTULO 2 - Marco Teórico.

2.1. Antecedentes del desarrollo, implementación o transferencia tecnológica.

"PLAN DE MEJORA DE LA SEGURIDAD DE INFORMACIÓN Y CONTINUIDAD DEL CENTRO DE DATOS DE LA GERENCIA REGIONAL DE EDUCACIÓN LA LIBERTAD APLICANDO LINEAMIENTOS ISO 27001 Y BUENAS PRÁCTICAS COBIT" – Tesis de pre grado de la Universidad Privada Antenor Orrego – Trujillo.

Resumen: La presente tesis trata sobre Elaborar un plan de mejora de seguridad de la información y continuidad del centro de datos, y mostrar los resultados obtenidos de la auditoria de sistemas, utilizando la metodología MAIGTI, y usando los marcos de referencia de ISO 27001 y buenas prácticas de COBIT 4.0, en el desarrollo de los capítulos podremos ver las definiciones, buenas practicas, lineamientos y metodología utilizada así como también la situación actual del centro de datos de la GRELL y la auditoría realizada, donde se obtienen los procesos adecuados por el ISO 27001 y la selección de las buenas prácticas de COBIT 4.0.

Comentario: La presente tesis se usó para apoyar el uso de COBIT y sus buenas prácticas además de ver las diferencias con el ISO 27001 y de esta manera tener mejores conocimientos para aplicar al modelo propuesto.

"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA UNA COMPAÑÍA DE SEGUROS" – Tesis de pre grado de la Pontificia Universidad Católica del Perú – Lima.

Resumen: Trata de la elaboración de un SGSI para una compañía de seguros, ya que según la Superintendencia de Banca, Seguro y AFP, en el 2009, elaboro la circular G140, que pacta en que todas las empresas peruanas que son reguladas por este organismo deben contar con un Sistema de Gestión de Seguridad de Información, usaron diferentes estándares mundiales como son COBIT e ITIL.

Comentario: La presente tesis me ayudo a cómo aplicar COBIT 4.1 en una empresa, y así poder ver las diferencias con COBIT 5 para entender de mejor manera como es que mejoro COBIT 5.

"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA UN INSTITUTO EDUCATIVO" - Tesis de pre grado de la Pontificia Universidad Católica del Perú – Lima.

Resumen: La tesis tiene una introducción que habla sobre las incidencias que ocurrieron en el mundo y en el Perú, justifican el uso de programas de seguridad informáticos, habla sobre la pérdida de clientes en instituciones educativas por la filtración de información y también nombra algunos estándares con los cuales elaboraran un SGSI.

Comentario: El presente trabajo me ayudo en mi investigación para diferenciar los modelos de los y los sistemas de seguridad además de poder ver el uso de la ISO 270001 y COBIT 5.

"SEGURIDAD EN INFORMÁTICA (AUDITORIA DE SISTEMAS)" – Tesis de pos grado de la Universidad Iberoamericana – México FC.

Resumen: La tesis nos pone en contexto sobre todo lo que es seguridad de la información y seguridad informática, comprende sobre las leyes establecidas en México y como la seguridad está al servicio de las empresas solo que no hay mucha cultura sobre el tema, la idea del trabajo es crear un plan de seguridad de información contra todo tipo de ataques tantos físicos como digitales.

Comentario: La presente tesis me ayudo a comprender más sobre la seguridad informática para poder aplicarla a mi tesis.

"PROPUESTA TECNOLÓGICA BASADA EN COBIT 5 APLICADA A LA GESTIÓN DE LA TI EN LA EIS" – Tesis de pre grado de la Escuela Superior Politécnica de Chimborazo - Ecuador

Resumen: Esta tesis trata sobre cómo se gestionó COBIT 5 y como se aplicó a la escuela de sistemas, se aplica los pasos se COBIT 5 y se aplican diferentes herramientas de obtención de resultados, además se hace una comprobación del antes y el después de COBIT 5.

Comentario: Esta tesis me ayudo a saber cómo COBIT 5 mejora la administración de las TI en una empresa y la seguridad de la información.

"DISEÑO DE UN MANUAL DE MEJORA DE PROCESOS DE TECNOLOGÍAS DE INFORMACIÓN PARA EL DEPARTAMENTO DE TI DE OÍL POWER UTILIZANDO EL MARCO DE REFERENCIA COBIT" Tesis de postgrado de la Universidad San Francisco de Quito - Ecuador.

Resumen: La tesis trata de la elaboración de un manual de mejora de los procesos tecnológicos de información para la empresa Oíl Power, te explica el uso de COBIT en el ámbito de la oficina de Tecnologías de Información, además se logra obtener el manual y la aplicación de tal.

Comentario: Esta tesis me ayudo en comprender como de importante es el aporte del departamento de TI a toda una empresa y la relevancia de un plan de seguridad de información, bajo los parámetros definidos de COBIT e ISACA.

“DISEÑO DE UN MODELO DE GOBIERNO DE TI UTILIZANDO EL MARCO DE TRABAJO DE COBIT 5 CON ENFOQUE EN SEGURIDAD DE LA INFORMACIÓN. CASO DE ESTUDIO: UNA EMPRESA PRIVADA ADMINISTRADORA DE FONDO DE PENSIONES” – Tesis de pre grado de la Pontificia Universidad Católica del Perú – Lima

Resumen: La tesis presente te pone en contexto sobre la importancia de la información además del uso de esta ya que es un bien muy valioso, trata sobre el uso de COBIT 5 y como esta herramienta la usan para poder crear un modelo de gobierno de TI y el uso de las buenas prácticas de TI de COBIT 5

Comentario: Esta tesis me ayudo en ver la diferencia de hacer un gobierno con COBIT 5 y crear un modelo.

2.2. Bases teórico – científicas.

2.2.1 Modelo de gestión

Los modelos de gestión que existente acceden a que las empresas puedan explotar las practicas recomendadas para el área de TI.

Los modelos apilan las prácticas, guías y recomendaciones más idóneas en el sector de la gestión de los Servicios de IT, los dueños de las empresas u organizaciones ya pueden mejorar la relación con sus clientes.

El uso de los modelos de gestión, aprovecha las ventajas además de que es un factor diferencial entre otras empresas.

Las metodologías se adaptan a las empresas por lo tanto cuando se hace un proyecto tecnológico los inicios y fines no son claros ni definidos.

Por el contrario, la aproximación a este tipo de iniciativas debe ser realizada bajo el paradigma de los programas, o planes de acción continuada que se realizarán en la organización de forma cíclica y que pasarán a formar parte de la propia cultura empresarial.

En el área de soluciones, la utilización de Modelos de Gestión permite dar una coherencia completa a los diseños funcionales realizados con las prácticas recomendadas, permitiendo que las implantaciones tengan una visión global de los objetivos tácticos y estratégicos a lograr por el área de TI de nuestros clientes. (G2, 2019)

2.2.2 Dimensiones de los sistemas de información

Para comprender por completo los sistemas de información, debe conocer las dimensiones más amplias de organización, administración y tecnología de la información de los sistemas, junto con su poder para proveer soluciones a los desafíos y problemas en el entorno de negocios. Nos referimos a esta comprensión más extensa de los sistemas de información, que abarca un entendimiento de los niveles gerenciales y organizacionales de los sistemas, así como de sus dimensiones técnicas.

Ilustración 6 Dimensiones de los sistemas de información
Fuente: Sistemas de Información Gerencial – K. Laudon y J. Laudon

Las **organizaciones** tienen una estructura compuesta por distintos niveles y áreas. Sus estructuras revelan una clara división de labores. La autoridad y responsabilidad en una empresa de negocios se organizan como una jerarquía, o estructura de pirámide. Los niveles superiores de esta jerarquía consisten en empleados gerenciales, profesionales y técnicos, mientras que los niveles base de la pirámide consisten en personal operacional.

El trabajo de la gerencia **(Administración)** es dar sentido a las distintas situaciones a las que se enfrentan las organizaciones, tomar decisiones y formular planes de acción para resolver los problemas organizacionales. Los gerentes perciben los desafíos de negocios en el entorno; establecen la estrategia organizacional para responder a esos retos y asignan los recursos tanto financieros como humanos para coordinar el trabajo y tener éxito.

La **tecnología de la información** es una de las diversas herramientas que utilizan los gerentes para lidiar con el cambio. El hardware de computadora es el equipo físico que se utiliza para las actividades de entrada, procesamiento y salida en un sistema de información. Consiste en lo siguiente: computadoras de diversos tamaños y formas (incluyendo los dispositivos móviles de bolsillo); varios dispositivos de entrada, salida y almacenamiento; y dispositivos de telecomunicaciones que conectan a las computadoras entre sí.

2.2.3 Seguridad

La seguridad es la ausencia del riesgo además que es la protección de cualquier peligro, el alcance de un nivel de seguridad óptimo necesita que los individuos,

las comunidades, gobiernos y otros interventores creen y mantengan las siguientes condiciones, y esto, sea cual sea el nivel de vida considerado:

- Un ambiente de buena relaciones entre todos.
- La prevención de heridas
- Control de daños.
- El respeto a los valores y a la integridad física.
- El acceso a medios eficaces de prevención, control y rehabilitación.

Estas condiciones puedes ser garantizada a través de acciones sobre el medio ambiente y los comportamientos. (INSPQ, 1998)

2.2.4 Seguridad informática

El uso de medidas de seguridad informática hace que no esté comprometida la información, cualquier medida de seguridad es tomada en cuenta por las empresas.

Además, (Gómez, 2007) considera destacar los siguientes aspectos con relación a la seguridad informática:

1. Ejecutar las regulaciones legales aplicables a cada tipo de organización.
2. Controlar el ingreso a los servicios ofrecidos e información guardada por un sistema informático.
3. Controlar el ingreso y emplear fichas protegidas por las normas.
4. Identificación de la información o mensajes de los creadores.
5. Verificar el uso de un sistema informático.

Importantes objetivos de la seguridad informática:

- Ganar la fidelidad de los usuarios.
- Proteger los datos mediante una normativa.
- Proteger y reservar los datos del usuario.
- Libre ingreso a la data.
- Disminuir los incidentes informáticos.
- Prevenir los ataques informáticos y filtración de virus

Para poder alcanzar estos objetivos, la gestión de la seguridad informática debe llevar a cabo las siguientes funciones:

- Confidencialidad.
- Disponibilidad.
- Integridad.

En los procesos se deben contemplar los siguientes aspectos de organización:

- Personas
- Tecnología
- Código de utilización.
- Distribución organizativa

El desarrollo de medidas de seguridad informáticas, trata de proteger a la información, las medidas básicas por simple sentido común son, hacer copas de seguridad y controlar el nivel de acceso, la seguridad en una organización tiene que tener estos tres puntos:

- Adaptación a los requisitos del marco legal y de las exigencias de los clientes
- Gestión integral de la seguridad de la información
- Certificación de la gestión de la seguridad de la información

Para lograr alcanzar los objetivos y desarrollar el sistema de seguridad informática es importante que la organización aclare, planee e implemente una cantidad de estrategias, programas y acciones.

2.2.5 Seguridad de información

La seguridad de la información permite asegurar la identificación, valoración y gestión de los activos de información y sus riesgos, en función del impacto que representan para una organización. Es un concepto amplio que no se centra en la protección de las TIC sino de todos los activos de información que son de un alto valor para la institución.

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

Las dimensiones de la seguridad están constituidas por tres conceptos fundamentales:

- Confidencialidad: propiedad que permite que la información solo esté disponible o sea revelada a personas, entidades o procesos autorizados.
- Integridad: propiedad de la exactitud e integridad de la información.
- Disponibilidad: propiedad de la información para estar accesible y utilizable al solicitarlo una entidad autorizada.

La importancia de la seguridad de la información

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

Existen dos factores importantes de la seguridad de la información:

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

2.2.6 Modelo de gobierno de la protección de los datos informáticos

Los Sistemas de Gestión de la Seguridad de la Información (SGSI) son aquellos que preservan la confidencialidad, integridad y disponibilidad.

Fundamentos:

Para decir que un SGSI está siendo usado de forma correcta se tiene que medir sus niveles de seguridad en cuanto a:

- Confidencialidad.
- Integridad.
- Disponibilidad.

Si uno conoce el ciclo de vida de la información sabe que es relevante optar con el uso de un SGSI para no correr riesgos empresariales y además de tener un plus frente a otras empresas.

Utilización

La información es uno de los activos más valiosos para las empresas, la confidencialidad, integridad y disponibilidad de dicha información, es esencial para sustentar los niveles de competencia frente a otras empresas, y además de que tiene que ser rentable y cuidar la imagen de la empresa para que exista mejor entrada económica.

Las empresas y los sistemas de información se encuentran descubiertos a ciertas amenazas informáticas, y estas a su vez al activo más preciado que es la información, existen un sinfín de ataques, espionaje, extracción, etc. de virus para poder atacar la información, además de que no solo corre peligro la información sino también los equipos informáticos en general.

El cumplimiento de algunas leyes que norman algunos países exigen que las empresas tengan un forma de protección de su información es por eso que los SGSI ya se están haciendo un estándar en todo el mundo para cada tipo de organización.

Los niveles de seguridad creados para cada empresa tienen que estar en constante actualización porque los atacantes siempre inventan o ven alguna forma de infiltrarse en los sistemas de las organizaciones.

El modelo de gestión de la seguridad tiene que contemplar unos procedimientos adecuados y planificar e implementar controles de seguridad que se basan en una evaluación de riesgos y en una medición de la eficiencia de los mismos.

Beneficios

- Reducir el riesgo de pérdida y/o robo de la información.
- Las amenazas y los manuales son continuamente examinados.
- Se asegura se fiabilidad de los clientes y asociados de la entidad.
- Las auditorías colaboran en reconocer las deficiencias del SGSI y los campos a mejorar.
- Simplifica la incorporación de sistemas de gobierno.
- Avala la perseverancia de la compañía si hubiera algún percance.
- Obedece a las leyes existentes sobre los datos privados, atributos intelectuales otras.
- La reputación de la entidad mejora a niveles internacionales.
- Mejora la seguridad y aclara las reglas los servidores de la entidad.
- Minoriza los gastos y además mejora los procesos y el servicio.
- Aumenta en entusiasmo en los trabajadores y complace al personal.
- Mejora de seguridad en todo lo que es gestión de procesos tecnológicos.

2.2.7 Importancia de la seguridad informática

Para medir el nivel de seguridad primero se tiene que analizar los incidentes de todo ámbito tecnológico de la empresa para poder gestionar unos sistemas de seguridad de la información, los incidentes siempre van a existir pero sin embargo los vamos a poder controlar.

Todos los sistemas de gestión de la seguridad de la información que se usan, priorizan la gestión de incidentes, con el objeto de poder detectarlo en el menor tiempo posible y así poder actuar, mitigar y controlar los incidentes.

¿Cómo beneficia a las grandes organizaciones la seguridad de la información?

- La gestión de incidente permite a la empresa ya tener un plan de seguridad apenas pase algo
- Presentar las posibles soluciones para la mitigación correctiva o preventiva de estos incidentes
- Tener un registro de evidencias para cualquier inoportuno.
- Tener claro el modelo son el que se gestiona los incidentes de seguridad
- Es imprescindible que la gestión de incidentes sea la base para iniciar un proceso de gestión integral en la seguridad de la información(Espitia, 2015)

2.2.8 COBIT 5

Se define como un aglomerado de instrumentos de soporte que se pueden emplear por los directores de las empresas para minimizar la rendija que existe entre los requerimientos de control, los temas técnicos y los riesgos del negocio.

De esta manera COBIT 5 permite controlar de mejor manera las TI de las organizaciones. Al emplear este marco, hace que el valor de las áreas asociadas a TI incremente su importancia. Cuando COBIT inicio se propuso para la auditoria de TI, y seguidamente en su evolución paso para el control de gestión de TI, gobierno de TI y actualmente con es un enfoque global para el gobierno de TI.

COBIT 5 cuenta con 5 principios para adoptar la gestión de TI:

Principio 1: Satisfacer las necesidades de las partes interesadas:
Las empresas existen para crear valor para sus accionistas. En consecuencia, cualquier empresa, comercial o no, tendrá la creación de valor como un objetivo de Gobierno. Creación de valor significa conseguir beneficios a un coste óptimo de los recursos mientras se optimiza el riesgo. Los beneficios pueden tomar muchas formas, por ejemplo, financieros para las empresas comerciales o de servicio público para entidades gubernamentales.

Las empresas tienen muchas partes interesadas, y 'crear valor' significa cosas diferentes — y a veces contradictorias — para cada uno de ellos. Las actividades de gobierno tratan sobre negociar y decidir entre los diferentes intereses en el valor de las partes interesadas. En consecuencia, el sistema de gobierno debe considerar a todas las partes interesadas al tomar decisiones sobre beneficios, evaluación de riesgos y recursos. Para cada decisión, las siguientes preguntas pueden y deben hacerse: ¿Para quién son los beneficios? ¿Quién asume el riesgo? ¿Qué recursos se requieren?

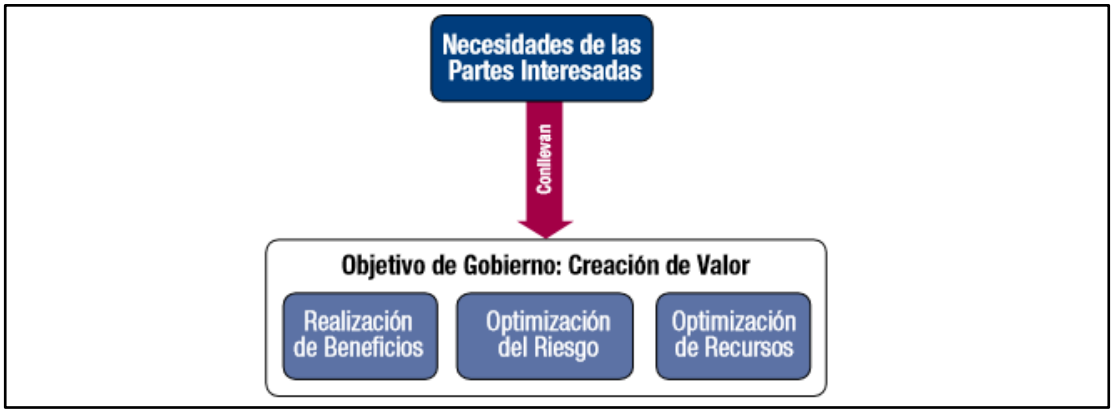


Ilustración 7 El Objetivo de Gobierno: Creación de Valor.
Fuente: COBIT 5 – Un marco de Negocio para el Gobierno y la gestión de las TI de la empresa

Cascadas de metas de COBIT5

Cada empresa opera en un contexto diferente; este contexto está determinado por factores externos (el mercado, la industria, geopolítica, etc.) y factores internos (la cultura, organización, umbral de riesgo, etc.) y requiere un sistema de gobierno y gestión personalizado.
Las necesidades de las partes interesadas deben transformarse en una estrategia corporativa factible. La cascada de metas de COBIT 5 es el mecanismo para traducir las necesidades de las partes interesadas en metas corporativas, metas relacionadas con las TI y metas catalizadoras específicas, útiles y a medida. Esta traducción permite establecer metas específicas en todos los niveles y en todas las áreas de la empresa en apoyo de los objetivos generales y requisitos de las partes interesadas y así, efectivamente, soportar la alineación entre las necesidades de la empresa y las soluciones y servicios de TI.

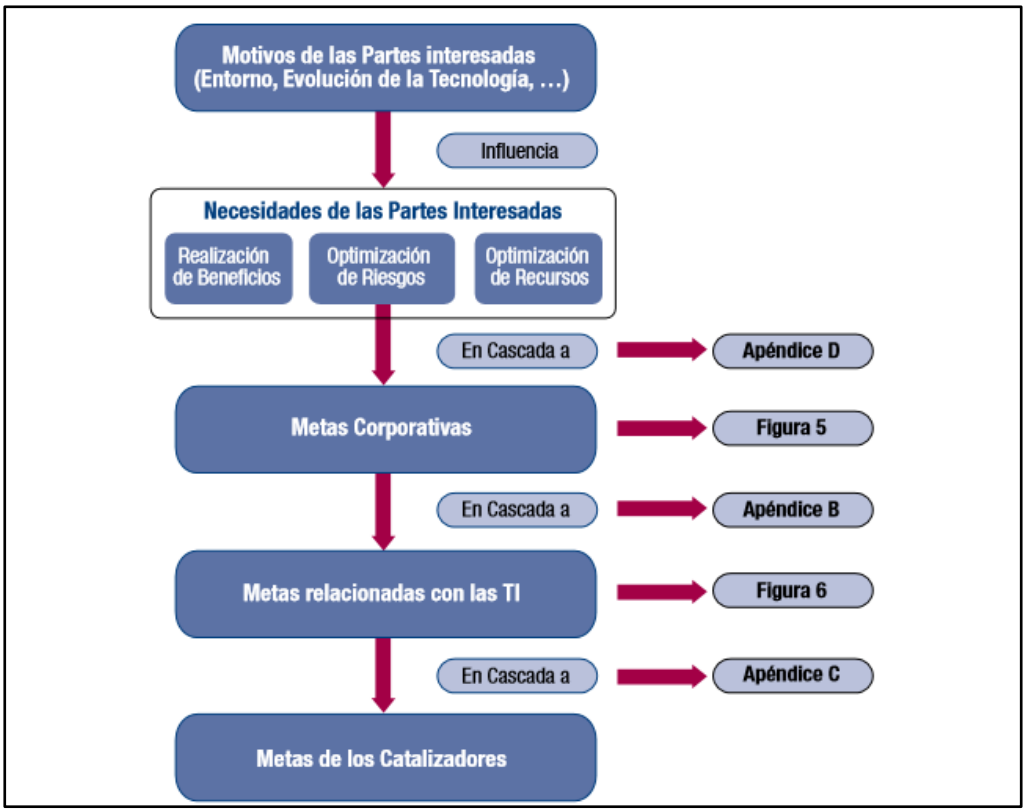


Ilustración 8 Visión General de la Cascada de Metas de COBIT 5
Fuente: COBIT 5 – Un marco de Negocio para el Gobierno y la gestión de las TI de la empresa

Principio 2: Cubrir la empresa de extremo a extremo:
COBIT 5 contempla el gobierno y la gestión de la información y la tecnología relacionada desde una perspectiva extremo-a-extremo y para toda la empresa. Esto significa que COBIT 5:

- Integra el gobierno de la empresa TI en el gobierno corporativo. Es decir, el sistema de gobierno para la empresa TI propuesto por COBIT 5 se integra sin problemas en cualquier sistema de gobierno. COBIT 5 se alinea con las últimas visiones sobre gobierno.
- Cubre todas las funciones y procesos necesarios para gobernar y gestionar la información corporativa y las tecnologías relacionadas donde quiera que esa información pueda ser procesada. Dado este alcance corporativo amplio, COBIT 5 contempla todos los servicios TI internos y externos relevantes, así como los procesos de negocio internos y externos.

COBIT 5 proporciona una visión integral y sistémica del gobierno y la gestión de la empresa TI (ver el principio 4), basada en varios catalizadores. Los catalizadores son para toda la empresa y extremo-a-extremo, es decir, incluyendo todo y a todos, internos y externos, que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionada, incluyendo las actividades y responsabilidades tanto de las funciones TI como de las funciones de negocio.

La información es una de las categorías de catalizadores de COBIT. El modelo mediante el que COBIT 5 define los catalizadores permite a cada grupo de interés definir requisitos exhaustivos y completos para la información y el ciclo de vida de procesamiento de la información, conectando de este modo el negocio y su necesidad de una información adecuada y la función TI, y soportando el negocio y el enfoque de contexto

COBIT 5 observa la empresa en lo tecnológico desde una perspectiva extremo a extremo, lo que quiere decir:

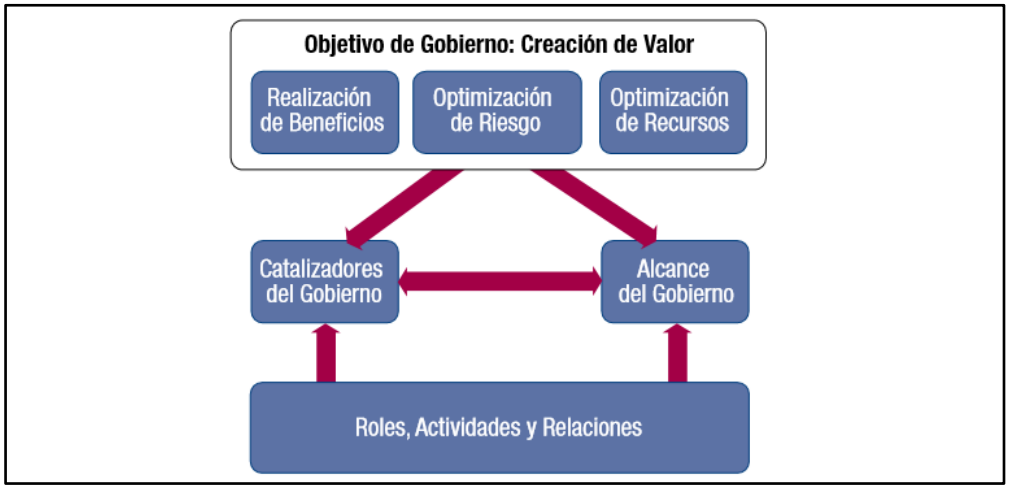


Ilustración 9 Gobierno y Gestión de COBIT 5.
Fuente: COBIT 5 – Un marco de Negocio para el Gobierno y la gestión de las TI de la empresa

Principio 3: Aplicar un marco de referencia único integrado:
COBIT 5 es un marco de referencia único e integrado porque:

- Se alinea con otros estándares y marcos de referencia relevantes y, por tanto, permite a la empresa usar COBIT 5 como el marco integrador general de gestión y gobierno.
- Es completo en cuanto a la cobertura de la empresa, proporcionando una base para integrar de manera efectiva otros marcos, estándares y prácticas utilizadas. Un marco general único sirve como una fuente consistente e integrada de guía en un lenguaje común, no-técnico y tecnológicamente agnóstico.
- Proporciona una arquitectura simple para estructurar los materiales de guía y producir un conjunto consistente.
- Integra todo el conocimiento disperso previamente en los diferentes marcos de ISACA. ISACA ha investigado las áreas clave del gobierno corporativo durante muchos años y ha desarrollado marcos tales como COBIT, Val IT, Risk IT, BMIS, la publicación Información sobre Gobierno de TI para la Dirección (Board Briefing on IT Governance) e ITAF para proporcionar guía y asistencia a las empresas. COBIT 5 integra todo este conocimiento.

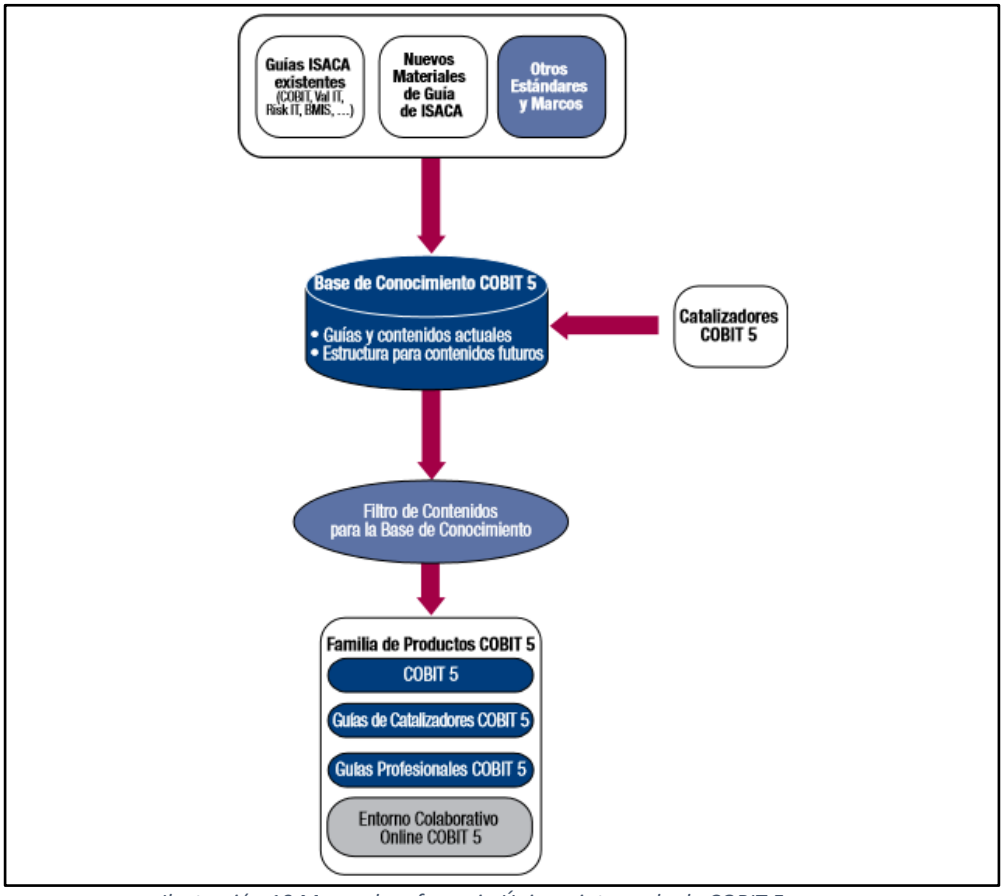


Ilustración 10 Marco de referencia Único e integrado de COBIT 5.
Fuente: COBIT 5 – Un marco de Negocio para el Gobierno y la gestión de las TI de la empresa

Principio 4: Hacer posible un enfoque holístico:
Los catalizadores son factores que, individual y colectivamente, influyen sobre si algo funcionará – en este caso, el gobierno y la gestión de la empresa TI. Los catalizadores son guiados por la cascada de metas, es decir, objetivos de alto nivel relacionados con TI definen lo que los diferentes catalizadores deberían conseguir.

El marco de referencia COBIT 5 describe siete categorías de catalizadores:

- Principios, políticas y marcos de referencia son el vehículo para traducir el comportamiento deseado en guías prácticas para la gestión del día a día.
- Los procesos describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de resultados que soporten las metas generales relacionadas con TI.
- Las estructuras organizativas son las entidades de toma de decisiones clave en una organización.
- La Cultura, ética y comportamiento de los individuos y de la empresa son muy a menudo subestimados como factor de éxito en las actividades de gobierno y gestión.
- La información impregna toda la organización e incluye toda la información producida y utilizada por la empresa. La información es necesaria para mantener la organización funcionando y bien gobernada, pero a nivel operativo, la información es muy a menudo el producto clave de la empresa en sí misma.
- Los servicios, infraestructuras y aplicaciones incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.
- Las personas, habilidades y competencias están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y de acciones correctivas.

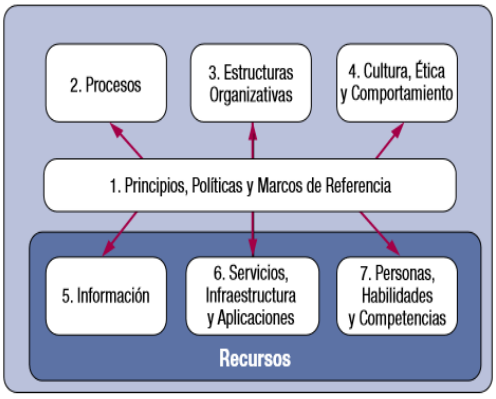


Ilustración 11 Catalizadores corporativos de COBIT 5.
Fuente: COBIT 5 – Un marco de Negocio para el Gobierno y la gestión de las TI de la empresa

Algunos de los catalizadores definidos previamente son también recursos corporativos que también necesitan ser gestionados y gobernados. Esto aplica a:

- La información, que necesita ser gestionada como un recurso. Alguna información, tal como informes de gestión y de inteligencia de negocio son importantes catalizadores para el gobierno y la gestión de la empresa.

- Servicios, infraestructura y aplicaciones.
- Personas, habilidades y competencias

Principio 5: Separar el gobierno de la gestión:

El marco de COBIT 5 realiza una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren estructuras organizativas diferentes y sirven para diferentes propósitos. La posición de COBIT 5 sobre esta fundamental distinción entre gobierno y gestión es:

Gobierno:

- Evaluación, orientación y supervisión (EDM).

Gestión:

- Alinear, Planificar y Organizar (APO).
- Construir, Adquirir e Implementar (BAI).
- Entregar, dar Servicio y Soporte (DSS).
- Supervisar, Evaluar y Valorar (MEA).

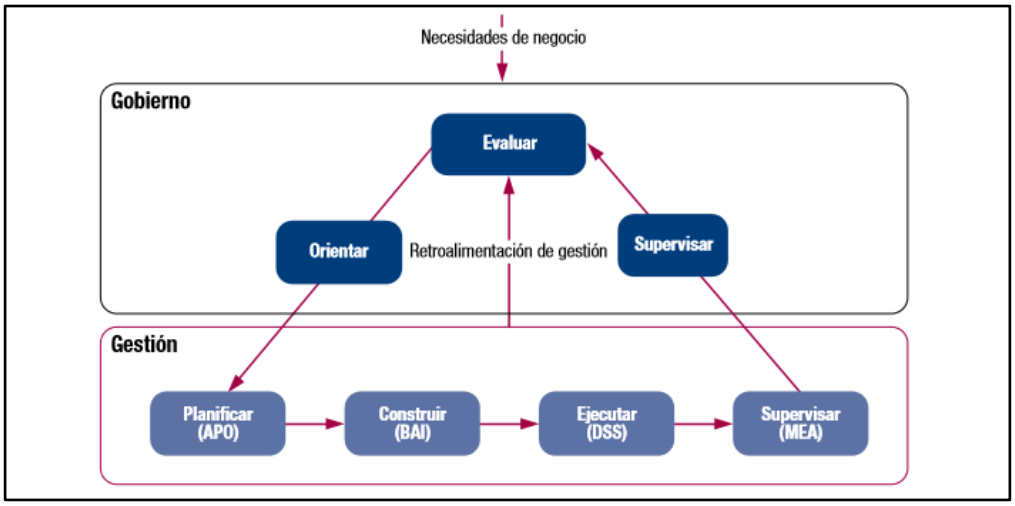


Ilustración 12 Las áreas claves de gobierno y gestión de COBIT 5.
Fuente: COBIT 5 – Un marco de Negocio para el Gobierno y la gestión de las TI de la empresa.

2.2.9 COBIT 5 y la seguridad

Los marcos de referencias se usan para que las empresas las tomen de guía y hagan que sea un aglomerado de planes determinados y gobernados gracias al jefe de TI.

El marco de trabajo COBIT 5 se centra en lo que es Seguridad de la Información, y además recomienda el uso de buenas prácticas que esta misma tiene, se engarce de proteger la información a toda costa.

COBIT 5 te brinda una dirección básica para monitorear un sistema de gestión de seguridad y toma las gestiones anteriormente definidas que son:

- Gestionar el riesgo, APO12.
- Gestionar la seguridad, APO13.
- Gestión de la continuidad, DSS04.
- Gestión de servicios de seguridad, DSS05.

COBIT 5 establece procesos y te permite hacer la cascada de metas para entrelazar metas de TI y de la empresa.

Consideraciones y pautas principales para la seguridad de la información

No se puede negar que la aplicación de medidas para proteger la información es, hoy en día, una necesidad, ya que es un activo útil. Se establece un mayor alcance relacionado con la continuidad de las operaciones y la protección del negocio, siendo la razón de ser de las organizaciones.

Los diferentes procesos, actividades o iniciativas se pueden completar con las diferentes propuestas realizadas en este documento, es el resultado del consenso de todos los expertos en el tema, además de que está en continuo desarrollo para mejorar las prácticas.

En la siguiente figura de COBIT 5 es donde se mapean todos los procesos que se presentan en las cláusulas y en los controles de los estándares, se agrega información que completa a las mejores prácticas, de forma principal todas las metas y las métricas para realizar prácticas y gestionarlas. Las actividades específicas de seguridad y protección deben ser adoptadas y adaptadas a todas las características y necesidades que presenta la organización, además de proteger la información y conseguir su misión. (Mendoza, 2015)

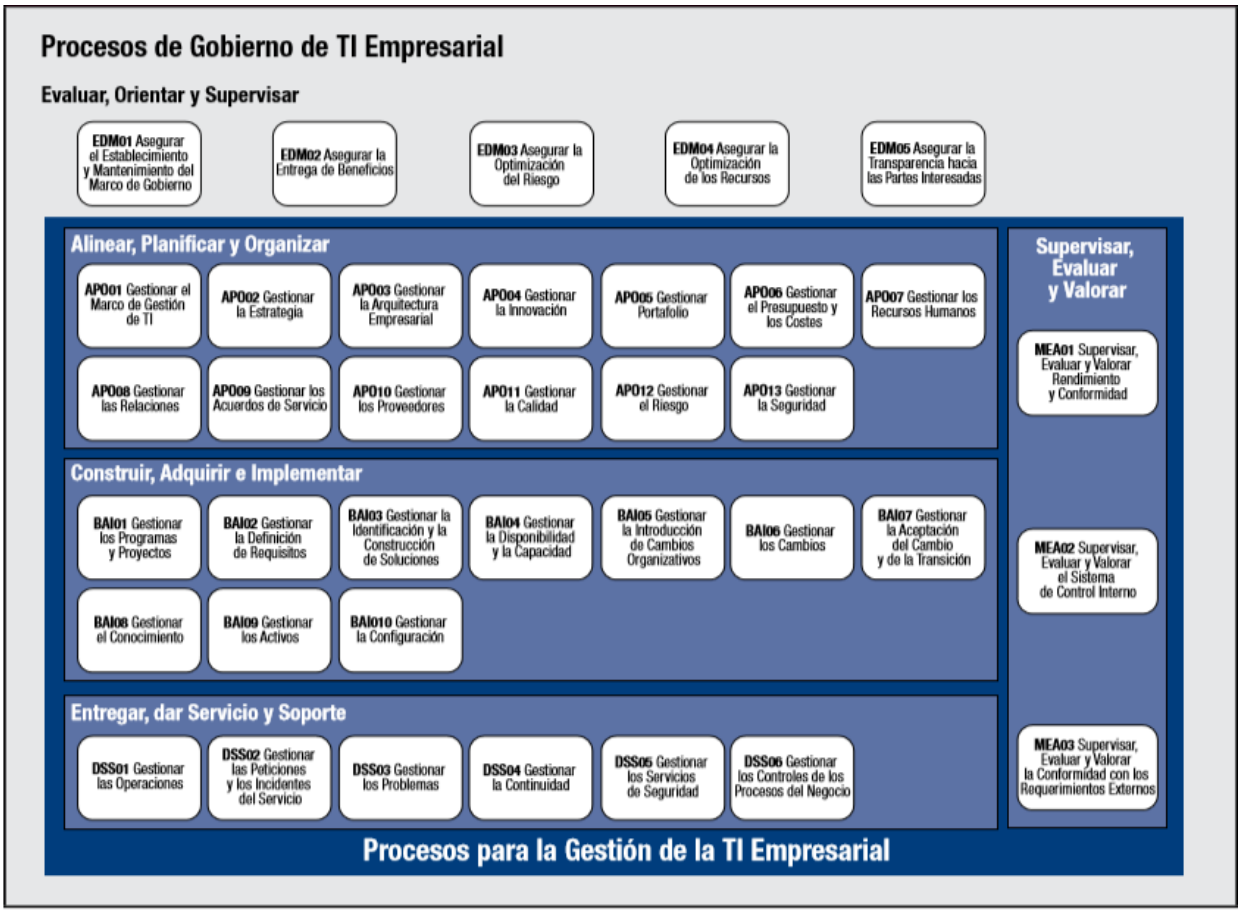


Ilustración 13 Modelo de referencia de Procesos COBIT 5.
Fuente: COBIT 5 – Un marco de Negocio para el Gobierno y la gestión de las TI de la empresa.

2.2.10 MAGERIT

MAGERIT fue creada para ser una metodología de análisis y gestión de riesgos en respuesta a la seguridad de la información que estaba siendo atacada, el Consejo Superior de Administración Electrónica fue el responsable de su creación.

MAGERIT te permite saber cuáles son los riesgos tecnológicos al cual están sometidos, además de identificarlos medir su nivel de concurrencia, con la aparición de MAGERIT se trata de hacer que todo tenga un método y no esté al desafuero ni a la improvisación de cómo resolver los problemas informáticos (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Objetivos

1. Informar a los encargados de la realidad de los riesgos y la obligación de cómo gestionarlos
2. Dar una metodología para observar las amenazas de las TIC.
3. Colaborar en la gestión oportuna para mantener los riesgos indirectos y directos bajo control.
4. Planificar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

2.2.11 Matriz de riesgos

Es una herramienta para establecer y conocer los riesgos más importantes que tiene una organización para de esta manera poder controlarlos en cuanto a la seguridad de la organización.

Nos permite hacer un diagnóstico objetivo y global a todo tipo de empresa u organización, además esta nos permite tener en control la efectividad de la administración de los riesgos, en todo ámbito como financiero, operativo y estratégico, y poder ver cuál es el impacto en determinado punto de la organización.

Características de la matriz de riesgo

Toda matriz de riesgo debe tener y garantizar su eficacia y utilidad además de contar con estas peculiaridades:

- Adaptarse a todo.
- Fácil manejo y elaboración.
- El uso de consultas tiene que ser objetivos con relación a las características de cada riesgo.
- Poder relacionarlas con otros propósitos, oficinas y actividades.

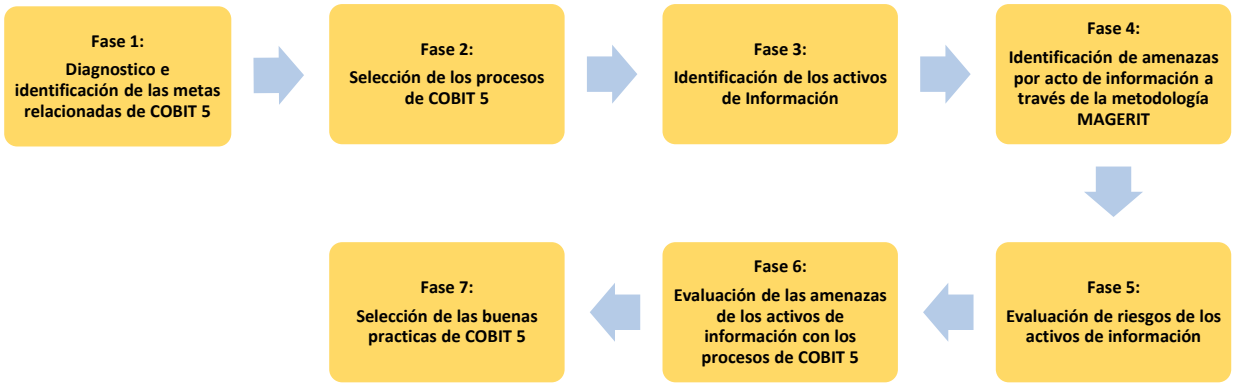
Pasos para la elaboración de una matriz de riesgo

1) Identificación de riesgos
2) Evaluar la probabilidad de que se acabe confirmando el riesgo
3) Representación de la matriz de riesgos

(ISOTools, 2015)

CAPÍTULO 3 –Desarrollo de la propuesta del modelo de gestión de seguridad de la información.

Para el desarrollo de la propuesta del modelo de gestión de seguridad de la información propuesto se creó el siguiente modelo:



3.1 Diagnostico e identificación de las metas relacionadas de COBIT 5

Primero empezaremos haciendo un mapeo detallado sobre las metas relacionadas con TI y las metas corporativas de COBIT 5, este procedimiento lo recomienda hacer dicho marco de trabajo.

En las columnas, las 17 metas corporativas definidas en el en libro de COBIT 5, en las filas, las 17 metas relacionadas con TI.

Se usa la siguiente interpretación:

–"P" significa una relación primaria (importante).

–"S" significa usa relación secundaria (fuerte).

Teniendo en cuenta nuestro objetivo general que es "Proponer un modelo de gestión para la seguridad de la información de la Cooperativa Santo Domingo de Guzmán agencia Sicuani usando el marco de referencia de COBIT 5", y haciendo uso de la tabla 1, usaremos las siguientes metas que se encuentra en la sección de Metas Corporativa–Financiera:

- 3 - Riesgo de negocio gestionados (Salvaguardar los activos).
- 4 – Cumplimiento de Leyes y regulaciones externas.

Tabla 1 Objetivos corporativos de COBIT 5 con los objetivos de TI

			Meta Corporativa																
			Valor para las partes interesadas de las Inversiones de Negocio	Cartero de productos y servicios competitivos	**Riesgos de negocio gestionados (Salvaguarda de activos)**	**Cumplimiento de Leyes y regulaciones externas**	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas agiles a un entorno de negocio cambiante	Toma estratégica de decisiones basada en información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personas preparadas y motivadas	Cultura de innovación de producto y negocio
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Meta relacionada con TI			Financiera					Cliente					Interna					Aprendizaje y crecimiento	
Financiera	1	Alineamiento de TI y la estrategia de negocio	P	P	S			P	S	P	P	S	P	S	P			S	S
	2	**Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas**			S	P											P		
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	4	**Riesgos de negocio relacionados con las TI gestionados**			P	S			P	S		P			S		S	S	
	5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	P	P				S		S		S	S	P		S			S

	6	Transparencia de los costes, beneficios y riesgos de las TI	S		S		P				S	P		P					
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Matriz	9	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10	**Seguridad de la información, infraestructura de procesamiento y aplicaciones**			P	P			P								P		
	11	Optimización de activos, recursos y capacidades de las TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	P	S	S			S				S		S	P				
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de las políticas internas por parte de las TI			S	S											P		
Aprendizaje y Crecimiento	**16**	**Personal del negocio y de las TI competente y motivado**	S	S	P			S		S						P		P	S
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P				S		P	S		S		S			S	P

Fuente: COBIT 5 – Un marco de Negocio para el Gobierno y la gestión de las TI de la empresa

Análisis

Las metas corporativas de COBIT 5, meta 3 y 4, se intersectan mediante una importante relación (P) con:

- 2 - Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
- 4 - Riesgos de negocio relacionados con las TI gestionados.
- 10 - Seguridad de la información, infraestructura de procesamiento y aplicaciones.
- 16 - Personal del negocio y de las TI competente y motivado.

Una vez seleccionadas nuestras metas relacionadas con TI en este caso las metas 2, 4,10 y 16, procedemos a la siguiente tabla para poder hacer un mapeo de cada meta relacionada con TI y los procesos de COBIT 5.

3.2 Selección de los procesos de COBIT 5

Haremos un mapeo detallado sobre las metas relacionadas con TI y los procesos de COBIT 5. En las columnas, las 17 metas genéricas relacionadas con TI definidas en el en libro de COBIT 5, en las filas, los 37 procesos de COBIT 5, agrupados por dominio, un mapeo de cómo cada meta relacionada con TI se sustenta por un proceso relacionado con TI de COBIT 5.

Este mapeo se expresa usando la siguiente escala:

–"P" significa primario, cuando hay una importante relación, es decir, el proceso de COBIT 5 es un soporte primario para conseguir la meta relacionada con TI.

–"S" significa secundario, cuando todavía hay una relación fuerte, pero menos importante, es decir, el proceso de COBIT 5 es un soporte secundario para conseguir la meta relacionada con TI.

Tabla 2 Objetivos relacionados con TI y procesos de Evaluar, Orientar y Supervisar (EDM)

			OBJETIVO RELACIONADO CON TI																
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
PROCESOS DE COBIT 5			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
			Financiera						Cliente		Interna							Aprendizaje y crecimiento	
Evaluar, Orientar y Supervisar (EDM)	**EDM01**	**Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno**	**P**	S	**P**	S	S	S	**P**		S	S	S	S	S	S	S	S	S
	EDM02	**Asegurar la entrega de beneficios**	**P**		S		**P**	**P**	**P**	S			S	S	S	S		S	**P**

	EDM03	Asegurar la optimización del riesgo	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Asegurar la optimización de recursos	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Asegurar la transparencia hacia las partes interesadas	S	S	P			P	P						S	S	S		S

Fuente: COBIT 5 – Un marco de Negocio para el Gobierno y la gestión de las TI de la empresa

Análisis

Teniendo en cuenta nuestras metas relacionadas con TI las cuales son:

- 2 - Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
- 4 - Riesgos de negocio relacionados con las TI gestionados.
- 10 - Seguridad de la información, infraestructura de procesamiento y aplicaciones.
- 16 - Personal del negocio y de las TI competente y motivado.

Veremos con cuál de los procesos se tiene una relación primaria (P).

Como relación primaria entre nuestras metas relacionadas con TI y el proceso de COBIT 5 – Evaluar, orientar y supervisar son:

- EDM 03 - Asegurar la optimización del riesgo.
- EDM 04 - Asegurar la optimización de recursos.

Los procesos EDM 03 Y EDM 04 no serán tomados en cuenta porque como en el capítulo anterior (Marco teórico) se vio que para hacer nuestra propuesta de un modelo de gestión de seguridad de la información para la CACSDG agencia Sicuani basado en el marco de referencia de COBIT 5 solo se necesita 4 procesos anteriormente nombrados, el marco de referencia COBIT 5 te permite escoger de los procesos y los objetivos relacionados de TI entre “Principales” y “Secundarios” solo los que serán de uso para la investigación.

Tabla 3 Objetivos relacionados con TI y procesos de Alinear, planear y organizar (APO)

			OBJETIVO RELACIONADO CON TI																
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
PROCESOS DE COBIT 5			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
			Financiera						Cliente		Interna							Aprendizaje y crecimiento	
Alinear, Planear y Organizar (APO)	**APO01**	Gestionar el Marco de Gestión de TI	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	Gestionar la Estrategia	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Gestionar la Arquitectura Empresarial	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	Gestionar la Innovación	S			S	P			P	P		P	S		S			P
	APO05	Gestionar el Portafolio	P		S	S	P	S	S	S	S		S		P				S
	APO06	Gestionar el Presupuesto y los Costes	S		S	S	P	P	S	S			S		S				

	APO07	Gestionar los Recursos Humanos	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	Gestionar las relaciones	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	Gestionar los acuerdos de servicio	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	Gestionar los Proveedores		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	Gestionar la Calidad	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	Gestionar el Riesgo		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	Gestionar la Seguridad		P		P		P	S	S		P				P			

Fuente: COBIT 5 – Un marco de Negocio para el Gobierno y la gestión de las TI de la empresa

Análisis

Teniendo en cuenta nuestras metas relacionadas con TI las cuales son:

- 2 - Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
- 4 - Riesgos de negocio relacionados con las TI gestionados.
- 10 - Seguridad de la información, infraestructura de procesamiento y aplicaciones.
- 16 - Personal del negocio y de las TI competente y motivado.

Veremos con cuál de los procesos se tiene una relación primaria (P).

Como relación primaria entre nuestras metas relacionadas con TI y el proceso de COBIT 5 – Alinear, planear y organizar son:

- APO 01 - Gestionar el marco de gestión de TI.
- APO 07 - Gestionar los recursos humanos.
- APO 10 - Gestionar los proveedores.
- APO 12 - Gestionar el riesgo.
- APO 13 - Gestionar la seguridad.

Los procesos APO 01, APO 07 Y APO 10 no serán tomados en cuenta porque como en el capítulo anterior (Marco teórico) se vio que para hacer nuestra propuesta de un modelo de gestión de seguridad de la información para la CACSDG agencia Sicuani basado en el marco de referencia de COBIT 5 solo se necesita 4 procesos anteriormente nombrados, el marco de referencia COBIT 5 te permite escoger de los procesos y los objetivos relacionados de TI entre “Principales” y “Secundarios” solo los que serán de uso para la investigación.

Se usaran los procesos APO 12 Y APO 13 para la propuesta de un modelo de gestión de seguridad de la información para la cooperativa santo domingo de guzmán agencia Sicuani basado en el marco de referencia de COBIT 5, ya que estos 2 procesos están dentro de los 4 procesos anteriormente nombrados en el Capítulo 2.

Tabla 4 Objetivos relacionados con TI y procesos de Construir, adquirir e implementar (BAI)

PROCESOS DE COBIT 5			OBJETIVO RELACIONADO CON TI																
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
			Financiera						Cliente		Interna							Aprendizaje y crecimiento	
Construir, Adquirir e Implementar (BAI)	BAI01	Gestión de Programas y Proyectos	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Gestionar la Definición de Requisitos	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Gestionar la Identificación y Construcción de Soluciones	S			S	S		P	S			S	S	S	S			S
	BAI04	Gestionar la Disponibilidad y la Capacidad				S	S		P	S	S		P		S	P			S

	BAI05	Gestionar la Facilitación del Cambio Organizativo	S		S		S		S	P	S		S	S	P				P
	BAI06	Gestionar los Cambios			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Gestionar la Aceptación del Cambio y la Transición				S	S		S	P	S			P	S	S	S		S
	BAI08	Gestionar el Conocimiento	S				S		S	S	P	S	S			S		S	P
	BAI09	Gestionar los Activos		S		S		P	S		S	S	P			S	S		
	BAI10	Gestionar la Configuración		P		S		S		S	S	S	P			P	S		

Fuente: COBIT 5 – Un marco de Negocio para el Gobierno y la gestión de las TI de la empresa

Análisis

Teniendo en cuenta nuestras metas relacionadas con TI las cuales son:

- 2 - Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
- 4 - Riesgos de negocio relacionados con las TI gestionados.
- 10 - Seguridad de la información, infraestructura de procesamiento y aplicaciones.
- 16 - Personal del negocio y de las TI competente y motivado.

Veremos con cuál de los procesos se tiene una relación primaria (P).

Como relación primaria entre nuestras metas relacionadas con TI y el proceso de COBIT 5 – Construir, adquirir e implementar son:

- BAI 01 - Gestión de programas y proyectos.
- BAI 06 - Gestionar los cambios.
- BAI 10 - Gestionar la configuración.

Los procesos BAI 01, BAI 06 Y BAI 10 no serán tomados en cuenta porque como en el capítulo anterior (Marco teórico) se vio que para hacer nuestra propuesta de un modelo de gestión de seguridad de la información para la CACSDG agencia Sicuani basado en el marco de referencia de COBIT 5 solo se necesita 4 procesos anteriormente nombrados, el marco de referencia COBIT 5 te permite escoger de los procesos y los objetivos relacionados de TI entre “Principales” y “Secundarios” solo los que serán de uso para la investigación.

Tabla 5 Objetivos relacionados con TI y procesos de Entregar, dar servicio y soporte (DSS)

PROCESOS DE COBIT 5			OBJETIVO RELACIONADO CON TI																
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
			Financiera						Cliente		Interna							Aprendizaje y crecimiento	
Entregar, Dar Servicio y Soporte	DSS01	Gestionar Operaciones		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Gestionar Peticiones e Incidentes de Servicio				P			P	S		S				S	S		S

	DSS03	Gestionar Problemas		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Gestionar la Continuidad	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Gestionar Servicios de Seguridad	S	P		P			S	S		P	S	S		S	S		
	DSS06	Gestionar Controles de Proceso de Negocio		S		P			P	S		S	S	S		S	S	S	S

Fuente: COBIT 5 – Un marco de Negocio para el Gobierno y la gestión de las TI de la empresa

Análisis

Teniendo en cuenta nuestras metas relacionadas con TI las cuales son:

- 2 - Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
- 4 - Riesgos de negocio relacionados con las TI gestionados.
- 10 - Seguridad de la información, infraestructura de procesamiento y aplicaciones.
- 16 - Personal del negocio y de las TI competente y motivado.

Veremos con cuál de los procesos se tiene una relación primaria (P).

Como relación primaria entre nuestras metas relacionadas con TI y el proceso de COBIT 5 – Entregar, dar servicio y soporte son:

- DSS 01 - Gestionar operaciones.
- DSS 02 - Gestionar peticiones e incidentes de servicio.
- DSS 03 - Gestionar problemas.
- DSS 04 - Gestionar la continuidad.
- DSS 05 - Gestionar servicios de seguridad.
- DSS 06 - Gestionar controles de proceso de negocio.

Los procesos DSS 01, DSS 02, DSS 03 Y DSS 06 no serán tomados en cuenta porque como en el capítulo anterior (Marco teórico) se vio que para hacer nuestra propuesta de un modelo de gestión de seguridad de la información para la CACSDG agencia Sicuani basado en el marco de referencia de COBIT 5 solo se necesita 4 procesos anteriormente nombrados, el marco de referencia COBIT 5 te permite escoger de los procesos y los objetivos relacionados de TI entre “Principales” y “Secundarios” solo los que serán de uso para la investigación.

Se usaran los procesos DSS 04 Y DSS 05 para la propuesta de un modelo de gestión de seguridad de la información para la cooperativa santo domingo de guzmán agencia Sicuani basado en el marco de referencia de COBIT 5, ya que estos 2 procesos están dentro de los 4 procesos anteriormente nombrados en el Capítulo 2.

Tabla 6 Objetivos relacionados con TI y procesos de Supervisar, evaluar y valorar (MEA)

PROCESOS DE COBIT 5			OBJETIVO RELACIONADO CON TI																
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
			Financiera						Cliente		Interna							Aprendizaje y crecimiento	
Supervisar, Evaluar y Valorar (MEA)	MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno		P		P		S	S	S		S				S	P		S

	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos		P		P	S		S			S					S	S

Fuente: COBIT 5 – Un marco de Negocio para el Gobierno y la gestión de las TI de la empresa

Análisis

Teniendo en cuenta nuestras metas relacionadas con TI las cuales son:

- 2 - Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
- 4 - Riesgos de negocio relacionados con las TI gestionados.
- 10 - Seguridad de la información, infraestructura de procesamiento y aplicaciones.
- 16 - Personal del negocio y de las TI competente y motivado.

Veremos con cuál de los procesos se tiene una relación primaria (P).

Como relación primaria entre nuestras metas relacionadas con TI y el proceso de COBIT 5 – Entregar, dar servicio y soporte son:

- MEA 01 - Supervisar, evaluar y valorar el rendimiento y la conformidad.
- MEA 02 - Supervisar, evaluar y valorar el sistema de control interno.
- MEA 03 - Supervisar, evaluar y valorar la conformidad con los requerimientos externos.

Los procesos MEA 01, MEA 02 Y MEA 03 no serán tomados en cuenta porque como en el capítulo anterior (Marco teórico) se vio que para hacer nuestra propuesta de un modelo de gestión de seguridad de la información para la CACSDG agencia Sicuani basado en el marco de referencia de COBIT 5 solo se necesita 4 procesos anteriormente nombrados, el marco de referencia COBIT 5 te permite escoger de los procesos y los objetivos relacionados de TI entre “Principales” y “Secundarios” solo los que serán de uso para la investigación.

Seguidamente se hace un resumen de todos los procesos seleccionados y se sombrea solo aquellos que se usaran en la “Propuesta de un modelo de gestión de seguridad de la información para la Cooperativa Santo Domingo de Guzmán agencia Sicuani basado en el marco de referencia COBIT 5” estos procesos son seleccionados debidamente utilizando el Capítulo 2 – “Marco Teórico”.

Tabla 7 Resumen procesos COBIT 5 y Objetivos relacionados con TI

	OBJETIVOS RELACIONADO CON TI			
	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.	Riesgos de negocio relacionados con las TI gestionados.	Seguridad de la información, infraestructura de procesamiento y aplicaciones.	Personal del negocio y de las TI competente y motivado.
PROCESOS COBIT 5	2	4	10	16
Evaluar, Orientar y Supervisar (EDM)	-	EDM 03- Asegurar la optimización del riesgo	EDM 03- Asegurar la optimización del riesgo	EDM 04-Asegurar la optimización de recursos
Alinear, Planear y Organizar (APO)	APO 01- Gestionar el marco de gestión de TI. **APO 12- Gestionar el riesgo.** **APO 13- Gestionar la seguridad.**	APO 10- Gestionar proveedores. **APO 12- Gestionar el riesgo.** **APO 13- Gestionar la seguridad.**	**APO 12- Gestionar el riesgo.** **APO 13- Gestionar la seguridad.**	APO 01- Gestionar el margo de gestión de TI. APO 07- Gestionar los recursos humanos.
Construir, Adquirir e Implementar (BAI)	BAI 10- Gestionar la configuración.	BAI 01- Gestión de programas y proyectos. BAI 06- Gestionar los cambios.	BAI 06- Gestionar los cambios.	-
Entregar, Dar Servicio y Soporte (DSS)	**DSS 05- Gestionar servicios de seguridad.**	DSS 01- Gestionar operaciones. DSS 02- Gestionar peticiones e incidentes de servicio. DSS 03- Gestionar problemas. **DSS 04- Gestionar la continuidad.** **DSS 05- Gestionar servicios de seguridad.** DSS 06- Gestionar controles de proceso de negocio.	**DSS 05- Gestionar servicios de seguridad.**	-
Supervisar, Evaluar y Valorar (MEA)	MEA 02- Supervisar, evaluar y valorar el sistema de control interno. MEA 03- Supervisar, evaluar y valorar la conformidad con los requerimientos.	MEA 01- Supervisar, evaluar y valorar el rendimiento y la conformidad. MEA 02- Supervisar, evaluar y valorar el sistema de control interno. MEA 03- Supervisar, evaluar y valorar la conformidad con los requerimientos.	-	-

3.3 Identificación de los Activos de información.

Una vez hecha nuestras matrices de COBIT 5 y al relacionarlas con nuestros objetivos relacionados de TI, analizamos cuales son los adecuados para la propuesta de un modelo de gestión de seguridad de la información para la CACSDG agencia Sicuani basado en el marco de referencia de COBIT 5, además de tener en cuenta los estudios realizados en el Marco Teórico y llegando a una conclusión de que estos procesos son:

- APO 12 - Gestionar el riesgo.
- APO 13 - Gestionar la seguridad.
- DSS 04 - Gestionar la continuidad.
- DSS 05 - Gestionar servicios de seguridad.

Ahora procedemos a identificar los Activos de Información que la Cooperativa Santo Domingo de Guzmán tiene gracias a las entrevistas realizadas (ver anexo 5) a los trabajadores de la oficina de Tecnología de Información de dicha identidad financiera los cuales son:

Tabla 8 Descripción de los activos de información

Activos de Información	Descripción
A) Equipos informáticos	Sistema de asistencia biométrico.
B) Servidores	Servidores locales propios y servidores exteriores.
C) Equipos de red local	Los equipos dentro de las redes.
D) Periféricos y pendrives	Los USBs, MicroSDs, CDs, DVDs entre otros.
E) Portátiles, tabletas y móviles	Son los equipos de la misma empresa que por trabajo a veces tienen que salir de la empresa.
F) Oficinas	Aparadores, cajas de seguridad, ficheros, repisas, habitaciones adaptadas para servidores, oficinas de archivos, que contienen los ordenadores, servidores físicos, documentación.
G) Personal propio	Personas que trabajan para la Cooperativa.
H) Aplicaciones informáticas	Sistema financiero, simuladores de crédito, programas ofimáticos (Word, Excel, Powerpoint, etc), gestor de copias de seguridad y creador de imágenes de PC.
I) Gestores de base de datos	Requiere de un cuidado más exigente y delicado.
J) Sistemas externos	Sistemas de uso externo que la cooperativa usa, BESTER, RENIEC, EXPERIAN EQUIFAX Y SUNARP

Después se procedió a usar MAGERIT v3, que es una metodología de análisis y gestión de riesgos, se procedió a entrevistar a algunos trabajadores, donde ellos marcaron con una X en caso de que dicha amenaza ocurra y su probabilidad de ocurrencia es de 1 a 5, donde 1 es menos probables y 5 es muy probable de esta manera se pudo identificar las amenazas existentes para cada activo de información.

3.4 Identificación de amenazas por activo de información a través de la metodología MAGERIT

A) EQUIPOS INFORMÁTICOS

Tabla 9 Identificación de amenazas del activo de información-Equipos Informáticos

Amenaza	Marca (X)	Probabilidad de ocurrencia
Fuego	X	1
Tormenta eléctrica, rayo	X	3
Error de Usuario	X	2
Errores del administrador	X	2
Errores de configuración	X	2
Alteración accidental de la información	X	1
Destrucción de Información	X	1
Fugas de Información		
Vulnerabilidades de los programas (software)	X	1
Errores de mantenimiento / actualización de programas (software)		
Errores de mantenimiento / actualización de equipos (hardware)	X	2
Caída del sistema por agotamiento de recursos (interrupción en los servicios)		
Indisponibilidad del personal	X	2
Manipulación de los registros de Actividad (log)		
Manipulación de la configuración	X	3
Suplantación de la identidad del usuario		
Abuso de privilegios de acceso	X	2
Difusión de software dañino		
Acceso no autorizado	X	4
Modificación deliberada de la información	X	3
Destrucción deliberada de Información		
Divulgación de la Información	X	4
Manipulación de programas		
Manipulación de los equipos	X	2
Denegación del servicio		
Robo de Equipos	X	3
Indisponibilidad deliberada del personal	X	4
Extorsión		
Ejecución de ingeniería social		
Corte del suministro eléctrico	X	2
Condiciones inadecuadas de temperatura o humedad		
Degradación de los soportes de almacenamiento de la información	X	2
Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones	X	3
Hacking no ético	X	3
Instalación de software no autorizado		
Otro:		

Fuente: MAGERIT v3, elaboración propia

B) SERVIDORES

Tabla 10 Identificación de amenazas del activo de información-Servidores

Amenaza	Marca (X)	Probabilidad de ocurrencia
Fuego	X	1
Tormenta eléctrica, rayo	X	3
Error de Usuario		
Errores del administrador	X	3
Errores de configuración	X	3
Alteración accidental de la información	X	2
Destrucción de Información	X	2
Fugas de Información	X	2
Vulnerabilidades de los programas (software)	X	1
Errores de mantenimiento / actualización de programas (software)	X	1
Errores de mantenimiento / actualización de equipos (hardware)	X	1
Caída del sistema por agotamiento de recursos (interrupción en los servicios)	X	1
Indisponibilidad del personal		
Manipulación de los registros de Actividad (log)		
Manipulación de la configuración	X	2
Suplantación de la identidad del usuario	X	4
Abuso de privilegios de acceso	X	4
Difusión de software dañino	X	2
Acceso no autorizado	X	3
Modificación deliberada de la información	X	2
Destrucción deliberada de Información	X	1
Divulgación de la Información	X	2
Manipulación de programas	X	2
Manipulación de los equipos	X	2
Denegación del servicio	X	3
Robo de Equipos	X	1
Indisponibilidad deliberada del personal		
Extorsión		
Ejecución de ingeniería social		
Corte del suministro eléctrico	X	2
Condiciones inadecuadas de temperatura o humedad		
Degradación de los soportes de almacenamiento de la información	X	2
Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones		
Hacking no ético	X	3
Instalación de software no autorizado		
Otro:		

Fuente: MAGERIT v3, elaboración propia

C) EQUIPOS DE RED LOCAL

Tabla 11 Identificación de amenazas del activo de información-Equipos de red local

Amenaza	Marca (X)	Probabilidad de ocurrencia
Fuego	X	1
Tormenta eléctrica, rayo	X	3
Error de Usuario	X	3
Errores del administrador	X	2
Errores de configuración	X	2
Alteración accidental de la información	X	3
Destrucción de Información	X	3
Fugas de Información	X	4
Vulnerabilidades de los programas (software)	X	4
Errores de mantenimiento / actualización de programas (software)	X	4
Errores de mantenimiento / actualización de equipos (hardware)	X	4
Caída del sistema por agotamiento de recursos (interrupción en los servicios)	X	2
Indisponibilidad del personal	X	2
Manipulación de los registros de Actividad (log)		
Manipulación de la configuración	X	3
Suplantación de la identidad del usuario	X	1
Abuso de privilegios de acceso	X	2
Difusión de software dañino	X	2
Acceso no autorizado	X	3
Modificación deliberada de la información	X	3
Destrucción deliberada de Información	X	3
Divulgación de la Información	X	3
Manipulación de programas	X	3
Manipulación de los equipos	X	3
Denegación del servicio	X	2
Robo de Equipos	X	1
Indisponibilidad deliberada del personal	X	3
Extorsión		
Ejecución de ingeniería social		
Corte del suministro eléctrico	X	2
Condiciones inadecuadas de temperatura o humedad		
Degradación de los soportes de almacenamiento de la información	X	2
Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones	X	4
Hacking no ético	X	2
Instalación de software no autorizado	X	4
Otro:		

Fuente: MAGERIT v3, elaboración propia

D) PERIFÉRICOS Y PENDRIVES

Tabla 12 Identificación de amenazas del activo de información-Periféricos y pendrives

Amenaza	Marca (X)	Probabilidad de ocurrencia
Fuego		
Tormenta eléctrica, rayo		
Error de Usuario	X	2
Errores del administrador	X	2
Errores de configuración	X	3
Alteración accidental de la información	X	4
Destrucción de Información	X	4
Fugas de Información	X	4
Vulnerabilidades de los programas (software)		
Errores de mantenimiento / actualización de programas (software)		
Errores de mantenimiento / actualización de equipos (hardware)		
Caída del sistema por agotamiento de recursos (interrupción en los servicios)		
Indisponibilidad del personal	X	2
Manipulación de los registros de Actividad (log)		
Manipulación de la configuración	X	2
Suplantación de la identidad del usuario	X	2
Abuso de privilegios de acceso	X	4
Difusión de software dañino	X	4
Acceso no autorizado	X	4
Modificación deliberada de la información	X	4
Destrucción deliberada de Información	X	4
Divulgación de la Información	X	4
Manipulación de programas		
Manipulación de los equipos		
Denegación del servicio		
Robo de Equipos	X	5
Indisponibilidad deliberada del personal	X	3
Extorsión		
Ejecución de ingeniería social		
Corte del suministro eléctrico		
Condiciones inadecuadas de temperatura o humedad		
Degradación de los soportes de almacenamiento de la información		
Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones		
Hacking no ético	X	3
Instalación de software no autorizado		
Otro:		

Fuente: MAGERIT v3, elaboración propia

E) PORTÁTILES, TABLETAS Y MÓVILES

Tabla 13 Identificación de amenazas del activo de información-Portátiles, tabletas y móviles

Amenaza	Marca (X)	Probabilidad de ocurrencia
Fuego	X	1
Tormenta eléctrica, rayo	X	4
Error de Usuario	X	2
Errores del administrador	X	2
Errores de configuración	X	2
Alteración accidental de la información	X	3
Destrucción de Información	X	3
Fugas de Información	X	5
Vulnerabilidades de los programas (software)	X	5
Errores de mantenimiento / actualización de programas (software)	X	5
Errores de mantenimiento / actualización de equipos (hardware)	X	5
Caída del sistema por agotamiento de recursos (interrupción en los servicios)		
Indisponibilidad del personal		
Manipulación de los registros de Actividad (log)		
Manipulación de la configuración	X	4
Suplantación de la identidad del usuario	X	4
Abuso de privilegios de acceso	X	3
Difusión de software dañino	X	4
Acceso no autorizado		
Modificación deliberada de la información	X	3
Destrucción deliberada de Información	X	3
Divulgación de la Información	X	4
Manipulación de programas	X	3
Manipulación de los equipos	X	3
Denegación del servicio		
Robo de Equipos	X	5
Indisponibilidad deliberada del personal	X	4
Extorsión		
Ejecución de ingeniería social		
Corte del suministro eléctrico		
Condiciones inadecuadas de temperatura o humedad		
Degradación de los soportes de almacenamiento de la información	X	3
Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones	X	4
Hacking no ético	X	4
Instalación de software no autorizado	X	3
Otro:		

Fuente: MAGERIT v3, elaboración propia

F) OFICINAS

Tabla 14 Identificación de amenazas del activo de información-Oficinas

Amenaza	Marca (X)	Probabilidad de ocurrencia
Fuego	X	1
Tormenta eléctrica, rayo		
Error de Usuario	X	2
Errores del administrador	X	2
Errores de configuración	X	2
Alteración accidental de la información	X	2
Destrucción de Información	X	3
Fugas de Información	X	2
Vulnerabilidades de los programas (software)		
Errores de mantenimiento / actualización de programas (software)		
Errores de mantenimiento / actualización de equipos (hardware)	X	2
Caída del sistema por agotamiento de recursos (interrupción en los servicios)	X	2
Indisponibilidad del personal	X	2
Manipulación de los registros de Actividad (log)		
Manipulación de la configuración		
Suplantación de la identidad del usuario	X	3
Abuso de privilegios de acceso	X	3
Difusión de software dañino	X	2
Acceso no autorizado	X	3
Modificación deliberada de la información	X	2
Destrucción deliberada de Información	X	2
Divulgación de la Información	X	4
Manipulación de programas	X	2
Manipulación de los equipos	X	2
Denegación del servicio	X	1
Robo de Equipos	X	3
Indisponibilidad deliberada del personal	X	3
Extorsión		
Ejecución de ingeniería social	X	2
Corte del suministro eléctrico		
Condiciones inadecuadas de temperatura o humedad		
Degradación de los soportes de almacenamiento de la información	X	3
Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones	X	2
Hacking no ético	X	2
Instalación de software no autorizado		
Otro:		

Fuente: MAGERIT v3, elaboración propia

G) PERSONAL PROPIO

Tabla 15 Identificación de amenazas del activo de información-Personal propio

Amenaza	Marca (X)	Probabilidad de ocurrencia
Fuego		
Tormenta eléctrica, rayo		
Error de Usuario	X	3
Errores del administrador		
Errores de configuración		
Alteración accidental de la información	X	3
Destrucción de Información	X	2
Fugas de Información	X	2
Vulnerabilidades de los programas (software)		
Errores de mantenimiento / actualización de programas (software)		
Errores de mantenimiento / actualización de equipos (hardware)		
Caída del sistema por agotamiento de recursos (interrupción en los servicios)		
Indisponibilidad del personal	X	1
Manipulación de los registros de Actividad (log)		
Manipulación de la configuración		
Suplantación de la identidad del usuario	X	1
Abuso de privilegios de acceso		
Difusión de software dañino		
Acceso no autorizado		
Modificación deliberada de la información	X	3
Destrucción deliberada de Información	X	2
Divulgación de la Información	X	2
Manipulación de programas		
Manipulación de los equipos		
Denegación del servicio		
Robo de Equipos	X	4
Indisponibilidad deliberada del personal	X	3
Extorsión		
Ejecución de ingeniería social		
Corte del suministro eléctrico		
Condiciones inadecuadas de temperatura o humedad		
Degradación de los soportes de almacenamiento de la información		
Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones		
Hacking no ético		
Instalación de software no autorizado		
Otro:		

Fuente: MAGERIT v3, elaboración propia

H) APPS INFORMÁTICAS

Tabla 16 Identificación de amenazas del activo de información-Apps Informáticas

Amenaza	Marca (X)	Probabilidad de ocurrencia
Fuego		
Tormenta eléctrica, rayo		
Error de Usuario	X	3
Errores del administrador	X	3
Errores de configuración	X	2
Alteración accidental de la información	X	3
Destrucción de Información	X	4
Fugas de Información	X	4
Vulnerabilidades de los programas (software)	X	4
Errores de mantenimiento / actualización de programas (software)	X	3
Errores de mantenimiento / actualización de equipos (hardware)		
Caída del sistema por agotamiento de recursos (interrupción en los servicios)	X	3
Indisponibilidad del personal		
Manipulación de los registros de Actividad (log)	X	3
Manipulación de la configuración	X	2
Suplantación de la identidad del usuario	X	2
Abuso de privilegios de acceso	X	1
Difusión de software dañino		
Acceso no autorizado	X	3
Modificación deliberada de la información	X	3
Destrucción deliberada de Información	X	2
Divulgación de la Información	X	2
Manipulación de programas	X	1
Manipulación de los equipos		
Denegación del servicio	X	1
Robo de Equipos	X	2
Indisponibilidad deliberada del personal		
Extorsión		
Ejecución de ingeniería social		
Corte del suministro eléctrico		
Condiciones inadecuadas de temperatura o humedad		
Degradación de los soportes de almacenamiento de la información	X	3
Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones	X	2
Hacking no ético	X	2
Instalación de software no autorizado		
Otro:		

Fuente: MAGERIT v3, elaboración propia

I) GESTORES DE BASE DE DATOS

Tabla 17 Identificación de amenazas del activo de información- Gestores de base de datos

Amenaza	Marca (X)	Probabilidad de ocurrencia
Fuego		
Tormenta eléctrica, rayo		
Error de Usuario	X	2
Errores del administrador	X	1
Errores de configuración	X	3
Alteración accidental de la información	X	2
Destrucción de Información	X	2
Fugas de Información	X	2
Vulnerabilidades de los programas (software)	X	1
Errores de mantenimiento / actualización de programas (software)	X	2
Errores de mantenimiento / actualización de equipos (hardware)		
Caída del sistema por agotamiento de recursos (interrupción en los servicios)	X	1
Indisponibilidad del personal		
Manipulación de los registros de Actividad (log)	X	1
Manipulación de la configuración	X	1
Suplantación de la identidad del usuario	X	1
Abuso de privilegios de acceso	X	2
Difusión de software dañino		
Acceso no autorizado	X	1
Modificación deliberada de la información	X	2
Destrucción deliberada de Información	X	1
Divulgación de la Información	X	1
Manipulación de programas	X	2
Manipulación de los equipos		
Denegación del servicio	X	2
Robo de Equipos	X	1
Indisponibilidad deliberada del personal		
Extorsión		
Ejecución de ingeniería social		
Corte del suministro eléctrico		
Condiciones inadecuadas de temperatura o humedad		
Degradación de los soportes de almacenamiento de la información		
Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones		
Hacking no ético		
Instalación de software no autorizado		
Otro:		

Fuente: MAGERIT v3, elaboración propia

J) SISTEMAS EXTERNOS

Tabla 18 Identificación de amenazas del activo de información-Sistemas externos

Amenaza	Marca (X)	Probabilidad de ocurrencia
Fuego		
Tormenta eléctrica, rayo		
Error de Usuario	X	2
Errores del administrador	X	1
Errores de configuración	X	2
Alteración accidental de la información		
Destrucción de Información		
Fugas de Información	X	4
Vulnerabilidades de los programas (software)	X	2
Errores de mantenimiento / actualización de programas (software)	X	1
Errores de mantenimiento / actualización de equipos (hardware)		
Caída del sistema por agotamiento de recursos (interrupción en los servicios)	X	2
Indisponibilidad del personal		
Manipulación de los registros de Actividad (log)		
Manipulación de la configuración		
Suplantación de la identidad del usuario	X	3
Abuso de privilegios de acceso	X	3
Difusión de software dañino		
Acceso no autorizado	X	4
Modificación deliberada de la información		
Destrucción deliberada de Información		
Divulgación de la Información	X	2
Manipulación de programas		
Manipulación de los equipos		
Denegación del servicio		
Robo de Equipos		
Indisponibilidad deliberada del personal		
Extorsión		
Ejecución de ingeniería social		
Corte del suministro eléctrico		
Condiciones inadecuadas de temperatura o humedad		
Degradación de los soportes de almacenamiento de la información	X	2
Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones	X	2
Hacking no ético	X	1
Instalación de software no autorizado		
Otro:		

Fuente: MAGERIT v3, elaboración propia

3.5 Evaluación de riesgos de los Activos de información

Para cada activo de información, los requerimientos de seguridad propuestos por COBIT 5 son:

- Confidencialidad
- Integridad
- Disponibilidad

Para hacer la matriz de impactos y riesgos primero tuvimos que darle valor a nuestros activos de información, los cuales fueron obtenidos con la ayuda de los trabajadores del área de TI la cooperativa Santo Domingo de Guzmán (ver anexo 5) se logró obtener dichos valores y estos que quedaron de la siguiente manera:

Tabla 19 Valoración de los activos de información

ACTIVO DE LA INFORMACIÓN	VALOR (1 – 5)
A) Equipos informáticos	3
B) Servidores	5
C) Equipos de red local	5
D) Periféricos y pendrives	3
E) Portátiles, tabletas y móviles	2
F) Oficinas	5
G) Personal propio	5
H) Aplicaciones informáticas	4
I) Gestores de base de datos	4
J) Sistemas externos	4

Fuente: Elaboración conjunta con trabajadores de la CACSDG.

I) Degradación

Seguidamente creamos parámetros para nuestra **degradación** que fueron los siguientes:

Tabla 20 Parámetros de degradación.

CRITERIO	VALOR
Sin degradación	**1**
Degradación baja	**2**
Degradación media	**3**
Degradación alta	**4**

Fuente: Elaboración propia.

Teniendo en cuenta los parámetros de degradación se crea una pequeña matriz para poder calcular el impacto

Tabla 21 Degradación de la amenaza

DEGRADACIÓN DE LA AMENAZA	VALOR DEL ACTIVO				
	1	2	3	4	5
1 (sin degradación)	**1**	**1**	**1**	**1**	**1**
2 (degradación baja)	**1**	**2**	**2**	**3**	**3**
3 (degradación media)	**1**	**3**	**4**	**4**	**5**
4 (degradación alta)	**1**	**3**	**4**	**5**	**5**

Fuente: Elaboración propia.

II) Impacto

Después para calificar el valor del **impacto** se usó los siguientes parámetros:

Tabla 22 Valores del impacto

DESCRIPCIÓN	VALOR
Insignificante	**1**
Menor	**2**
Medio	**3**
Critico	**4**
Catastrófico	**5**

Fuente: Elaboración propia.

III) Riesgo

Una vez teniendo nuestros valores del impacto pasamos a estimar el **riesgo** de la siguiente manera.

Cruzamos los valores de nuestro **impacto** con los valores de **riesgo** existente:

Tabla 23 Matriz de valoración de riesgos

Matriz de valoración de riesgos		Riesgo			
		Insignificante	Moderada	Dañina	Extrema
		1	2	3	4
Impacto	5 (Catastrófico)	Medio	Alto	Alto	Alto
	4 (Critico)	Medio	Medio	Alto	Alto
	3 (Medio)	Bajo	Medio	Medio	Alto
	2 (Menor)	Bajo	Bajo	Bajo	Medio
	1 (Insignificante)	Bajo	Bajo	Bajo	Medio

Fuente: Elaboración propia.

Tabla 24 Evaluación de las amenazas y riesgos del activo de información – Equipos informáticos

A) EQUIPOS INFORMÁTICOS											
Amenaza	Probabilidad	Degradación			Impacto			Estimación del riesgo			
		Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	
Fuego	1	1	1	2	Insignificante	Insignificante	Menor	BAJO	BAJO	MEDIO	
Tormenta eléctrica, rayo	3	1	1	2	Insignificante	Insignificante	Menor	BAJO	BAJO	BAJO	
Error de Usuario	2	2	1	2	Menor	Insignificante	Menor	BAJO	BAJO	BAJO	
Errores del administrador	2	2	2	2	Menor	Menor	Menor	BAJO	MEDIO	BAJO	
Errores de configuración	2	1	2	1	Insignificante	Menor	Insignificante	MEDIO	MEDIO	BAJO	
Alteración accidental de la información	1	3	2	2	Critico	Menor	Menor	ALTO	BAJO	BAJO	
Destrucción de Información	1	4	2	4	Critico	Menor	Critico	MEDIO	BAJO	ALTO	
Vulnerabilidades de los programas (software)	1	2	1	2	Menor	Insignificante	Menor	BAJO	BAJO	BAJO	
Errores de mantenimiento / actualización de equipos (hardware)	2	3	2	2	Critico	Menor	Menor	MEDIO	BAJO	BAJO	
Indisponibilidad del personal	2	1	1	1	Insignificante	Insignificante	Insignificante	BAJO	BAJO	BAJO	
Manipulación de la configuración	3	1	2	1	Insignificante	Menor	Insignificante	BAJO	MEDIO	BAJO	
Abuso de privilegios de acceso	2	1	3	1	Insignificante	Critico	Insignificante	BAJO	ALTO	BAJO	
Acceso no autorizado	4	1	3	1	Insignificante	Critico	Insignificante	BAJO	ALTO	BAJO	
Modificación deliberada de la información	3	3	1	1	Critico	Insignificante	Insignificante	ALTO	BAJO	BAJO	
Divulgación de la Información	4	4	4	1	Critico	Critico	Insignificante	MEDIO	MEDIO	BAJO	
Manipulación de los equipos	2	2	2	1	Menor	Menor	Insignificante	BAJO	BAJO	BAJO	
Robo de Equipos	3	3	1	1	Critico	Insignificante	Insignificante	ALTO	BAJO	BAJO	

Indisponibilidad deliberada del personal	4	2	1	1	Menor	Insignificante	Insignificante	BAJO	BAJO	BAJO
Corte del suministro eléctrico	2	2	2	4	Menor	Menor	Critico	MEDIO	BAJO	MEDIO
Degradación de los soportes de almacenamiento de la información	2	1	1	4	Insignificante	Insignificante	Critico	BAJO	MEDIO	MEDIO
Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones	3	2	2	1	Menor	Menor	Insignificante	BAJO	BAJO	BAJO
Hacking no ético	3	2	1	1	Menor	Insignificante	Insignificante	BAJO	BAJO	BAJO

Fuente: Elaboración propia.

Tabla 25 Evaluación de las amenazas y riesgos del activo de información – Servidores

B) SERVIDORES											
Amenaza	Probabilidad	Degradación			Impacto			Estimación del riesgo			
		Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	
Fuego	1	3	3	3	Catastrófico	Catastrófico	Catastrófico	MEDIO	MEDIO	ALTO	
Tormenta eléctrica, rayo	3	1	3	2	Insignificante	Catastrófico	Medio	BAJO	ALTO	MEDIO	
Errores del administrador	3	2	2	1	Medio	Medio	Insignificante	BAJO	MEDIO	BAJO	
Errores de configuración	3	3	2	1	Catastrófico	Medio	Insignificante	ALTO	MEDIO	BAJO	
Alteración accidental de la información	2	3	2	2	Catastrófico	Medio	Medio	ALTO	BAJO	BAJO	
Destrucción de Información	2	4	4	4	Catastrófico	Catastrófico	Catastrófico	ALTO	MEDIO	MEDIO	
Fugas de Información	2	4	2	4	Catastrófico	Medio	Catastrófico	ALTO	BAJO	MEDIO	
Vulnerabilidades de los programas (software)	1	3	3	3	Catastrófico	Catastrófico	Catastrófico	ALTO	ALTO	ALTO	
Errores de mantenimiento / actualización de programas (software)	1	3	2	2	Catastrófico	Medio	Medio	ALTO	BAJO	BAJO	
Errores de mantenimiento / actualización de equipos (hardware)	1	3	3	3	Catastrófico	Catastrófico	Catastrófico	MEDIO	ALTO	MEDIO	
Caída del sistema por agotamiento de recursos (interrupción en los servicios)	1	3	3	3	Catastrófico	Catastrófico	Catastrófico	MEDIO	MEDIO	MEDIO	
Manipulación de la configuración	2	3	3	2	Catastrófico	Catastrófico	Medio	ALTO	MEDIO	BAJO	
Suplantación de la identidad del usuario	4	3	2	3	Catastrófico	Medio	Catastrófico	ALTO	MEDIO	MEDIO	
Abuso de privilegios de acceso	4	2	2	2	Medio	Medio	Medio	BAJO	MEDIO	BAJO	
Difusión de software dañino	2	3	4	4	Catastrófico	Catastrófico	Catastrófico	ALTO	MEDIO	ALTO	
Acceso no autorizado	3	4	4	4	Catastrófico	Catastrófico	Catastrófico	MEDIO	MEDIO	ALTO	
Modificación deliberada de la información	2	3	3	3	Catastrófico	Catastrófico	Catastrófico	MEDIO	MEDIO	ALTO	

Destrucción deliberada de Información	1	3	1	4	Catastrófico	Insignificante	Catastrófico	MEDIO	BAJO	MEDIO
Divulgación de la Información	2	4	1	4	Catastrófico	Insignificante	Catastrófico	MEDIO	BAJO	MEDIO
Manipulación de programas	2	1	1	1	Insignificante	Insignificante	Insignificante	BAJO	BAJO	BAJO
Manipulación de los equipos	2	1	1	1	Insignificante	Insignificante	Insignificante	BAJO	BAJO	BAJO
Denegación del servicio	3	3	1	4	Catastrófico	Insignificante	Catastrófico	ALTO	BAJO	MEDIO
Robo de Equipos	1	3	3	2	Catastrófico	Catastrófico	Medio	MEDIO	MEDIO	BAJO
Corte del suministro eléctrico	2	1	1	1	Insignificante	Insignificante	Insignificante	BAJO	BAJO	BAJO
Degradación de los soportes de almacenamiento de la información	2	1	1	1	Insignificante	Insignificante	Insignificante	BAJO	BAJO	BAJO
Hacking no ético	3	1	2	1	Insignificante	Medio	Insignificante	BAJO	MEDIO	BAJO

Fuente: Elaboración propia.

Tabla 26 Evaluación de las amenazas y riesgos del activo de información – Equipos de red local

C) EQUIPOS DE RED LOCAL											
Amenaza	Probabilidad	Degradación			Impacto			Estimación del riesgo			
		Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	
Fuego	1	2	1	1	Medio	Insignificante	Insignificante	BAJO	BAJO	BAJO	
Tormenta eléctrica, rayo	3	3	1	1	Catastrófico	Insignificante	Insignificante	ALTO	BAJO	BAJO	
Error de Usuario	3	2	2	2	Medio	Medio	Medio	MEDIO	MEDIO	BAJO	
Errores del administrador	2	1	2	1	Insignificante	Medio	Insignificante	BAJO	BAJO	BAJO	
Errores de configuración	2	2	2	2	Medio	Medio	Medio	BAJO	BAJO	BAJO	
Alteración accidental de la información	3	3	4	3	Catastrófico	Catastrófico	Catastrófico	ALTO	MEDIO	MEDIO	
Destrucción de Información	3	4	4	3	Catastrófico	Catastrófico	Catastrófico	ALTO	ALTO	MEDIO	
Fugas de Información	4	3	3	3	Catastrófico	Catastrófico	Catastrófico	MEDIO	MEDIO	ALTO	
Vulnerabilidades de los programas (software)	4	1	2	1	Insignificante	Medio	Insignificante	BAJO	BAJO	BAJO	
Errores de mantenimiento / actualización de programas (software)	4	1	3	2	Insignificante	Catastrófico	Medio	BAJO	ALTO	BAJO	
Errores de mantenimiento / actualización de equipos (hardware)	4	2	1	3	Medio	Insignificante	Catastrófico	BAJO	BAJO	MEDIO	
Caída del sistema por agotamiento de recursos (interrupción en los servicios)	2	1	2	3	Insignificante	Medio	Catastrófico	BAJO	BAJO	MEDIO	
Indisponibilidad del personal	2	3	2	2	Catastrófico	Medio	Medio	ALTO	BAJO	BAJO	
Manipulación de la configuración	3	1	2	1	Insignificante	Medio	Insignificante	BAJO	BAJO	BAJO	
Suplantación de la identidad del usuario	1	3	4	4	Catastrófico	Catastrófico	Catastrófico	MEDIO	ALTO	MEDIO	
Abuso de privilegios de acceso	2	2	2	2	Medio	Medio	Medio	BAJO	MEDIO	ALTO	
Difusión de software dañino	2	3	3	4	Catastrófico	Catastrófico	Catastrófico	ALTO	MEDIO	ALTO	
Acceso no autorizado	3	3	1	3	Catastrófico	Insignificante	Catastrófico	MEDIO	BAJO	MEDIO	

Modificación deliberada de la información	3	4	1	1	Catastrófico	Insignificante	Insignificante	ALTO	BAJO	BAJO
Destrucción deliberada de Información	3	4	4	4	Catastrófico	Catastrófico	Catastrófico	MEDIO	MEDIO	MEDIO
Divulgación de la Información	3	3	3	3	Catastrófico	Catastrófico	Catastrófico	MEDIO	MEDIO	MEDIO
Manipulación de programas	3	1	2	4	Insignificante	Medio	Catastrófico	BAJO	BAJO	ALTO
Manipulación de los equipos	3	3	1	2	Catastrófico	Insignificante	Medio	MEDIO	BAJO	BAJO
Denegación del servicio	2	2	3	1	Medio	Catastrófico	Insignificante	MEDIO	ALTO	BAJO
Robo de Equipos	1	3	1	4	Catastrófico	Insignificante	Catastrófico	MEDIO	BAJO	MEDIO
Indisponibilidad deliberada del personal	3	3	2	4	Catastrófico	Medio	Catastrófico	ALTO	BAJO	ALTO
Corte del suministro eléctrico	2	2	1	3	Medio	Insignificante	Catastrófico	MEDIO	BAJO	ALTO
Degradación de los soportes de almacenamiento de la información	2	1	1	2	Insignificante	Insignificante	Medio	MEDIO	BAJO	MEDIO
Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones	4	1	2	2	Insignificante	Medio	Medio	BAJO	BAJO	MEDIO
Hacking no ético	2	1	2	3	Insignificante	Medio	Catastrófico	BAJO	BAJO	MEDIO
Instalación de software no autorizado	4	3	3	4	Catastrófico	Catastrófico	Catastrófico	ALTO	ALTO	ALTO

Fuente: Elaboración propia.

Tabla 27 Evaluación de las amenazas y riesgos del activo de información – Periféricos y pendrives

D) PERIFÉRICOS Y PENDRIVES											
Amenaza	Probabilidad	Degradación			Impacto			Estimación del riesgo			
		Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	
Error de Usuario	2	3	3	2	Critico	Critico	Menor	MEDIO	ALTO	BAJO	
Errores del administrador	2	2	1	3	Menor	Insignificante	Critico	BAJO	BAJO	ALTO	
Errores de configuración	3	2	1	2	Menor	Insignificante	Menor	BAJO	BAJO	BAJO	
Alteración accidental de la información	4	1	3	4	Insignificante	Critico	Critico	BAJO	MEDIO	ALTO	
Destrucción de Información	4	2	4	4	Menor	Critico	Critico	BAJO	MEDIO	ALTO	
Fugas de Información	4	4	2	4	Critico	Menor	Critico	MEDIO	BAJO	MEDIO	
Indisponibilidad del personal	2	1	1	2	Insignificante	Insignificante	Menor	BAJO	BAJO	BAJO	
Manipulación de la configuración	2	2	1	3	Menor	Insignificante	Critico	BAJO	BAJO	ALTO	
Suplantación de la identidad del usuario	2	1	1	2	Insignificante	Insignificante	Menor	BAJO	BAJO	BAJO	
Abuso de privilegios de acceso	4	1	2	1	Insignificante	Menor	Insignificante	BAJO	BAJO	BAJO	
Difusión de software dañino	4	2	3	4	Menor	Critico	Critico	BAJO	MEDIO	MEDIO	
Acceso no autorizado	4	4	4	4	Critico	Critico	Critico	ALTO	ALTO	MEDIO	
Modificación deliberada de la información	4	4	4	3	Critico	Critico	Critico	ALTO	ALTO	ALTO	
Destrucción deliberada de Información	4	4	3	3	Critico	Critico	Critico	ALTO	MEDIO	ALTO	
Divulgación de la Información	4	4	4	4	Critico	Critico	Critico	MEDIO	MEDIO	MEDIO	

Robo de Equipos	5	4	4	3	Critico	Critico	Critico	ALTO	ALTO	ALTO
Indisponibilidad deliberada del personal	3	1	1	1	Insignificante	Insignificante	Insignificante	BAJO	BAJO	BAJO
Hacking no ético	3	2	1	1	Menor	Insignificante	Insignificante	BAJO	BAJO	BAJO

Fuente: Elaboración propia.

Tabla 28 Evaluación de las amenazas y riesgos del activo de información – Portátiles, tabletas y móviles

E) PORTÁTILES, TABLETAS Y MÓVILES											
Amenaza	Probabilidad	Degradación			Impacto			Estimación del riesgo			
		Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	
Fuego	1	1	1	1	Insignificante	Insignificante	Insignificante	BAJO	BAJO	BAJO	
Tormenta eléctrica, rayo	4	2	1	1	Menor	Insignificante	Insignificante	MEDIO	BAJO	BAJO	
Error de Usuario	2	1	2	2	Insignificante	Menor	Menor	BAJO	BAJO	BAJO	
Errores del administrador	2	3	3	1	Medio	Medio	Insignificante	ALTO	ALTO	BAJO	
Errores de configuración	2	2	1	1	Menor	Insignificante	Insignificante	MEDIO	BAJO	BAJO	
Alteración accidental de la información	3	3	3	2	Medio	Medio	Menor	ALTO	ALTO	BAJO	
Destrucción de Información	3	3	2	1	Medio	Menor	Insignificante	ALTO	BAJO	BAJO	
Fugas de Información	5	2	1	1	Menor	Insignificante	Insignificante	MEDIO	BAJO	BAJO	
Vulnerabilidades de los programas (software)	5	1	2	4	Insignificante	Menor	Medio	BAJO	BAJO	BAJO	
Errores de mantenimiento / actualización de programas (software)	5	2	3	1	Menor	Medio	Insignificante	BAJO	ALTO	BAJO	
Errores de mantenimiento / actualización de equipos (hardware)	5	4	3	2	Medio	Medio	Menor	ALTO	ALTO	BAJO	
Manipulación de la configuración	4	1	2	2	Insignificante	Menor	Menor	BAJO	MEDIO	BAJO	
Suplantación de la identidad del usuario	4	2	1	1	Menor	Insignificante	Insignificante	BAJO	BAJO	BAJO	
Abuso de privilegios de acceso	3	4	3	1	Medio	Insignificante	Insignificante	ALTO	BAJO	BAJO	
Difusión de software dañino	4	4	4	3	Medio	Medio	Medio	MEDIO	ALTO	ALTO	
Modificación deliberada de la información	3	1	2	2	Insignificante	Menor	Menor	BAJO	BAJO	MEDIO	
Destrucción deliberada de Información	3	1	1	2	Insignificante	Insignificante	Menor	BAJO	BAJO	MEDIO	
Divulgación de la Información	4	1	3	4	Insignificante	Medio	Medio	BAJO	ALTO	ALTO	

Manipulación de programas	3	2	3	1	Menor	Medio	Insignificante	BAJO	ALTO	MEDIO
Manipulación de los equipos	3	2	1	1	Menor	Insignificante	Insignificante	BAJO	BAJO	MEDIO
Robo de Equipos	5	2	3	2	Menor	Medio	Menor	MEDIO	MEDIO	BAJO
Indisponibilidad deliberada del personal	4	3	1	1	Medio	Insignificante	Insignificante	ALTO	BAJO	BAJO
Degradación de los soportes de almacenamiento de la información	3	2	1	2	Menor	Insignificante	Menor	BAJO	BAJO	BAJO
Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones	4	3	2	1	Medio	Menor	Insignificante	ALTO	BAJO	BAJO
Hacking no ético	4	3	3	3	Medio	Medio	Medio	MEDIO	MEDIO	BAJO
Instalación de software no autorizado	3	2	1	1	Menor	Insignificante	Insignificante	BAJO	BAJO	BAJO

Fuente: Elaboración propia.

Tabla 29 Evaluación de las amenazas y riesgos del activo de información – Oficinas

F) OFICINAS										
Amenaza	Probabilidad	Degradación			Impacto			Estimación del riesgo		
		Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad
Fuego	1	2	4	2	Medio	Catastrófico	Medio	BAJO	MEDIO	BAJO
Error de Usuario	2	1	1	1	Insignificante	Insignificante	Insignificante	BAJO	BAJO	BAJO
Errores del administrador	2	1	2	2	Insignificante	Medio	Medio	BAJO	BAJO	MEDIO
Errores de configuración	2	3	2	3	Catastrófico	Medio	Catastrófico	MEDIO	ALTO	ALTO
Alteración accidental de la información	2	4	4	3	Catastrófico	Catastrófico	Catastrófico	ALTO	ALTO	MEDIO
Destrucción de Información	3	2	2	3	Medio	Medio	Catastrófico	MEDIO	BAJO	MEDIO
Fugas de Información	2	2	1	3	Medio	Insignificante	Catastrófico	MEDIO	BAJO	ALTO
Errores de mantenimiento / actualización de equipos (hardware)	2	4	4	3	Catastrófico	Catastrófico	Catastrófico	ALTO	MEDIO	ALTO
Caída del sistema por agotamiento de recursos (interrupción en los servicios)	2	2	4	3	Medio	Catastrófico	Catastrófico	ALTO	MEDIO	MEDIO
Indisponibilidad del personal	2	3	2	2	Catastrófico	Medio	Medio	ALTO	BAJO	BAJO
Suplantación de la identidad del usuario	3	1	3	1	Insignificante	Catastrófico	Insignificante	BAJO	MEDIO	BAJO
Abuso de privilegios de acceso	3	3	1	3	Catastrófico	Insignificante	Catastrófico	ALTO	BAJO	ALTO
Difusión de software dañino	2	1	1	3	Insignificante	Insignificante	Catastrófico	BAJO	BAJO	MEDIO
Acceso no autorizado	3	3	1	3	Catastrófico	Insignificante	Catastrófico	ALTO	BAJO	ALTO
Modificación deliberada de la información	2	3	2	2	Catastrófico	Medio	Medio	ALTO	ALTO	MEDIO
Destrucción deliberada de Información	2	4	3	4	Catastrófico	Catastrófico	Catastrófico	MEDIO	MEDIO	MEDIO
Divulgación de la Información	4	2	1	2	Medio	Insignificante	Medio	ALTO	BAJO	MEDIO
Manipulación de programas	2	4	3	1	Catastrófico	Catastrófico	Insignificante	ALTO	ALTO	BAJO

Manipulación de los equipos	2	4	3	2	Catastrófico	Catastrófico	Medio	ALTO	ALTO	MEDIO
Denegación del servicio	1	2	1	2	Medio	Insignificante	Medio	MEDIO	BAJO	ALTO
Robo de Equipos	3	4	3	2	Catastrófico	Catastrófico	Medio	MEDIO	ALTO	ALTO
Indisponibilidad deliberada del personal	3	3	2	1	Catastrófico	Medio	Insignificante	MEDIO	MEDIO	BAJO
Ejecución de ingeniería social	2	3	1	3	Catastrófico	Insignificante	Catastrófico	MEDIO	BAJO	ALTO
Degradación de los soportes de almacenamiento de la información	3	4	4	1	Catastrófico	Catastrófico	Insignificante	ALTO	ALTO	BAJO
Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones	2	1	3	2	Insignificante	Catastrófico	Medio	BAJO	ALTO	MEDIO
Hacking no ético	2	2	3	1	Medio	Catastrófico	Insignificante	ALTO	ALTO	ALTO

Fuente: Elaboración propia.

Tabla 30 Evaluación de las amenazas y riesgos del activo de información – Personal propio

G) PERSONAL PROPIO											
Amenaza	Probabilidad	Degradación			Impacto			Estimación del riesgo			
		Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	
Error de Usuario	3	1	2	1	Insignificante	Medio	Insignificante	BAJO	BAJO	MEDIO	
Alteración accidental de la información	3	3	1	2	Catastrófico	Insignificante	Medio	MEDIO	BAJO	BAJO	
Destrucción de Información	2	4	2	2	Catastrófico	Medio	Medio	MEDIO	BAJO	BAJO	
Fugas de Información	2	4	1	2	Catastrófico	Insignificante	Medio	ALTO	BAJO	MEDIO	
Indisponibilidad del personal	1	4	3	1	Catastrófico	Catastrófico	Insignificante	ALTO	MEDIO	BAJO	
Suplantación de la identidad del usuario	1	2	2	1	Medio	Medio	Insignificante	MEDIO	ALTO	BAJO	
Modificación deliberada de la información	3	2	3	4	Medio	Catastrófico	Catastrófico	BAJO	ALTO	MEDIO	
Destrucción deliberada de Información	2	2	3	1	Medio	Catastrófico	Insignificante	BAJO	MEDIO	BAJO	
Divulgación de la Información	2	3	1	1	Catastrófico	Insignificante	Insignificante	MEDIO	BAJO	BAJO	
Robo de Equipos	4	2	3	1	Medio	Catastrófico	Insignificante	ALTO	ALTO	MEDIO	
Indisponibilidad deliberada del personal	3	3	1	1	Catastrófico	Insignificante	Insignificante	MEDIO	MEDIO	BAJO	

Fuente: Elaboración propia.

Tabla 31 Evaluación de las amenazas y riesgos del activo de información – Aplicaciones informáticas

H) APLICACIONES INFORMÁTICAS											
Amenaza	Probabilidad	Degradación			Impacto			Estimación del riesgo			
		Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	
Error de Usuario	3	1	3	2	Insignificante	Critico	Medio	BAJO	MEDIO	MEDIO	
Errores del administrador	3	2	1	4	Medio	Insignificante	Catastrófico	MEDIO	BAJO	MEDIO	
Errores de configuración	2	3	2	2	Critico	Medio	Medio	ALTO	MEDIO	MEDIO	
Alteración accidental de la información	3	1	4	2	Insignificante	Catastrófico	Medio	BAJO	ALTO	ALTO	
Destrucción de Información	4	2	2	1	Medio	Medio	Insignificante	ALTO	MEDIO	BAJO	
Fugas de Información	4	3	4	2	Critico	Catastrófico	Medio	ALTO	ALTO	MEDIO	
Vulnerabilidades de los programas (software)	4	4	2	3	Catastrófico	Medio	Critico	ALTO	ALTO	MEDIO	
Errores de mantenimiento / actualización de programas (software)	3	1	3	2	Insignificante	Critico	Medio	BAJO	ALTO	MEDIO	
Caída del sistema por agotamiento de recursos (interrupción en los servicios)	3	1	3	2	Insignificante	Critico	Medio	BAJO	ALTO	ALTO	
Manipulación de los registros de Actividad (log)	3	1	3	1	Insignificante	Critico	Insignificante	BAJO	ALTO	BAJO	
Manipulación de la configuración	2	3	2	1	Critico	Medio	Insignificante	ALTO	ALTO	BAJO	
Suplantación de la identidad del usuario	2	2	3	4	Medio	Critico	Catastrófico	MEDIO	ALTO	ALTO	
Abuso de privilegios de acceso	1	2	2	1	Medio	Medio	Insignificante	ALTO	ALTO	BAJO	
Acceso no autorizado	3	2	3	3	Medio	Critico	Critico	BAJO	ALTO	ALTO	
Modificación deliberada de la información	3	3	3	2	Critico	Critico	Medio	ALTO	MEDIO	MEDIO	
Destrucción deliberada de Información	2	1	1	2	Insignificante	Insignificante	Medio	BAJO	BAJO	MEDIO	
Divulgación de la Información	2	3	1	1	Critico	Insignificante	Insignificante	MEDIO	BAJO	BAJO	
Manipulación de programas	1	1	2	1	Insignificante	Medio	Insignificante	BAJO	MEDIO	BAJO	
Denegación del servicio	1	3	3	4	Critico	Critico	Catastrófico	MEDIO	MEDIO	ALTO	

Robo de Equipos	2	1	2	3	Insignificante	Medio	Critico	BAJO	MEDIO	ALTO
Degradación de los soportes de almacenamiento de la información	3	2	1	3	Medio	Insignificante	Critico	ALTO	BAJO	MEDIO
Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones	2	1	1	3	Insignificante	Insignificante	Critico	BAJO	BAJO	MEDIO
Hacking no ético	2	2	3	4	Medio	Critico	Catastrófico	MEDIO	MEDIO	ALTO

Fuente: Elaboración propia.

Tabla 32 Evaluación de las amenazas y riesgos del activo de información – Gestores de base de datos

I) GESTORES DE BASE DE DATOS										
Amenaza	Probabilidad	Degradación			Impacto			Estimación del riesgo		
		Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad
Error de Usuario	2	3	2	1	Critico	Medio	Insignificante	MEDIO	BAJO	BAJO
Errores del administrador	1	1	1	3	Insignificante	Insignificante	Critico	BAJO	BAJO	MEDIO
Errores de configuración	3	1	1	2	Insignificante	Insignificante	Medio	BAJO	BAJO	ALTO
Alteración accidental de la información	2	3	4	2	Critico	Catastrófico	Medio	MEDIO	MEDIO	ALTO
Destrucción de Información	2	1	3	1	Insignificante	Critico	Insignificante	BAJO	MEDIO	BAJO
Fugas de Información	2	4	1	2	Catastrófico	Insignificante	Medio	ALTO	BAJO	MEDIO
Vulnerabilidades de los programas (software)	1	1	2	3	Insignificante	Medio	Critico	BAJO	MEDIO	MEDIO
Errores de mantenimiento / actualización de programas (software)	2	4	2	1	Catastrófico	Medio	Insignificante	ALTO	MEDIO	BAJO
Caída del sistema por agotamiento de recursos (interrupción en los servicios)	1	3	4	1	Critico	Catastrófico	Insignificante	ALTO	MEDIO	BAJO
Manipulación de los registros de Actividad (log)	1	3	2	1	Critico	Medio	Insignificante	ALTO	BAJO	BAJO
Manipulación de la configuración	1	2	3	4	Medio	Critico	Catastrófico	MEDIO	MEDIO	MEDIO
Suplantación de la identidad del usuario	1	3	3	1	Critico	Critico	Insignificante	MEDIO	MEDIO	BAJO
Abuso de privilegios de acceso	2	2	3	1	Medio	Critico	Insignificante	BAJO	ALTO	BAJO
Acceso no autorizado	1	2	3	2	Medio	Critico	Medio	BAJO	ALTO	MEDIO
Modificación deliberada de la información	2	1	3	1	Insignificante	Critico	Insignificante	BAJO	MEDIO	BAJO

Destrucción deliberada de Información	1	2	3	4	Medio	Critico	Catastrófico	BAJO	MEDIO	ALTO
Divulgación de la Información	1	3	1	3	Critico	Insignificante	Critico	MEDIO	MEDIO	ALTO
Manipulación de programas	2	1	2	3	Insignificante	Medio	Critico	BAJO	MEDIO	ALTO
Denegación del servicio	2	1	4	2	Insignificante	Catastrófico	Medio	BAJO	MEDIO	BAJO
Robo de Equipos	1	3	2	4	Critico	Medio	Catastrófico	ALTO	BAJO	MEDIO

Fuente: Elaboración propia.

Tabla 33 Evaluación de las amenazas y riesgos del activo de información – Sistemas externos

J) SISTEMAS EXTERNOS											
Amenaza	Probabilidad	Degradación			Impacto			Estimación del riesgo			
		Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	
Error de Usuario	2	3	2	4	Critico	Medio	Catastrófico	ALTO	MEDIO	MEDIO	
Errores del administrador	1	2	2	4	Medio	Medio	Catastrófico	MEDIO	BAJO	MEDIO	
Errores de configuración	2	1	1	1	Insignificante	Insignificante	Insignificante	MEDIO	BAJO	BAJO	
Fugas de Información	4	3	4	2	Critico	Catastrófico	Medio	MEDIO	ALTO	ALTO	
Vulnerabilidades de los programas (software)	2	4	3	1	Catastrófico	Critico	Insignificante	ALTO	ALTO	BAJO	
Errores de mantenimiento / actualización de programas (software)	1	2	2	3	Medio	Medio	Critico	BAJO	MEDIO	ALTO	
Caída del sistema por agotamiento de recursos (interrupción en los servicios)	2	2	4	3	Medio	Catastrófico	Critico	BAJO	ALTO	MEDIO	
Suplantación de la identidad del usuario	3	3	4	2	Critico	Catastrófico	Medio	ALTO	MEDIO	ALTO	
Abuso de privilegios de acceso	3	2	3	4	Medio	Critico	Catastrófico	BAJO	MEDIO	ALTO	
Acceso no autorizado	4	2	2	2	Medio	Medio	Medio	BAJO	MEDIO	MEDIO	
Divulgación de la Información	2	1	1	4	Insignificante	Insignificante	Catastrófico	BAJO	BAJO	ALTO	
Degradación de los soportes de almacenamiento de la información	2	3	2	2	Critico	Medio	Medio	MEDIO	MEDIO	ALTO	
Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones	2	3	2	2	Critico	Medio	Medio	ALTO	BAJO	MEDIO	
Hacking no ético	1	3	4	1	Critico	Catastrófico	Insignificante	MEDIO	ALTO	BAJO	

Fuente: Elaboración propia.

3.6 Evaluación de las amenazas de los activos de información con los procesos de COBIT 5.

Hecha nuestras Matrices de riesgos e impactos (tabla 24 a 33), ahora se entrelaza los Activos de Información y sus amenazas en su estimación de riesgo Confidencialidad, Integridad y Disponibilidad las cuales tengan un riesgo de ocurrencia de nivel ALTO, con los procesos y sub procesos seleccionados con COBIT 5, se usa la interpretación:

- "P" significa una relación primaria (importante).
- "S" significa una relación secundaria (fuerte).

Tabla 34 Amenazas, riesgos y procesos de COBIT 5 - Equipos informáticos

Amenaza	Estimación del riesgo			APO 12						APO 13			DSS 04								DSS 05						
	Confidencialidad	Integridad	Disponibilidad	APO12.01	APO12.02	APO12.03	APO12.04	APO12.05	APO12.06	APO13.01	APO13.02	APO13.03	DSS04.01	DSS04.02	DSS04.03	DSS04.04	DSS04.05	DSS04.06	DSS04.07	DSS04.08	DSS05.01	DSS05.02	DSS05.03	DSS05.04	DSS05.05	DSS05.06	DSS05.07
A) EQUIPOS INFORMÁTICOS																											
1 - Alteración accidental de la información	ALTO	BAJO	BAJO	P			P		S	S	S	S											P	P			
2 - Destrucción de Información	MEDIO	BAJO	ALTO							S	S	S									P	S	P	P	S	S	P
3 - Abuso de privilegios de acceso	BAJO	ALTO	BAJO							S	S	S									S	S	P	P		S	
4 - Acceso no autorizado	BAJO	ALTO	BAJO							S	S	S									S		P	P			S
5 - Modificación deliberada de la información	ALTO	BAJO	BAJO	P	P		P	P	P	S	S	S									S		S	S	S		S
6 - Robo de Equipos	ALTO	BAJO	BAJO	P	S	S	P	P	P	S	S	S													P	P	P

Tabla 35 Amenazas, riesgos y procesos de COBIT 5 - Servidores

Amenaza	Estimación del riesgo			APO 12						APO 13			DSS 04								DSS 05						
	Confidencialidad	Integridad	Disponibilidad	APO12.01	APO12.02	APO12.03	APO12.04	APO12.05	APO12.06	APO13.01	APO13.02	APO13.03	DSS04.01	DSS04.02	DSS04.03	DSS04.04	DSS04.05	DSS04.06	DSS04.07	DSS04.08	DSS05.01	DSS05.02	DSS05.03	DSS05.04	DSS05.05	DSS05.06	DSS05.07
B) SERVIDORES																											
1 - Fuego	MEDIO	MEDIO	ALTO							P	P	P							P			S			P		P
2 - Tormenta eléctrica, rayo	BAJO	ALTO	MEDIO							P	P	P				S	S		P			S					P
3 - Errores de configuración	ALTO	MEDIO	BAJO		P	P	P	S	P	S	S	S						S	P				P				
4 - Alteración accidental de la información	ALTO	BAJO	BAJO		P				P						P			P			S		P				
5 - Destrucción de Información	ALTO	MEDIO	MEDIO		P				P	S		S											P	P			
6 - Fugas de Información	ALTO	BAJO	MEDIO		P				P				S	P									P	P		P	S
7 - Vulnerabilidades de los programas (software)	ALTO	ALTO	ALTO		P		P	P	P	S	S	S									P		P	P			
8 - Errores de mantenimiento / actualización de programas (software)	ALTO	BAJO	BAJO		P				P	S	S	S							P		P		P				
9 - Errores de mantenimiento / actualización de equipos (hardware)	MEDIO	ALTO	MEDIO		P				P	S	S	S										P			P	P	P
10 - Manipulación de la configuración	ALTO	MEDIO	BAJO		S		S		P														P	P			P

11 - Suplantación de la identidad del usuario	ALTO	MEDIO	MEDIO		P		P		P													S	P			
12 - Difusión de software dañino	ALTO	MEDIO	ALTO	P	P	S	P	S	P				S					S	P	S							
13 - Acceso no autorizado	MEDIO	MEDIO	ALTO																		S		P	P	P	P	P
14 - Modificación deliberada de la información	MEDIO	MEDIO	ALTO														S			S			P	P			P
15 - Denegación del servicio	ALTO	BAJO	MEDIO	P	S	P	P	S	P				P	P			P	P		P							

Tabla 36 Amenazas, riesgos y procesos de COBIT 5 - Equipos de red local

Amenaza	Estimación del riesgo			APO 12						APO 13			DSS 04								DSS 05						
	Confidencialidad	Integridad	Disponibilidad	APO12.01	APO12.02	APO12.03	APO12.04	APO12.05	APO12.06	APO13.01	APO13.02	APO13.03	DSS04.01	DSS04.02	DSS04.03	DSS04.04	DSS04.05	DSS04.06	DSS04.07	DSS04.08	DSS05.01	DSS05.02	DSS05.03	DSS05.04	DSS05.05	DSS05.06	DSS05.07
C) EQUIPOS DE RED LOCAL																											
1 - Tormenta eléctrica, rayo	ALTO	BAJO	BAJO		S	S	S	S	S	P	P	P										S			S		P
2 - Alteración accidental de la información	ALTO	MEDIO	MEDIO	P	P				P										P		P		P	P		P	P
3 - Destrucción de Información	ALTO	ALTO	MEDIO	P	P	S	P	S	P	S	S	S		S	S	S			P	S			P			P	P
4 - Fugas de Información	MEDIO	MEDIO	ALTO			S		S		S	S	S											P	P	P	P	P
5 - Errores de mantenimiento / actualización de programas (software)	BAJO	ALTO	BAJO							S		S							P		P		P	P		S	P
6 - Indisponibilidad del personal	ALTO	BAJO	BAJO										P	P	P	P	P	P		P							
7 - Suplantación de la identidad del usuario	MEDIO	ALTO	MEDIO				S		S														P				
8 - Abuso de privilegios de acceso	BAJO	MEDIO	ALTO							S		S												P	P		
9 - Difusión de software dañino	ALTO	MEDIO	ALTO		P	S	S		P																	S	P

10 - Modificación deliberada de la información	ALTO	BAJO	BAJO		P				P												P		P	P		P	
11 - Manipulación de programas	BAJO	BAJO	ALTO																				S	P		P	
12 - Denegación del servicio	MEDIO	ALTO	BAJO		P				P				P	P		P		P		P							
13 - Indisponibilidad deliberada del personal	ALTO	BAJO	ALTO	P	P			P	P				S	P	P	S	S	S	S	P							
14 - Corte del suministro eléctrico	MEDIO	BAJO	ALTO		S				S	P	P	P			P							S			S		S
15 - Instalación de software no autorizado	ALTO	ALTO	ALTO		S				S												S		P	P		P	P

Tabla 37 Amenazas, riesgos y procesos de COBIT 5 - Periféricos y pendrives

Amenaza	Estimación del riesgo			APO 12						APO 13			DSS 04								DSS 05						
	Confidencialidad	Integridad	Disponibilidad	APO12.01	APO12.02	APO12.03	APO12.04	APO12.05	APO12.06	APO13.01	APO13.02	APO13.03	DSS04.01	DSS04.02	DSS04.03	DSS04.04	DSS04.05	DSS04.06	DSS04.07	DSS04.08	DSS05.01	DSS05.02	DSS05.03	DSS05.04	DSS05.05	DSS05.06	DSS05.07
D) PERIFÉRICOS Y PENDRIVES																											
1- Error de Usuario	MEDIO	ALTO	BAJO																			P	P	S	P	S
2 - Errores del administrador	BAJO	BAJO	ALTO		S				S				S	S	S							P	P		S	S
3 - Alteración accidental de la información	BAJO	MEDIO	ALTO							S		S							P			S	S		P	P
4 - Destrucción de Información	BAJO	MEDIO	ALTO		S				S	S	S	S	P	P	P		S		P	S					P	
5 - Manipulación de la configuración	BAJO	BAJO	ALTO																			P	S		S	P
6 - Acceso no autorizado	ALTO	ALTO	MEDIO		S	S		S														P	P			P
7 - Modificación deliberada de la información	ALTO	ALTO	ALTO		S				S				S	S	S	S			P			P	P		S	P
8 - Destrucción deliberada de Información	ALTO	MEDIO	ALTO							S		S	S					P	P	S		P	S		S	P
9 - Robo de Equipos	ALTO	ALTO	ALTO							P	P	P									S			P	P	P

Tabla 38 Amenazas, riesgos y procesos de COBIT 5 - Portátiles, tablets y móviles

Amenaza	Estimación del riesgo			APO 12						APO 13			DSS 04								DSS 05						
	Confidencialidad	Integridad	Disponibilidad	APO12.01	APO12.02	APO12.03	APO12.04	APO12.05	APO12.06	APO13.01	APO13.02	APO13.03	DSS04.01	DSS04.02	DSS04.03	DSS04.04	DSS04.05	DSS04.06	DSS04.07	DSS04.08	DSS05.01	DSS05.02	DSS05.03	DSS05.04	DSS05.05	DSS05.06	DSS05.07
E) PORTÁTILES, TABLETS Y MÓVILES																											
1 - Errores del administrador	ALTO	ALTO	BAJO												P	P	P	S	S	S							
2 - Alteración accidental de la información	ALTO	ALTO	BAJO		P			P	P										P				S	S		P	P
3 - Destrucción de Información	ALTO	BAJO	BAJO	S	S	S									P				P				S	S		P	P
4 - Errores de mantenimiento / actualización de programas (software)	BAJO	ALTO	BAJO							P	P	P									P		P	S		S	P
5 - Errores de mantenimiento / actualización de equipos (hardware)	ALTO	ALTO	BAJO							P	P	P										P			P	P	P
6 - Abuso de privilegios de acceso	ALTO	BAJO	BAJO																				P	P		P	P
7 - Difusión de software dañino	MEDIO	ALTO	ALTO													P	P	P			P		S	S		S	
8 - Divulgación de la Información	BAJO	ALTO	ALTO		S	S	S		S				P	P	P	P	P										

9 - Manipulación de programas	BAJO	ALTO	MEDIO																	S		P	P		P	P
10 - Indisponibilidad deliberada del personal	ALTO	BAJO	BAJO										P	P	P	P	P	P								
11 - Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones	ALTO	BAJO	BAJO																		P			P	P	P

Tabla 39 Amenazas, riesgos y procesos de COBIT 5 - Oficinas

Amenaza	Estimación del riesgo			APO 12						APO 13			DSS 04								DSS 05						
	Confidencialidad	Integridad	Disponibilidad	APO12.01	APO12.02	APO12.03	APO12.04	APO12.05	APO12.06	APO13.01	APO13.02	APO13.03	DSS04.01	DSS04.02	DSS04.03	DSS04.04	DSS04.05	DSS04.06	DSS04.07	DSS04.08	DSS05.01	DSS05.02	DSS05.03	DSS05.04	DSS05.05	DSS05.06	DSS05.07
F) OFICINAS																											
1 - Errores de configuración	MEDIO	ALTO	ALTO														S		S		S		P	P		S	P
2 - Alteración accidental de la información	ALTO	ALTO	MEDIO		P				P										P		S		P	S			S
3 - Fugas de Información	MEDIO	BAJO	ALTO							P	P	P					S		P				P			S	P
4 - Errores de mantenimiento / actualización de equipos (hardware)	ALTO	MEDIO	ALTO							P	P	P										P			P	P	P
5 - Caída del sistema por agotamiento de recursos (interrupción en los servicios)	ALTO	MEDIO	MEDIO		P	P	P	P	P							S	S										S
6 - Indisponibilidad del personal	ALTO	BAJO	BAJO		P	P			P				S	S	S	S	S		S								
7 - Abuso de privilegios de acceso	ALTO	BAJO	ALTO		P				P														P	P		S	
8 - Acceso no autorizado	ALTO	BAJO	ALTO		S				S	S		S											P	P		P	P
9 - Modificación deliberada de la información	ALTO	ALTO	MEDIO	S	P	P			P										P				P	P		P	P

10 - Divulgación de la Información	ALTO	BAJO	MEDIO		P				P													P	S		S	P
11 - Manipulación de programas	ALTO	ALTO	BAJO		P				P													P	S		P	P
12 - Manipulación de los equipos	ALTO	ALTO	MEDIO																		P			P		P
13 - Denegación del servicio	MEDIO	BAJO	ALTO				S		S				P	P	P		P			P						
14 - Robo de Equipos	MEDIO	ALTO	ALTO				S		S										P			P			P	P	P
15 - Ejecución de ingeniería social	MEDIO	BAJO	ALTO		S				S	P	P	P					S									
16 - Degradación de los soportes de almacenamiento de la información	ALTO	ALTO	BAJO							P	P	P										P	S	S	P	S	P
17 - Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones	BAJO	ALTO	MEDIO																			P	S	S	P	P	P
18 - Hacking no ético	ALTO	ALTO	ALTO							P	P	P					S		P		P		P	P		P	P

Tabla 40 Amenazas, riesgos y procesos de COBIT 5 - Personal propio

Amenaza	Estimación del riesgo			APO 12						APO 13			DSS 04								DSS 05						
	Confidencialidad	Integridad	Disponibilidad	APO12.01	APO12.02	APO12.03	APO12.04	APO12.05	APO12.06	APO13.01	APO13.02	APO13.03	DSS04.01	DSS04.02	DSS04.03	DSS04.04	DSS04.05	DSS04.06	DSS04.07	DSS04.08	DSS05.01	DSS05.02	DSS05.03	DSS05.04	DSS05.05	DSS05.06	DSS05.07
G) PERSONAL PROPIO																											
1 - Fugas de Información	ALTO	BAJO	MEDIO		P				P	S	S	S					S		P		P		S	P		P	P
2 - Indisponibilidad del personal	ALTO	MEDIO	BAJO		P				P				S		P	P	P	P		P							
3 - Suplantación de la identidad del usuario	MEDIO	ALTO	BAJO																			S	P	S		P	P
4 - Modificación deliberada de la información	BAJO	ALTO	MEDIO																P				P	S		S	P
5 - Robo de Equipos	ALTO	ALTO	MEDIO							P	P	P										P			P		P

Tabla 41 Amenazas, riesgos y procesos de COBIT 5 - Aplicaciones informáticas

Amenaza	Estimación del riesgo			APO 12						APO 13			DSS 04								DSS 05						
	Confidencialidad	Integridad	Disponibilidad	APO12.01	APO12.02	APO12.03	APO12.04	APO12.05	APO12.06	APO13.01	APO13.02	APO13.03	DSS04.01	DSS04.02	DSS04.03	DSS04.04	DSS04.05	DSS04.06	DSS04.07	DSS04.08	DSS05.01	DSS05.02	DSS05.03	DSS05.04	DSS05.05	DSS05.06	DSS05.07
H) APLICACIONES INFORMÁTICAS																											
1 - Errores de configuración	ALTO	MEDIO	MEDIO		S	S			S	S		S							P	S						P	P
2 - Alteración accidental de la información	BAJO	ALTO	ALTO																				P	P		P	P
3 - Destrucción de Información	ALTO	MEDIO	BAJO		P	P			P										P								P
4 - Fugas de Información	ALTO	ALTO	MEDIO					S	S								S						P	P		P	P
5 - Vulnerabilidades de los programas (software)	ALTO	ALTO	MEDIO		P				P										P		P					P	P
6 - Errores de mantenimiento / actualización de programas (software)	BAJO	ALTO	MEDIO							S	S	S									P					P	P
7 - Caída del sistema por agotamiento de recursos (interrupción en los servicios)	BAJO	ALTO	ALTO							P	P	P															P
8 - Manipulación de los registros de Actividad (log)	BAJO	ALTO	BAJO							P	P	P					S		S								
9 - Manipulación de la configuración	ALTO	ALTO	BAJO	P	P				P														P	P			P

10 - Suplantación de la identidad del usuario	MEDIO	ALTO	ALTO														S						S	S		P	P
11 - Abuso de privilegios de acceso	ALTO	ALTO	BAJO		P				P														P	S		P	P
12 - Acceso no autorizado	BAJO	ALTO	ALTO																				S	P		P	P
13 - Modificación deliberada de la información	ALTO	MEDIO	MEDIO		P		P	P	P														P	S		P	P
14 - Denegación del servicio	MEDIO	MEDIO	ALTO										P	P	P	P	P	P		P							
15 - Robo de Equipos	BAJO	MEDIO	ALTO							P	P	P										P			P		P
16 - Degradación de los soportes de almacenamiento de la información	ALTO	BAJO	MEDIO	P	P				P																		P
17 - Hacking no ético	MEDIO	MEDIO	ALTO							P	P	P							P		P						P

Tabla 42 Amenazas, riesgos y procesos de COBIT 5 - Gestores de base de datos

Amenaza	Estimación del riesgo			APO 12						APO 13			DSS 04								DSS 05						
	Confidencialidad	Integridad	Disponibilidad	APO12.01	APO12.02	APO12.03	APO12.04	APO12.05	APO12.06	APO13.01	APO13.02	APO13.03	DSS04.01	DSS04.02	DSS04.03	DSS04.04	DSS04.05	DSS04.06	DSS04.07	DSS04.08	DSS05.01	DSS05.02	DSS05.03	DSS05.04	DSS05.05	DSS05.06	DSS05.07
I) GESTORES DE BASE DE DATOS																											
1 - Errores de configuración	BAJO	BAJO	ALTO														S		P		S						P
2 - Alteración accidental de la información	MEDIO	MEDIO	ALTO																P				S	S		P	P
3 - Fugas de Información	ALTO	BAJO	MEDIO		P				P														S	S	S	P	P
4 - Errores de mantenimiento / actualización de programas (software)	ALTO	MEDIO	BAJO		P				P												P			S			P
5 - Caída del sistema por agotamiento de recursos (interrupción en los servicios)	ALTO	MEDIO	BAJO							P	P	P															S
6 - Manipulación de los registros de Actividad (log)	ALTO	BAJO	BAJO							P	P	P												S			
7 - Abuso de privilegios de acceso	BAJO	ALTO	BAJO																				P	S		S	P
8 - Acceso no autorizado	BAJO	ALTO	MEDIO																				P	P		P	P
9 - Destrucción deliberada de Información	BAJO	MEDIO	ALTO				S	S		S		S					S		P					P		S	

10 - Divulgación de la Información	MEDIO	MEDIO	ALTO												P	P	P	P		P			S	S			
11 - Manipulación de programas	BAJO	MEDIO	ALTO																				P	P		P	P
12 - Robo de Equipos	ALTO	BAJO	MEDIO	S	S					P	P	P															

Tabla 43 Amenazas, riesgos y procesos de COBIT 5 - Sistemas externos

Amenaza	Estimación del riesgo			APO 12						APO 13			DSS 04								DSS 05						
	Confidencialidad	Integridad	Disponibilidad	APO12.01	APO12.02	APO12.03	APO12.04	APO12.05	APO12.06	APO13.01	APO13.02	APO13.03	DSS04.01	DSS04.02	DSS04.03	DSS04.04	DSS04.05	DSS04.06	DSS04.07	DSS04.08	DSS05.01	DSS05.02	DSS05.03	DSS05.04	DSS05.05	DSS05.06	DSS05.07
J) SISTEMAS EXTERNOS																											
1 - Error de Usuario	ALTO	MEDIO	MEDIO		P				P														S	S		P	S
2 - Fugas de Información	MEDIO	ALTO	ALTO																				S	P		P	P
3 - Vulnerabilidades de los programas (software)	ALTO	ALTO	BAJO		P											S	S				P		S	P		S	S
4 - Errores de mantenimiento / actualización de programas (software)	BAJO	MEDIO	ALTO									S	S				S	S			P			P			
5 - Caída del sistema por agotamiento de recursos (interrupción en los servicios)	BAJO	ALTO	MEDIO							P	P	P															S
6 - Suplantación de la identidad del usuario	ALTO	MEDIO	ALTO		P				P														P	P		P	P
7 - Abuso de privilegios de acceso	BAJO	MEDIO	ALTO														S						P	S		S	
8 - Divulgación de la Información	BAJO	BAJO	ALTO										P	P	S	P	P	S									
9 - Degradación de los soportes de	MEDIO	MEDIO	ALTO							S		S									S	P			P		P

almacenamiento de la información																											
10 - Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones	ALTO	BAJO	MEDIO		P	S	S	S	P										S			P			P		P
11 - Hacking no ético	MEDIO	ALTO	BAJO							P	P	P									P						P

3.7 Selección de las buenas practicas COBIT 5

Se analiza los datos obtenidos de la matriz de riesgo, con su estimación del riesgo y los procesos y sub procesos de COBIT 5, para identificar cuáles serán usados para las soluciones de las amenazas, teniendo en cuenta que "P" es una solución principal y "S" es una solución secundaria, se procede a mitigar las amenazas teniendo en cuenta la experiencia de lo laborado en la institución y los análisis previos realizados solo se usara las soluciones principales "P". A continuación se seleccionan las buenas prácticas para cada activo de información:

3.7.1 Gestionar el riesgo (APO12)

3.7.1.1 Recopilar datos

Práctica de Gestión	Entradas		Salidas	
APO12.01 Recopilar datos. Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI.	**De**	**Descripción**	**Descripción**	**A**
	EDM03.01	Evaluación de actividades de gestión de riesgos	Datos en el entorno de operación relacionados con el riesgo	Interno
	EDM03.02	• Procesos aprobados para medir la gestión de riesgos • Objetivos clave a ser monitorizados por la gestión de riesgos • Políticas de gestión de riesgos	Datos en eventos de riesgo y en factores contribuyentes	Interno
	APO02.02	Brechas y riesgos relacionados con capacidades actuales	Elementos y factores de riesgo emergentes	EDM03.01 APO01.03 APO02.02
	APO02.05	Evaluación del riesgo		
	APO10.04	Riesgo de entrega de proveedores identificado		
	DSS02.07	Estado de incidentes e informe de tendencias		

APO12.01 Actividades
1. Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con riesgo de TI, dando cabida a múltiples tipos de eventos, múltiples categorías de riesgo de TI y múltiples factores de riesgo.
2. Registrar datos relevantes sobre el entorno de operación interno y externo de la empresa que pudieran jugar un papel significativo en la gestión del riesgo de TI.
3. Medir y analizar los datos históricos de riesgo de TI y de pérdidas experimentadas tomados de datos y tendencias externas disponibles, empresas similares de la industria – basados en eventos registrados, bases de datos y acuerdos de la industria sobre divulgación de eventos comunes.
4. Registrar datos sobre eventos de riesgo que han causado o pueden causar impactos al beneficio/valor facilitado por TI, a la entrega de programas y proyectos de TI y/o a las operaciones y entrega de servicio de TI. Capturar datos relevantes sobre asuntos relacionados, incidentes, problemas e investigaciones.
5. Para clases o eventos similares, organizar los datos recogidos y destacar factores contribuyentes. Determinar los factores contribuyentes comunes para eventos múltiples.
6. Determinar las condiciones específicas que existían o faltaban cuando ocurrieron los eventos de riesgo y la forma en la cual las condiciones afectaban la frecuencia del evento y la magnitud de la pérdida.
7. Ejecutar análisis periódicos de eventos y de factores de riesgo para identificar asuntos nuevos o emergentes relacionados con el riesgo y para obtener un entendimiento de los asociados factores de riesgo internos y externos.

Ilustración 14 APO12.01 Recopilar datos - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso APO 12.01 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información EQUIPOS INFORMÁTICOS

- 1.- Alteración accidental de la información.
- 5.- Modificación deliberada de la información.
- 6.- Robo de equipos.

En el activo de información SERVIDORES

- 12.- Difusión de software dañino.
- 15.- Denegación del servicio.

En el activo de información EQUIPOS DE RED LOCAL

- 2.- Alteración accidental de la información.
- 3.- Destrucción de información.
- 13.- Indisponibilidad deliberada del personal.

En el activo de información APLICACIONES INFORMÁTICAS

- 9.- Manipulación de la configuración.
- 16.- Degradación de los soportes de almacenamiento de la información.

3.7.1.2 Analizar el riesgo.

Práctica de Gestión	Entradas		Salidas	
APO12.02 Analizar el riesgo. Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo.	**De**	**Descripción**	**Descripción**	**A**
	DSS04.02	Análisis de impacto en el negocio	Alcance de los esfuerzos de análisis de riesgos	Interno
	DSS05.01	Evaluaciones de amenazas potenciales	Escenarios de riesgo de TI	Interno
	Fuera del Ámbito de COBIT	Avisos de amenaza	Resultados de análisis de riesgos	EDM03.03 APO01.03 APO02.02 BAI01.10
Actividades				
1. Definir la amplitud y profundidad apropiadas para los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y la criticidad en el negocio de los activos. Establecer el alcance del análisis de riesgos después de llevar a cabo un análisis coste-beneficio.				
2. Construir y actualizar regularmente escenarios de riesgo de TI, que incluyan escenarios compuestos en cascada y/o tipos de amenaza coincidentes y desarrollar expectativas para actividades de control específicas, capacidades para detectar y otras medidas de respuesta.				
3. Estimar la frecuencia y magnitud de pérdida o ganancia asociada con escenarios de riesgo de TI. Tener en cuenta todos los factores de riesgo que apliquen, evaluar controles operacionales conocidos y estimar niveles de riesgo residual.				
4. Comparar el riesgo residual con la tolerancia al riesgo e identificar exposiciones que puedan requerir una respuesta al riesgo.				
5. Analizar el coste-beneficio de las opciones de respuesta al riesgo potencial, tales como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/capturar. Proponer la respuesta al riesgo óptima.				
6. Especificar requerimientos de alto nivel para los proyectos o programas que implementarán las respuestas de riesgo seleccionadas. Identificar requerimientos y expectativas para los controles clave que son apropiados para las respuestas de mitigación de riesgos.				
7. Validar los resultados de análisis de riesgos antes de usarlos para la toma de decisiones, confirmando que los análisis se alinean con requerimientos de empresa y verificando que las estimaciones fueron apropiadamente calibradas y examinadas ante una posible parcialidad.				

Ilustración 15 APO12.02 Analizar el riesgo - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso APO 12.02 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información EQUIPOS INFORMÁTICOS

- 5.- Modificación deliberada de la información.

En el activo de información SERVIDORES

- 3.- Errores de configuración.
- 4.- Alteración accidental de la información
- 5.- Destrucción de información.
- 6.- Fugas de información
- 7.- Vulnerabilidades de los programas (software)
- 8.- Errores de mantenimiento / actualización de programas (software).
- 9.- Errores de mantenimiento / actualización de programas (hardware).
- 11.- Suplantación de identidad del usuario
- 12.- Difusión de software dañino.

En el activo de información EQUIPOS DE RED LOCAL

- 2.- Alteración accidental de la información.

- 3.- Destrucción de información.
- 9.- Difusión de software dañino
- 10.- Modificación deliberada de la información.
- 12.- Denegación del servicio.
- 13.- Indisponibilidad deliberada del personal.

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 2.- Alteración accidental de la información.

En el activo de información OFICINAS

- 2.- Alteración accidental de la información.
- 5.- Caída del sistema por agotamiento de recursos (interrupción en los servicios).
- 6.- Indisponibilidad del personal.
- 7.- Abuso de privilegios de acceso.
- 9.- Modificación deliberada de la información.
- 10.- Divulgación de la información.
- 11.- Manipulación de programas.

En el activo de información PERSONAL PROPIO

- 1.- Fugas de información
- 2.- Indisponibilidad del personal

En el activo de información APLICACIONES INFORMÁTICAS

- 3.- Destrucción de información.
- 5.- Vulnerabilidades de los programas (software)
- 9.- Manipulación de la configuración.
- 11.- Abuso de privilegios de acceso.
- 13.- Modificación deliberada de la información.
- 16.- Degradación de los soportes de almacenamiento de la información.

En el activo de información GESTORES DE BASE DE DATOS

- 3.- Fugas de información
- 4.- Errores de mantenimiento / actualización de programas (software)

En el activo de información SISTEMAS EXTERNOS

- 1.- Error de usuario
- 3.- Vulnerabilidades de los programas (software)
- 6.- Suplantación de la identidad del usuario
- 11.- Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones.

3.7.1.3 Mantener un perfil de riesgo.

Práctica de Gestión	Entradas		Salidas	
APO12.03 Mantener un perfil de riesgo. Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados.	**De**	**Descripción**	**Descripción**	**A**
	EDM03.01	• Niveles aprobados de tolerancia el riesgo • Guía de apetito al riesgo	Escenarios de riesgo documentados por línea de negocio y función	Interno
	APO10.04	Riesgo de entrega de proveedores identificado	Perfil de riesgo agregado, incluyendo el estado de las acciones de gestión del riesgo	EDM03.02 APO02.02
	DSS05.01	Evaluaciones de amenazas potenciales		
Actividades				
1. Inventariar los procesos de negocio, incluyendo el personal de soporte, aplicaciones, infraestructura, instalaciones, registros manuales críticos, vendedores, proveedores y externalizados y documentar la dependencia de los procesos de gestión de servicio TI y de los recursos de infraestructuras TI.				
2. Determinar y acordar qué servicios TI y recursos de infraestructuras de TI son esenciales para sostener la operación de procesos de negocio. Analizar dependencias e identificar eslabones débiles.				
3. Agregar escenarios de riesgo actuales, por categoría, línea de negocio y área funcional.				
4. De forma regular, capturar toda la información sobre el perfil de riesgo y consolidarla dentro de un perfil de riesgo agregado.				
5. Sobre la base de todos los datos del perfil de riesgo, definir un conjunto de indicadores de riesgo que permitan la identificación rápida y la supervisión del riesgo actual y las tendencias de riesgo.				
6. Capturar información sobre eventos de riesgos de TI que se han materializado, para su inclusión en el perfil de riesgo de TI de la empresa.				
7. Capturar información sobre el estado del plan de acción del riesgo, para la inclusión en el perfil de riesgo de TI de la empresa.				

Ilustración 16 APO12.03 Mantener un perfil de riesgo - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso APO 12.03 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información SERVIDORES

- 3.- Errores de configuración.
- 15.- Denegación del servicio.

En el activo de información OFICINAS

- 5.- Caída del sistema por agotamiento de recursos (interrupción en los servicios).
- 6.- Indisponibilidad del personal.
- 9.- Modificación deliberada de la información.

En el activo de información APLICACIONES INFORMÁTICAS

- 3.- Destrucción de información.

3.7.1.4 Expresar el riesgo.

Práctica de Gestión	Entradas		Salidas	
APO12.04 Expresar el riesgo. Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada.	**De**	**Descripción**	**Descripción**	**A**
			Análisis de riesgos e informes del perfil de riesgos para las partes interesadas	EDM03.03 EDM05.02 APO10.04 MEA02.08
			Revisión de resultados de evaluaciones de riesgos de terceras partes	EDM03.03 APO10.04 MEA02.01
			Oportunidades para la aceptación de un riesgo mayor	EDM03.03
Actividades				
1. Informar de los resultados del análisis de riesgos a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones de empresa. Cuando sea posible, incluir probabilidades y rangos de pérdida o ganancia junto con niveles de confianza que permitan a la dirección equilibrar el retorno del riesgo.				
2. Proporcionar a los responsables de toma de decisiones un entendimiento de los escenarios peor y más probable, exposiciones de diligencia debida y consideraciones sobre la reputación, legales y regulatorias significativas.				
3. Informar el perfil de riesgo actual a todas las partes interesadas, incluyendo la efectividad del proceso de gestión de riesgos, la efectividad de los controles, diferencias, inconsistencias, redundancias, estado de la remediación y sus impactos en el perfil de riesgo.				
4. Revisar los resultados de evaluaciones objetivas de terceras partes, auditorías internas y revisiones del aseguramiento de la calidad y mapearlos con el perfil de riesgo. Revisar las diferencias y exposiciones identificadas para determinar la necesidad de análisis de riesgos adicionales.				
5. De forma periódica, para áreas con un riesgo relativo y una paridad de capacidad del riesgo, identificar oportunidades relacionadas con TI que podrían permitir la aceptación de un mayor riesgo y un crecimiento y retorno mayores.				

Ilustración 17 APO12.04 Expresar el riesgo - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso APO 12.04 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información EQUIPOS INFORMÁTICOS

- 1.- Alteración accidental de la información
- 5.- Modificación deliberada de la información.
- 6.- Robo de equipos.

En el activo de información SERVIDORES

- 3.- Errores de configuración.
- 7.- Vulnerabilidades de los programas (software).
- 11.- Suplantación de identidad del usuario
- 12.- Difusión de software dañino.
- 15.- Denegación del servicio.

En el activo de información EQUIPOS DE RED LOCAL

- 3.- Destrucción de información.

En el activo de información OFICINAS

- 5.- Caída del sistema por agotamiento de recursos (interrupción en los servicios).

En el activo de información APLICACIONES INFORMÁTICAS

- 13.- Modificación deliberada de la información.

3.7.1.5 Definir un portafolio de acciones para la gestión de riesgos.

Práctica de Gestión	Entradas		Salidas	
APO12.05 Definir un portafolio de acciones para la gestión de riesgos. Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.	**De**	**Descripción**	**Descripción**	**A**
			Propuestas de proyecto para reducir el riesgo	APO02.02 APO13.02
Actividades				
1. Mantener un inventario de actividades de control que estén en marcha para gestionar al riesgo y que permitan que el riesgo que se tome esté alineado con el apetito y tolerancia al riesgo. Clasificar las actividades de control y mapearlas con las declaraciones de riesgo específicas de TI y agrupaciones de riesgo de TI.				
2. Determinar si cada entidad organizativa supervisa el riesgo y acepta la responsabilidad para operar dentro de sus niveles de tolerancia individuales y de portafolio.				
3. Definir un conjunto de propuestas de proyecto equilibradas diseñadas para reducir el riesgo y/o proyectos que permitan oportunidades estratégicas empresariales, considerando costes/beneficios, el efecto en el perfil de riesgo actual y las regulaciones.				

Ilustración 18 APO12.05 Definir un portafolio de acciones para la gestión de riesgos - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso APO 12.05 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información EQUIPOS INFORMÁTICOS

- 5.- Modificación deliberada de la información.
- 6.- Robo de equipos.

En el activo de información SERVIDORES

- 7.- Vulnerabilidades de los programas (software).

En el activo de información EQUIPOS DE RED LOCAL

- 13.- Indisponibilidad deliberada del personal.

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 2.- Alteración accidental de la información.

En el activo de información OFICINAS

- 5.- Caída del sistema por agotamiento de recursos (interrupción en los servicios).

En el activo de información APLICACIONES INFORMÁTICAS

- 13.- Modificación deliberada de la información.

3.7.1.6 Responder al riesgo.

Práctica de Gestión	Entradas		Salidas	
APO12.06 Responder al riesgo. Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.	**De**	**Descripción**	**Descripción**	**A**
	EDM03.03	Acciones correctoras para tratar las desviaciones de gestión de riesgos	Planes de respuesta para incidentes relacionados con el riesgo	DSS02.05
			Comunicaciones del impacto del riesgo	APO01.04 APO08.04 DSS04.02
			Causas raíz relacionadas con el riesgo	DSS02.03 DSS03.01 DSS03.02 DSS04.02 MEA02.04 MEA02.07 MEA02.08
Actividades				
1. Preparar, mantener y probar planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente con un impacto de negocio grave. Asegurar que los planes incluyan vías de escalado a través de la empresa.				
2. Categorizar los incidentes y comparar las exposiciones reales con los umbrales de tolerancia al riesgo. Comunicar los impactos en el negocio a los responsables de toma de decisiones como parte de la notificación y actualizar el perfil de riesgo.				
3. Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes de riesgo.				
4. Examinar eventos adversos/pérdidas del pasado y oportunidades perdidas y determinar sus causas raíz. Comunicar la causa raíz, requerimientos de respuesta adicionales para el riesgo y mejoras de proceso a los responsables de toma de decisiones apropiados y asegurarse de que la causa, los requerimientos de respuesta y la mejora del proceso se incluyan en los procesos de gobierno del riesgo.				

Ilustración 19 APO12.06 Responder al riesgo - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso APO 12.06 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información EQUIPOS INFORMÁTICOS

- 5.- Modificación deliberada de la información.
- 6.- Robo de equipos

En el activo de información SERVIDORES

- 3.- Errores de configuración.
- 4.- Alteración accidental de la información
- 5.- Destrucción de información.
- 6.- Fugas de información
- 7.- Vulnerabilidades de los programas (software)
- 8.- Errores de mantenimiento / actualización de programas (software).
- 9.- Errores de mantenimiento / actualización de programas (hardware).
- 10.- Manipulación de la configuración.
- 11.- Suplantación de identidad del usuario
- 12.- Difusión de software dañino.
- 15.- Denegación del servicio.

En el activo de información EQUIPOS DE RED LOCAL

- 2.- Alteración accidental de la información.
- 3.- Destrucción de información.
- 9.- Difusión de software dañino
- 10.- Modificación deliberada de la información.
- 12.- Denegación del servicio.
- 13.- Indisponibilidad deliberada del personal.

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 2.- Alteración accidental de la información.

En el activo de información OFICINAS

- 2.- Alteración accidental de la información.
- 5.- Caída del sistema por agotamiento de recursos (interrupción en los servicios).
- 6.- Indisponibilidad del personal.
- 7.- Abuso de privilegios de acceso.
- 9.- Modificación deliberada de la información.
- 10.- Divulgación de la información.
- 11.- Manipulación de programas.

En el activo de información PERSONAL PROPIO

- 1.- Fugas de información
- 2.- Indisponibilidad del personal

En el activo de información APLICACIONES INFORMÁTICAS

- 3.- Destrucción de información.
- 5.- Vulnerabilidades de los programas (software).
- 9.- Manipulación de la configuración.
- 11.- Abuso de privilegios de acceso.
- 13.- Modificación deliberada de la información.
- 16.- Degradación de los soportes de almacenamiento de la información.

En el activo de información GESTORES DE BASE DE DATOS

- 3.- Fugas de información
- 4.- Errores de mantenimiento / actualización de programas (software)

En el activo de información SISTEMAS EXTERNOS

- 1.- Error de usuario
- 6.- Suplantación de la identidad del usuario
- 11.- Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones.

Al hacer uso del proceso, Alinear, Planificar y Organizar (APO) – 12. Gestionar el riesgo, esta responde a las metas de TI que podemos ver en el anexo 2 y además se analizó cada métrica identificada para poder hacer el uso de buenas prácticas - actividades de los sub procesos del APO 12 que nos brinda COBIT 5 para poder mitigar las estimaciones de riesgo y amenazas que fueron encontradas.

3.7.2 Gestionar la seguridad (APO13)

3.7.2.1 Establecer y mantener un SGSI.

Práctica de Gestión	Entradas		Salidas	
APO13.01 Establecer y mantener un SGSI. Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la empresa.	**De**	**Descripción**	**Descripción**	**A**
	Fuera del Ámbito de COBIT	Enfoque de seguridad de la empresa	Política de SGSI	Interno
			Declaración de alcance del SGSI	APO01.02 DSS06.03
Actividades				
1. Definir el alcance y los límites del SGSI en términos de las características de la empresa, la organización, su localización, activos y tecnología. Incluir detalles de y justificación para, cualquier exclusión del alcance.				
2. Definir un SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología.				
3. Alinear el SGSI con el enfoque global de la gestión de la seguridad en la empresa.				
4. Obtener autorización de la dirección para implementar y operar o cambiar el SGSI.				
5. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.				
6. Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información.				
7. Comunicar el enfoque de SGSI.				

Ilustración 20 APO13.01 Establecer y mantener un SGSI - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso APO 13.01 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información SERVIDORES

- 1.- Fuego.
- 2.- Tormenta eléctrica, rayo.

En el activo de información EQUIPOS DE RED LOCAL

- 1.- Tormenta eléctrica, rayo.
- 15.- Corte del suministro eléctrico.

En el activo de información PERIFÉRICOS Y PENDRIVES

- 9.- Robo de Equipos.

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 4.- Errores de mantenimiento / actualización de programas (software).
- 5.- Errores de mantenimiento / actualización de programas (hardware).

En el activo de información OFICINAS

- 3.- Fugas de información.
- 4.- Errores de mantenimiento / actualización de programas (hardware).
- 16.- Ejecución de ingeniería social.
- 17.- Degradación de los soportes de almacenamiento de la información.
- 19.- Hacking no ético.

En el activo de información PERSONAL PROPIO

- 5.- Robo de equipos.

En el activo de información APLICACIONES INFORMÁTICAS

- 7.- Caída del sistema por agotamiento de recursos (interrupción en los servicios).
- 8.- Manipulación de los registros de Actividad (log).
- 15.- Robo de equipos.
- 17.- Hacking no ético.

En el activo de información GESTORES DE BASE DE DATOS

- 5.- Caída del sistema por agotamiento de recursos (interrupción en los servicios).
- 6.- Manipulación de los registros de Actividad (log).
- 12.- Robo de equipos

En el activo de información SISTEMAS EXTERNOS

- 5.- Caída del sistema por agotamiento de recursos (interrupción en los servicios).
- 11.- Hacking no ético.

3.7.2.2 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.

Prácticas de Gestión	Entradas		Salidas	
APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información. Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio.	**De**	**Descripción**	**Descripción**	**A**
	APO02.04	Diferencias y cambios necesarios para alcanzar la capacidad objetivo	Plan de tratamiento de riesgos de seguridad de la información	Todo EDM Todo APO Todo BAI Todo DSS Todo MEA
	APO03.02	Descripciones de dominios de partida y definición de arquitectura	Casos de negocio de seguridad de información	APO02.05
	APO12.05	Propuestas de proyectos para reducir el riesgo		
Actividades				
1. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura de la empresa. Asegurar que el plan identifica las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, las responsabilidades y las prioridades asociadas para gestionar los riegos identificados de seguridad de información.				
2. Mantener un inventario de componentes de la solución implementados para gestionar los riesgos relacionados con la seguridad como parte de la arquitectura de la empresa.				
3. Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información, sustentados en casos de negocio adecuados que incluyan consideren la financiación la asignación de roles y responsabilidades.				
4. Proporcionar información para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas en base al plan de tratamiento de riesgos de seguridad de información.				
5. Definir la forma de medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizar estas mediciones para evaluar la efectividad y producir resultados reproducibles y comparables.				
6. Recomendar programas de formación y concienciación en seguridad de la información.				
7. Integrar la planificación, el diseño, la implementación y la supervisión de los procedimientos de seguridad de información y otros controles que permitan la prevención y detección temprana de eventos de seguridad, así como la respuesta a incidentes de seguridad.				

Ilustración 21 APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso APO 13.02 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información SERVIDORES

- 1.- Fuego.
- 2.- Tormenta eléctrica, rayo.

En el activo de información EQUIPOS DE RED LOCAL

- 1.- Tormenta eléctrica, rayo.
- 15.- Corte del suministro eléctrico.

En el activo de información PERIFÉRICOS Y PENDRIVES

- 9.- Robo de Equipos.

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 4.- Errores de mantenimiento / actualización de programas (software).
- 5.- Errores de mantenimiento / actualización de programas (hardware).

En el activo de información OFICINAS

- 3.- Fugas de información.
- 4.- Errores de mantenimiento / actualización de programas (hardware).
- 16.- Ejecución de ingeniería social.
- 17.- Degradación de los soportes de almacenamiento de la información.
- 19.- Hacking no ético.

En el activo de información PERSONAL PROPIO

- 5.- Robo de equipos.

En el activo de información APLICACIONES INFORMÁTICAS

- 7.- Caída del sistema por agotamiento de recursos (interrupción en los servicios).
- 8.- Manipulación de los registros de Actividad (log).
- 15.- Robo de equipos.
- 17.- Hacking no ético.

En el activo de información GESTORES DE BASE DE DATOS

- 5.- Caída del sistema por agotamiento de recursos (interrupción en los servicios).
- 6.- Manipulación de los registros de Actividad (log).
- 12.- Robo de equipos

En el activo de información SISTEMAS EXTERNOS

- 5.- Caída del sistema por agotamiento de recursos (interrupción en los servicios).
- 11.- Hacking no ético.

3.7.2.3 Supervisar y revisar el SGSI.

Prácticas de Gestión	Entradas		Salidas	
APO13.03 Supervisar y revisar el SGSI. Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua.	**De**	**Descripción**	**Descripción**	**A**
	DSS02.02	Incidentes clasificados y priorizados y requerimientos de servicios	Informes de auditoría del SGSI	MEA02.01
			Recomendaciones para mejorar el SGSI	Interno
Actividades				
1. Realizar revisiones periódicas del SGSI, incluyendo aspectos de políticas, objetivos y prácticas de seguridad del SGSI. Considerar los resultados de auditorías de seguridad, incidentes, resultados de mediciones de efectividad, sugerencias y retroalimentación de todas las partes interesadas.				
2. Realizar auditorías internas al SGSI a intervalos planificados.				
3. Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.				
4. Proporcionar información para el mantenimiento de los planes de seguridad para que consideren las incidencias de las actividades de supervisión y revisión periódica.				
5. Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.				

Ilustración 22 APO13.03 Supervisar y revisar el SGSI - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso APO 13.03 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información SERVIDORES

- 1.- Fuego.
- 2.- Tormenta eléctrica, rayo.

En el activo de información EQUIPOS DE RED LOCAL

- 1.- Tormenta eléctrica, rayo.
- 15.- Corte del suministro eléctrico.

En el activo de información PERIFÉRICOS Y PENDRIVES

- 9.- Robo de Equipos.

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 4.- Errores de mantenimiento / actualización de programas (software).
- 5.- Errores de mantenimiento / actualización de programas (hardware).

En el activo de información OFICINAS

- 3.- Fugas de información.
- 4.- Errores de mantenimiento / actualización de programas (hardware).
- 16.- Ejecución de ingeniería social.
- 17.- Degradación de los soportes de almacenamiento de la información.
- 19.- Hacking no ético.

En el activo de información PERSONAL PROPIO

- 5.- Robo de equipos.

En el activo de información APLICACIONES INFORMÁTICAS

- 7.- Caída del sistema por agotamiento de recursos (interrupción en los servicios).
- 8.- Manipulación de los registros de Actividad (log).
- 15.- Robo de equipos.
- 17.- Hacking no ético.

En el activo de información GESTORES DE BASE DE DATOS

- 5.- Caída del sistema por agotamiento de recursos (interrupción en los servicios).
- 6.- Manipulación de los registros de Actividad (log).
- 12.- Robo de equipos

En el activo de información SISTEMAS EXTERNOS

- 5.- Caída del sistema por agotamiento de recursos (interrupción en los servicios).
- 11.- Hacking no ético.

Al hacer uso del proceso, Alinear, Planificar y Organizar (APO) – 13. Gestionar la seguridad, esta responde a las metas de TI que podemos ver en el anexo 3 y además se analizó cada métrica identificada para poder hacer el uso de buenas prácticas - actividades de los sub procesos del APO 13 que nos brinda COBIT 5 para poder mitigar las estimaciones de riesgo y amenazas que fueron encontradas.

3.7.3 Gestionar la continuidad (DSS04)

3.7.3.1 Definir la política de continuidad de negocios, objetivos y alcance.

Práctica de Gestión	Entradas		Salidas	
DSS04.01 Definir la política de continuidad de negocio, objetivos y alcance. Definir la política y alcance de continuidad de negocio alineada con los objetivos de negocio y de las partes interesadas.	**De**	**Descripción**	**Descripción**	**A**
	AP009.03	ANSs	Política y objetivos de continuidad de negocio	AP001.04
			Escenarios de incidentes que causan una interrupción	Interno
			Valoraciones de las capacidades actuales y lagunas de continuidad	Interno
Actividades				
1. Identificar procesos de negocio internos y subcontratados y actividades de servicio que son críticas para las operaciones de la empresa o necesarias para cumplir con las obligaciones legales y/o contractuales.				
2. Identificar las partes interesadas clave y los roles y responsabilidades para definir y acordar la política de continuidad y su alcance.				
3. Definir y documentar los objetivos y el alcance mínimos acordados de la política de continuidad del negocio e imbricar la planificación de continuidad en la cultura empresarial.				
4. Identificar procesos de soporte al negocio esenciales y servicios TI relacionados.				

Ilustración 23 DSS04.01 Definir la política de continuidad de negocio, objetivos y alcance - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso DSS 04.01 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información SERVIDORES

- 15.- Denegación del servicio.

En el activo de información EQUIPOS DE RED LOCAL

- 6.- Indisponibilidad del personal.
- 12.- Denegación del servicio.

En el activo de información PERIFÉRICOS Y PENDRIVES

- 4.- Destrucción de la información.

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 8.- Divulgación de la información.
- 10.- Indisponibilidad deliberada del personal.

En el activo de información OFICINAS

- 13.- Denegación del servicio.

En el activo de información APLICACIONES INFORMÁTICAS

- 14.- Denegación del servicio.

En el activo de información SISTEMAS EXTERNOS

- 8.- Divulgación de la información.

3.7.3.2 Mantener una estrategia de continuidad.

Prácticas de Gestión	Entradas		Salidas	
DSS04.02 Mantener una estrategia de continuidad. Evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción.	**De**	**Descripción**	**Descripción**	**A**
	AP012.06	• Causas raíz relacionadas con riesgos • Comunicaciones del impacto de los riesgos	Análisis de impacto en el negocio	AP012.02
			Requerimientos de continuidad	Interno
			Opciones estratégicas aprobadas	AP002.05
Actividades				
1. Identificar escenarios potenciales probables que puedan dar pie a eventos que puedan causar incidentes disruptivos importantes.				
2. Realizar un análisis de impacto en el negocio para evaluar el impacto en tiempo de una disrupción en funciones críticas del negocio y el efecto que tendría en ellas.				
3. Establecer el tiempo mínimo necesario para recuperar un proceso de negocio y su soporte de TI, basándose en una duración aceptable de interrupción del negocio y la interrupción máxima tolerable.				
4. Analizar la probabilidad de amenazas que puedan causar pérdidas de continuidad de negocio e identificar medidas que puedan reducir la probabilidad y el impacto, mejorando la prevención e incrementando la resiliencia.				
5. Analizar los requerimientos de continuidad para identificar las posibles estrategias de negocio y opciones técnicas.				
6. Determinar las condiciones y los responsables de decisiones clave que puedan causar la invocación de los planes de continuidad.				
7. Identificar los requerimientos de recursos y costes para cada opción técnica estratégica y realizar recomendaciones estratégicas.				
8. Obtener la aprobación de los ejecutivos de negocio para las opciones estratégicas seleccionadas.				

Ilustración 24 DSS04.02 Mantener una estrategia la continuidad - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso DSS 04.02 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información SERVIDORES

- 6.- Fugas de información.
- 15.- Denegación del servicio.

En el activo de información EQUIPOS DE RED LOCAL

- 6.- Indisponibilidad del personal.
- 12.- Denegación del servicio.
- 13.- Indisponibilidad deliberada del personal.

En el activo de información PERIFÉRICOS Y PENDRIVES

- 4.- Destrucción de la información.

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 8.- Divulgación de la información.
- 10.- Indisponibilidad deliberada del personal.

En el activo de información OFICINAS

- 13.- Denegación del servicio.

En el activo de información APLICACIONES INFORMÁTICAS

- 14.- Denegación del servicio.

En el activo de información SISTEMAS EXTERNOS

- 8.- Divulgación de la información.

3.7.3.3 Desarrollar e implementar una respuesta a la continuidad del negocio.

Prácticas de Gestión	Entradas		Salidas	
DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio. Desarrollar un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para facilitar que la empresa continúe con sus actividades críticas	**De**	**Descripción**	**Descripción**	**A**
	AP009.03	Acuerdos de Nivel Operativo (OLAs)	Acciones y comunicaciones de respuesta a incidentes	DSS02.01
			Plan de Continuidad de Negocio (BCP)	Interno
Actividades				
1. Definir las acciones y comunicaciones de respuesta a incidentes que deben ser realizadas en un evento de disrupción. Definir los roles y responsabilidades relacionados, incluyendo la responsabilidad para la política y la implementación.				
2. Desarrollar y mantener planes de continuidad de negocio operativos que contengan los procedimientos que deben ser seguidos para permitir continuar operando los procesos críticos de negocio y/o planes temporales de proceso, incluyendo enlaces a los planes de proveedores de servicio externalizados.				
3. Asegurar que los proveedores y socios externos clave tengan implantados planes de continuidad efectivos. Obtener evidencias auditadas si es necesario.				
4. Definir las condiciones y procedimientos de recuperación que permitan la reanudación de los procesos de negocio, incluyendo la actualización y conciliación de las bases de datos para preservar la integridad de la información.				
5. Definir y documentar los recursos necesarios para soportar los procedimientos de continuidad y recuperación, considerando personas, instalaciones e infraestructura de TI.				
6. Definir y documentar los requerimientos de información de respaldo para soportar los planes, incluyendo planes y documentos en papel así como ficheros de datos y considerar las necesidades de seguridad y almacenamiento en otra ubicación.				
7. Determinar las habilidades necesarios para los individuos implicados en la ejecución de los planes y procedimientos.				
8. Distribuir los planes y la documentación de soporte de modo seguro a las partes interesadas y apropiadamente autorizadas y asegurar que estén accesibles en escenarios de desastre.				

Ilustración 25 DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso DSS 04.03 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información SERVIDORES

- 4.- Alteración accidental de la información.

En el activo de información EQUIPOS DE RED LOCAL

- 6.- Indisponibilidad del personal.
- 13.- Indisponibilidad deliberada del personal.
- 14.- Corte del suministro eléctrico.

En el activo de información PERIFÉRICOS Y PENDRIVES

- 4.- Destrucción de la información.

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 1.- Errores del administrador
- 3.- Destrucción de información.
- 8.- Divulgación de la información.
- 10.- Indisponibilidad deliberada del personal.

En el activo de información OFICINAS

- 13.- Denegación del servicio.

En el activo de información PERSONAL PROPIO

- 2.- Indisponibilidad del personal.

En el activo de información APLICACIONES INFORMÁTICAS

- 14.- Denegación del servicio.

En el activo de información GESTORES DE BASE DE DATOS

- 10.- Divulgación de la información.

3.7.3.4 Ejercitar, probar y revisar el BCP (Business Complementin Planning)

Prácticas de Gestión	Entradas		Salidas	
DSS04.04 Ejercitar, probar y revisar el BCP. Probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera.	**De**	**Descripción**	**Descripción**	**A**
			Pruebas de objetivos	Interno
			Pruebas de ejercicios	Interno
			Pruebas de resultados y recomendaciones	Interno
Actividades				
1. Definir los objetivos para ejercitar y probar los sistemas del plan (de negocio, técnicos, logísticos, administrativos, procedimentales y operacionales) para verificar la completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de negocio.				
2. Definir y acordar ejercicios que sean razonables con las partes interesadas, validar los procedimientos de continuidad, e incluir roles y responsabilidades y acuerdos de retención de datos que ocasionen la mínima disrupción en los procesos de negocio.				
3. Asignar roles y responsabilidades para realizar ejercicios y pruebas del plan de continuidad.				
4. Planificar ejercicios y actividades de prueba tal como esté definido en el plan de continuidad.				
5. Realizar un análisis y revisión post-ejercicio para considerar el logro.				
6. Desarrollar recomendaciones para mejorar el plan de continuidad actual en base a los resultados de la revisión.				

Ilustración 26 DSS04.04 Ejercitar, probar y revisar el BCP - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso DSS 04.04 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información EQUIPOS DE RED LOCAL

- 6.- Indisponibilidad del personal.
- 12.- Denegación del servicio.

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 1.- Errores del administrador.
- 7.- Difusión de software dañino.
- 8.- Divulgación de la información.
- 10.- Indisponibilidad deliberada del personal.

En el activo de información PERSONAL PROPIO

- 2.- Indisponibilidad del personal.

En el activo de información APLICACIONES INFORMÁTICAS

- 14.- Denegación del servicio.

En el activo de información GESTORES DE BASE DE DATOS

- 10.- Divulgación de la información.

En el activo de información SISTEMAS EXTERNOS

- 8.- Divulgación de la información

3.7.3.5 Revisar, mantener y mejorar el plan de continuidad

Prácticas de Gestión	Entradas		Salidas	
DSS04.05 Revisar, mantener y mejorar el plan de continuidad. Realizar una revisión por la Dirección de la capacidad de continuidad a intervalos regulares para asegurar su continua idoneidad, adecuación y efectividad. Gestionar los cambios en el plan de acuerdo al proceso de control de cambios para asegurar que el plan de continuidad se mantiene actualizado y refleja continuamente los requerimientos actuales del negocio.	**De**	**Descripción**	**Descripción**	**A**
			Resultados de las revisiones de los planes	Interno
			Cambios recomendados a los planes	Interno
Actividades				
1. Revisar el plan y la capacidad de continuidad de forma regular frente a las asunciones hechas y los objetivos de negocio actuales, tanto estratégicos como operativos.				
2. Considerar si es necesario una revisión del análisis de impacto en el negocio, dependiendo en la naturaleza de los cambios.				
3. Recomendar y comunicar los cambios en la política, planes, procedimientos, infraestructura, roles y responsabilidades para la aprobación de la dirección y su realización mediante el proceso de gestión de cambios.				
4. Revisar el plan de continuidad regularmente para considerar el impacto de cambios nuevos o mayores en: organización de la empresa, procesos de negocio, acuerdos de externalización, tecnologías, infraestructura, sistemas operativos y sistemas de aplicaciones.				

Ilustración 27 DSS04.05 Revisar, mantener y mejorar el plan de continuidad - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso DSS 04.05 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información SERVIDORES

- 15.- Denegación del servicio

En el activo de información EQUIPOS DE RED LOCAL

- 6.- Indisponibilidad del personal.

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 1.- Errores del administrador.
- 7.- Difusión de software dañino.
- 8.- Divulgación de la información.
- 10.- Indisponibilidad deliberada del personal.

En el activo de información OFICINAS

- 13.- Denegación del servicio.

En el activo de información PERSONAL PROPIO

- 2.- Indisponibilidad del personal.

En el activo de información APLICACIONES INFORMÁTICAS

- 14.- Denegación del servicio.

En el activo de información GESTORES DE BASE DE DATOS

- 10.- Divulgación de la información.

En el activo de información SISTEMAS EXTERNOS

- 8.- Divulgación de la información

3.7.3.6 Proporcionar formación en el plan de continuidad.

Prácticas de Gestión	Entradas		Salidas	
DSS04.06 Proporcionar formación en el plan de continuidad. Proporcionar a todas las partes implicadas, internas y externas, de sesiones formativas regulares que contemplen los procedimientos y sus roles y responsabilidades en caso de disrupción.	**De**	**Descripción**	**Descripción**	**A**
	RR.HH.	Lista del personal que requiere formación	Requerimientos de formación	APO07.03
			Resultados de la supervisión de habilidades y competencias	APO07.03
Actividades				
1. Definir y mantener los planes y requerimientos de formación para quienes realicen de manera continuada planificación de la continuidad, análisis de impacto, evaluaciones de riesgos, comunicación con los medios y respuesta a incidentes. Asegurar que los planes de formación consideren la frecuencia de formación y los mecanismos de entrega de la formación.				
2. Desarrollar competencias basadas en formación práctica que incluyan la participación en ejercicios y pruebas.				
3. Supervisar habilidades y competencias basándose en los resultados de los ejercicios y las pruebas.				

Ilustración 28 DSS04.06 Proporcionar formación en el plan de continuidad - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso DSS 04.06 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información SERVIDORES

- 4.- Alteración accidental de la información.
- 15.- Denegación del servicio.

En el activo de información EQUIPOS DE RED LOCAL

- 6.- Indisponibilidad del personal.
- 12.- Denegación del servicio.

En el activo de información PERIFÉRICOS Y PENDRIVES

- 8.- Destrucción deliberada de información

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 7.- Difusión de software dañino.
- 10.- Indisponibilidad deliberada del personal.

En el activo de información PERSONAL PROPIO

- 2.- Indisponibilidad del personal.

En el activo de información APLICACIONES INFORMÁTICAS

- 14.- Denegación del servicio.

En el activo de información GESTORES DE BASE DE DATOS

- 10.- Divulgación de la información.

3.7.3.7 Gestionar acuerdos de respaldo.

Prácticas de Gestión	Entradas		Salidas	
DSS04.07 Gestionar acuerdos de respaldo. Mantener la disponibilidad de la información crítica del negocio.	**De**	**Descripción**	**Descripción**	**A**
			Probar los resultados de las copias de seguridad de los datos	Interno
Actividades				
1. Hacer copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo a una planificación definida, considerando: • Frecuencia (mensual, semanal, diaria, etc.) • Modo de copias de seguridad (por ejemplo, discos espejo para copias de seguridad en tiempo real frente a DVD-ROM para retenciones de larga duración) • Tipo de copias de seguridad (por ejemplo, completa frente a incremental) • Tipo se soporte • Copias de seguridad automatizadas en línea • Tipos de datos (por ejemplo, voz, óptica) • Creación de registros • Datos de cálculos críticos de usuario final (por ejemplo, hojas de cálculo) • Localización física y lógica de las fuentes de los datos • Seguridad y derechos de acceso • Cifrado				
2. Asegurar que los sistemas, aplicaciones, datos y documentación mantenidos o procesados por terceras partes están adecuadamente respaldados o asegurados de otra forma. Considerar el hecho de requerir el retorno de las copias de seguridad de terceras partes. Considerar acuerdos de depósito (escrow).				
3. Definir los requerimientos del almacenamiento de las copias de seguridad, dentro y fuera de la propia ubicación, que satisfagan los requerimientos del negocio. Considerar la accesibilidad requerida a las copias de seguridad.				
4. Extender la concienciación y la formación en Planes de Continuidad de Negocio (BCP).				
5. Probar y mantener legibles las copias de seguridad y las archivadas periódicamente.				

Ilustración 29 DSS04.07 Gestionar acuerdos de respaldo - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso DSS 04.07 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información SERVIDORES

- 1.- Fuego
- 2.- Tormenta eléctrica, rayo
- 3.- Errores de configuración
- 8.- Errores de mantenimiento / actualización de programas (software)
- 12.- Difusión de software dañino

En el activo de información EQUIPOS DE RED LOCAL

- 2.- Alteración accidental de la información
- 3.- Destrucción de la información
- 5.- Errores de mantenimiento / actualización de programas (software)

En el activo de información PERIFÉRICOS Y PENDRIVES

- 3.- Alteración accidental de la información.
- 4.- Destrucción deliberada de información.
- 7.- Modificación deliberada de la información.
- 8.- Destrucción deliberada de la información.

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 2.- Alteración accidental de la información.
- 3.- Destrucción de información.

En el activo de información OFICINAS

- 2.- Alteración accidental de la información.
- 3.- Fugas de información
- 9.- Modificación deliberada de la información
- 14.- Robo de equipos
- 19.- Hacking no ético

En el activo de información PERSONAL PROPIO

- 1.- Fugas de información.
- 4.- Modificación deliberada de la información.

En el activo de información APLICACIONES INFORMÁTICAS

- 1.- Errores de configuración
- 3.- Destrucción de información
- 5.- Vulnerabilidades de los programas (software)
- 17.- Hacking no ético

En el activo de información GESTORES DE BASE DE DATOS

- 1.- Errores de configuración.
- 2.- Alteración accidental de la información.
- 9.- Destrucción deliberada de la información.

3.7.3.8 Ejecutar revisiones post-reanudación.

Prácticas de Gestión	Entradas		Salidas	
DSS04.08 Ejectuar revisiones post-reanudación. Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.	**De**	**Descripción**	**Descripción**	**A**
			Informe de revisión post-reanudación	Interno
			Cambios aprobados a los planes	BAI06.01
Actividades				
1. Evaluar la observancia del Plan de Continuidad de Negocio (BCP) documentado.				
2. Determinar la efectividad del plan, capacidades de continuidad, roles y responsabilidades, habilidades y competencias, resiliencia a incidentes, infraestructura técnica y estructuras organizativas y relaciones.				
3. Identificar debilidades u omisiones en el plan y las capacidades y hacer recomendaciones para la mejora.				
4. Obtener la aprobación de la dirección para los cambios en el plan y aplicarlos mediante el proceso de control de cambios de la empresa.				

Ilustración 30 DSS04.08 Ejecutar revisiones post reanudación - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso DSS 04.08 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información SERVIDORES

- 15.- Denegación del servicio.

En el activo de información EQUIPOS DE RED LOCAL

- 6.- Indisponibilidad del personal.
- 12.- Denegación del servicio.
- 13.- Indisponibilidad deliberada del personal

En el activo de información OFICINAS

- 13.- Denegación del servicio

En el activo de información PERSONAL PROPIO

- 2.- Indisponibilidad del personal.

En el activo de información APLICACIONES INFORMÁTICAS

- 14.- Denegación del servicio.

En el activo de información GESTORES DE BASE DE DATOS

- 10.- Divulgación de la información.

Al hacer uso del proceso, Alinear, Planificar y Organizar (APO) – 13. Gestionar la seguridad, esta responde a las metas de TI que podemos ver en el anexo 4 y además se analizó cada métrica identificada para poder hacer el uso de buenas prácticas - actividades de los sub procesos del APO 13 que nos brinda COBIT 5 para poder mitigar las estimaciones de riesgo y amenazas que fueron encontradas.

3.7.4 Gestionar los servicios de seguridad (DSS05)

3.7.4.1 Proteger contra software malicioso (malware).

Prácticas de Gestión	Entradas		Salidas	
DSS05.01 Proteger contra software malicioso (*malware*). 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).	**De**	**Descripción**	**Descripción**	**A**
			Política de prevención de software malicioso	AP001.04
			Evaluaciones de amenazas potenciales	AP012.02 AP012.03
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 phishing).				
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.				

Ilustración 31 DSS05.01 Proteger contra software malicioso (software) - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso DSS 05.01 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información EQUIPOS INFORMÁTICOS

- 2.- Destrucción de información.

En el activo de información SERVIDORES

- 7.- Vulnerabilidades de los programas (software).
- 8.- Errores de mantenimiento / actualización de programas (software).

En el activo de información EQUIPOS DE RED LOCAL

- 2.- Alteración accidental de la información.
- 5.- Errores de mantenimiento / actualización de programas (software).
- 10.- Modificación deliberada de la información.

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 4.- Errores de mantenimiento / actualización de programas (software).
- 7.- Difusión de software dañino

En el activo de información OFICINAS

- 19.- Hacking no ético

En el activo de información PERSONAL PROPIO

- 1.- Fugas de información.

En el activo de información APLICACIONES INFORMÁTICAS

- 5.- Vulnerabilidades de los programas (software)
- 7.- Errores de mantenimiento / actualización de programas (software).
- 17.- Hacking no ético.

En el activo de información GESTORES DE BASE DE DATOS

- 4.- Errores de mantenimiento / actualización de programas (software).

En el activo de información SISTEMAS EXTERNOS

- 3.- Vulnerabilidades de los programas (software).
- 4.- Errores de mantenimiento / actualización de programas (software).
- 12.- Hacking no ético.

3.7.4.2 Gestionar la seguridad de la red y conexiones.

Prácticas de Gestión	Entradas		Salidas	
DSS05.02 Gestionar la seguridad de la red y las conexiones. Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.	**De**	**Descripción**	**Descripción**	**A**
	APO01.06	Guías de clasificación de la información	Política de seguridad en la conectividad	APO01.04
	APO09.03	ANSs	Resultados de las pruebas de intrusión	MEA02.08
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.				
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 los equipamientos de red de forma segura.				
7. Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura 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.				

Ilustración 32 DSS05.02 Gestionar la seguridad de la red y las conexiones - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso DSS 05.02 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información SERVIDORES

- 9.- Errores de mantenimiento / actualización de programas (software).

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 5.- Errores de mantenimiento / actualización de programas (software).
- 11.- Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones.

En el activo de información OFICINAS

- 3.- Errores de mantenimiento / actualización de programas (software).
- 12.- Manipulación de los equipos
- 14.- Robo de equipos
- 17.- Degradación de los soportes de almacenamiento de la información
- 18.- Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones.

En el activo de información PERSONAL PROPIO

- 5.- Robo de equipos

En el activo de información APLICACIONES INFORMÁTICAS

- 15.- Robo de equipos.

En el activo de información SISTEMAS EXTERNOS

- 10.- Degradación de los soportes de almacenamiento de la información.
- 11.- Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones.

3.7.4.3 Gestionar la seguridad de los puestos de usuario final.

Prácticas de Gestión	Entradas		Salidas	
DSS05.03 Gestionar la seguridad de los puestos de usuario final. 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.	**De**	**Descripción**	**Descripción**	**A**
	APO03.02	Modelo de arquitectura de la información	Políticas de seguridad para dispositivos de usuario final	APO01.04
	APO09.03	• Acuerdos de Nivel de Servicio (ANSs) • Acuerdos de Nivel Operativo (OLAs)		
	BAI09.01	Resultados de pruebas de inventarios físicos		
	DSS06.06	Informes de violaciones		
Actividades				
1. Configurar los sistemas operativos de forma segura.				
2. Implementar mecanismos de bloqueo de los dispositivos.				
3. Cifrar la información almacenada de acuerdo a 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.				

Ilustración 33 DSS05.03 Gestionar la seguridad de los puestos de usuario final - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso DSS 05.03 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información EQUIPOS INFORMÁTICOS

- 1.- Alteración accidental de la información
- 2.- Destrucción de información.
- 3.- Abuso de privilegios de acceso
- 4.- Acceso no autorizado

En el activo de información SERVIDORES

- 3.- Errores de configuración.
- 4.- Alteración accidental de la información
- 5.- Destrucción de información
- 6.- Fugas de información
- 7.- Vulnerabilidades de los programas (software).
- 8.- Errores de mantenimiento / actualización de programas (software).
- 10.- Manipulación de configuración
- 13.- Acceso no autorizado
- 14.- Modificación deliberada de la información.

En el activo de información EQUIPOS DE RED LOCAL

- 2.- Alteración accidental de la información.
- 3.- Destrucción de información
- 4.- Fugas de información
- 5.- Errores de mantenimiento / actualización de programas (software).
- 7.- Suplantación de la identidad del usuario
- 10.- Modificación deliberada de la información.
- 16.- Instalación de software no autorizado

En el activo de información PERIFÉRICOS Y PENDRIVES

- 1.- Error de usuario
- 2.- Errores del administrador
- 5.- Manipulación de configuración
- 6.- Acceso no autorizado
- 7.- Modificación deliberada de la información
- 8.- Destrucción deliberada de información

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 4.- Errores de mantenimiento / actualización de programas (software).
- 6.- Abuso de privilegios de acceso
- 9.- Manipulación de programas

En el activo de información OFICINAS

- 1.- Errores de configuración
- 2.- Alteración accidental de la información
- 3.- Fugas de información
- 7.- Abuso de privilegios de acceso
- 8.- Acceso no autorizado
- 9.- Modificación deliberada de la información
- 10.- Divulgación de la información
- 11.- Manipulación de programas
- 19.- Hacking no ético

En el activo de información PERSONAL PROPIO

- 3.- Suplantación de identidad del usuario.
- 4.- Modificación deliberada de la información.

En el activo de información APLICACIONES INFORMÁTICAS

- 2.- Alteración accidental de la información
- 4.- Fugas de información
- 9.- Manipulación de la configuración
- 11.- Abuso de privilegios de acceso
- 13.- Modificación deliberada de la información.

En el activo de información GESTORES DE BASE DE DATOS

- 7.- Abuso de privilegios de acceso
- 8.- Acceso no autorizados
- 11.- Manipulación de programas

En el activo de información SISTEMAS EXTERNOS

- 6.- Suplantación de la identidad del usuario
- 7.- Abuso de privilegios de acceso

3.7.4.4 Gestionar la identidad del usuario y el acceso lógico.

Prácticas de Gestión	Entradas		Salidas	
DSS05.04 Gestionar la identidad del usuario y el acceso lógico. 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.	**De**	**Descripción**	**Descripción**	**A**
	AP001.02	Definición de roles y responsabilidades relacionadas con TI	Derechos de acceso de los usuarios aprobados	Interno
	AP003.02	Modelo de arquitectura de la información	Resultados de las revisiones de cuentas y privilegios de los usuarios	Interno
Actividades				
1. Mantener los derechos de acceso de los usuarios 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 por roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos consistentemente, incluyendo roles 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 derechos de acceso (creación, modificación y 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 usuario privilegiadas.				
6. Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.				
7. Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información por usuario.				
8. Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible.				

Ilustración 34 DSS05.04 Gestionar la identidad del usuario y el acceso lógico - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso DSS 05.04 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información EQUIPOS INFORMÁTICOS

- 1.- Alteración accidental de la información
- 2.- Destrucción de información.
- 3.- Abuso de privilegios de acceso
- 4.- Acceso no autorizado

En el activo de información SERVIDORES

- 5.- Destrucción de información
- 6.- Fugas de información
- 7.- Vulnerabilidades de los programas (software).
- 10.- Manipulación de configuración
- 11.- Suplantación de la identidad del usuario.
- 13.- Acceso no autorizado
- 14.- Modificación deliberada de la información.

En el activo de información EQUIPOS DE RED LOCAL

- 2.- Alteración accidental de la información.
- 4.- Fugas de información
- 5.- Errores de mantenimiento / actualización de programas (software).
- 8.- Abuso de privilegios de acceso
- 10.- Modificación deliberada de la información.
- 11.- Manipulación de programas.
- 16.-Instalación de software no autorizado

En el activo de información PERIFÉRICOS Y PENDRIVES

- 1.- Error de usuario
- 2.- Errores del administrador
- 6.- Acceso no autorizado
- 7.- Modificación deliberada de la información

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 6.- Abuso de privilegios de acceso
- 9.- Manipulación de programas

En el activo de información OFICINAS

- 1.- Errores de configuración
- 7.- Abuso de privilegios de acceso
- 8.- Acceso no autorizado
- 9.- Modificación deliberada de la información
- 19.- Hacking no ético

En el activo de información PERSONAL PROPIO

- 1.- Fugas de información

En el activo de información APLICACIONES INFORMÁTICAS

- 2.- Alteración accidental de la información
- 4.- Fugas de información
- 9.- Manipulación de la configuración
- 12.- Acceso no autorizado

En el activo de información GESTORES DE BASE DE DATOS

- 8.- Acceso no autorizado
- 9.- Destrucción deliberada de información.
- 11.- Manipulación de programas

En el activo de información SISTEMAS EXTERNOS

- 2.- Fugas de información
- 3.- Vulnerabilidades de los programas (software)
- 4.- Errores de mantenimiento / actualización de programas (software)
- 6.- Suplantación de la identidad del usuario

3.7.4.5 Gestionar el acceso físico a los activos de TI.

Prácticas de Gestión	Entradas		Salidas	
DSS05.05 Gestionar el acceso físico a los activos de TI. Definir e implementar procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con 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.	**De**	**Descripción**	**Descripción**	**A**
			Peticiones de acceso aprobadas	Interno
			Registros de acceso	DSS06.03
Actividades				
1. Gestionar las peticiones y concesiones 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 concedido.				
2. Asegurar que los perfiles de acceso 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 las ubicaciones de TI. Registrar 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 estén 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.				
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 alama 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.				

Ilustración 35 DSS05.05 Gestionar el acceso físico a los activos de TI - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso DSS 05.05 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información EQUIPOS INFORMÁTICOS

- 6.- Robo de equipos

En el activo de información SERVIDORES

- 1.- Fuego
- 9.- Errores de mantenimiento / actualización de programas (hardware).
- 13.- Acceso no autorizado

En el activo de información EQUIPOS DE RED LOCAL

- 4.- Fugas de información
- 8.- Abuso de privilegios de acceso

En el activo de información PERIFÉRICOS Y PENDRIVES

- 9.- Robo de equipos.

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 5.- Errores de mantenimiento / actualización de programas (hardware).
- 11.- Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones

En el activo de información OFICINAS

- 4.- Errores de mantenimiento / actualización de programas (hardware).
- 12.- Manipulación de equipos
- 14.- Robo de equipos
- 17.- Degradación de los soportes de almacenamiento de la información.
- 18.- Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones

En el activo de información PERSONAL PROPIO

- 5.- Robo de equipos

En el activo de información APLICACIONES INFORMÁTICAS

- 15.- Robo de equipos

En el activo de información SISTEMAS EXTERNOS

- 10.- Degradación de los soportes de almacenamiento de la información.
- 11.- Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones

3.7.4.6 Gestionar documentos sensibles y dispositivos de salida.

Prácticas de Gestión	Entradas		Salidas	
DSS05.06 Gestionar documentos sensibles y dispositivos de salida. 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.	**De**	**Descripción**	**Descripción**	**A**
	AP003.02	Modelo de arquitectura de la información	Inventario de documentos y dispositivos sensibles	Interno
			Privilegios de acceso	Interno
Actividades				
1. Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida, dentro, en y fuera de la empresa.				
2. Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basados en el principio del menor privilegio, equilibrando riesgo y requerimientos 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, desmagnetizando soportes magnéticos, destruir físicamente dispositivos de memoria, poniendo trituradoras o papeleras cerradas disponibles para destruir formularios especiales y otros documentos confidenciales).				

Ilustración 36 DSS05.06 Gestionar documentos sensibles y dispositivos de salida - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso DSS 05.06 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información EQUIPOS INFORMÁTICOS

- 6.- Robo de equipos

En el activo de información SERVIDORES

- 6.- Fugas de información
- 9.- Errores de mantenimiento / actualización de programas (hardware).
- 13.- Acceso no autorizado

En el activo de información EQUIPOS DE RED LOCAL

- 2.- Alteración accidental de la información
- 3.- Destrucción de información
- 4.- Fugas de información
- 10.- Modificación deliberada de la información
- 11.- Manipulación de programas
- 16.- Instalación de software no autorizado

En el activo de información PERIFÉRICOS Y PENDRIVES

- 1.- Error de usuario
- 3.- Alteración accidental de la información
- 4.- Destrucción de información
- 9.- Robo de equipos.

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 2.- Alteración accidental de la información
- 3.- Destrucción de información
- 5.- Errores de mantenimiento / actualización de programas (hardware).
- 6.- Abuso de privilegios de acceso
- 9.- Manipulación de programas
- 11.- Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones

En el activo de información OFICINAS

- 4.- Errores de mantenimiento / actualización de programas (hardware).
- 8.- Acceso no autorizado
- 9.- Modificación deliberada de la información
- 11.- Manipulación de programas
- 14.- Robo de equipos
- 18.- Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones
- 19.- Hacking no ético

En el activo de información PERSONAL PROPIO

- 1.- Fugas de información
- 3.- Suplantación de identidad del usuario

En el activo de información APLICACIONES INFORMÁTICAS

- 1.- Errores de configuración
- 2.- Alteración accidental de la información
- 4.- Fugas de información
- 5.- Vulnerabilidad de los programas (software)
- 6.- Errores de mantenimiento / actualización de programas (software).
- 10.- Suplantación de la identidad del usuario
- 11.- Abuso de privilegios de acceso
- 12.- Acceso no autorizado
- 13.- Modificación deliberada de la información

En el activo de información GESTORES DE BASE DE DATOS

- 2.- Alteración accidental de la información
- 3.- Fugas de información
- 8.- Acceso no autorizado
- 11.- Manipulación de programas

En el activo de información SISTEMAS EXTERNOS

- 1.- Error de usuario
- 2.- Fugas de información
- 6.- Suplantación de la identidad del usuario

3.7.4.7 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.

Prácticas de Gestión	Entradas		Salidas	
DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad. 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.	**De**	**Descripción**	**Descripción**	**A**
			Registros de incidentes de seguridad	Interno
			Características de incidentes de seguridad	Interno
			Tiques de incidentes de seguridad	DSS02.02
Actividades				
1. Registrar los eventos relacionados con la seguridad reportados por las herramientas de monitorización 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 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 detectar 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.				

Ilustración 37 DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad - Buenas practicas
Fuente: COBIT 5 – Procesos catalizadores

Se analizó la tablas 34, 35, 36, 37, 38, 39, 40, 41, 42 y 43 y se obtuvo los resultados donde el sub proceso DSS 05.07 de COBIT 5 responde con el uso de sus buenas prácticas a contrarrestar las amenazas:

En el activo de información EQUIPOS INFORMÁTICOS

- 2.- Destrucción de información
- 6.- Robo de equipos

En el activo de información SERVIDORES

- 1.- Fuego.
- 2.- Tormenta eléctrica, rayo
- 9.- Errores de mantenimiento / actualización de equipos (hardware)
- 10.- Manipulación de la configuración
- 13.- Acceso no autorizado
- 14.- Modificación deliberada de la información

En el activo de información EQUIPOS DE RED LOCAL

- 1.- Tormenta eléctrica, rayo
- 2.- Alteración accidental de la información
- 3.- Destrucción de información
- 4.- Fugas de información
- 5.- Errores de mantenimiento / actualización de equipos (software)
- 9.- Difusión de software dañino
- 16.- Instalación de software no autorizado

En el activo de información PERIFÉRICOS Y PENDRIVES

- 3.- Alteración accidental de la información
- 5.- Manipulación de la configuración
- 6.- Acceso no autorizado
- 7.- Modificación deliberada de la información
- 8.- Destrucción deliberada de información.
- 9.- Robo de equipos

En el activo de información PORTÁTILES, TABLETS Y MÓVILES

- 2.- Alteración accidental de la información
- 3.- Destrucción de información
- 4.- Errores de mantenimiento / actualización de programas (software).
- 5.- Errores de mantenimiento / actualización de programas (hardware).
- 6.- Abuso de privilegios de acceso
- 9.- Manipulación de programas
- 11.- Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones

En el activo de información OFICINAS

- 1.- Errores de configuración
- 3.- Fugas de información
- 4.- Errores de mantenimiento / actualización de programas (hardware).
- 8.- Acceso no autorizado
- 9.- Modificación deliberada de la información
- 10.- Divulgación de la información
- 11.- Manipulación de programas
- 12.- Manipulación de equipos
- 14.- Robo de equipos
- 17.- Degradación de los soportes de almacenamiento de la información
- 18.- Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones
- 19.- Hacking no ético

En el activo de información PERSONAL PROPIO

- 1.- Fugas de información
- 3.- Suplantación de identidad del usuario
- 4.- Modificación deliberada de la información
- 5.- Robo de equipos

En el activo de información APLICACIONES INFORMÁTICAS

- 1.- Errores de configuración
- 2.- Alteración accidental de la información
- 3.- Destrucción de información
- 4.- Fugas de información

- 5.- Vulnerabilidad de los programas (software)
- 6.- Errores de mantenimiento / actualización de programas (software).
- 7.- Caída del sistema por agotamiento de recursos (interrupción en los servicios).
- 9.- Manipulación de la configuración.
- 10.- Suplantación de la identidad del usuario
- 11.- Abuso de privilegios de acceso
- 12.- Acceso no autorizado
- 13.- Modificación deliberada de la información
- 15.- Robo de equipos
- 16.- Degradación de los soportes de almacenamiento de la información
- 17.- Hacking no ético

En el activo de información GESTORES DE BASE DE DATOS

- 1.- Errores de configuración
- 2.- Alteración accidental de la información
- 3.- Fugas de información
- 4.- Errores de mantenimiento / actualización de programas (software).
- 7.- Abuso de privilegios de acceso
- 8.- Acceso no autorizado
- 11.- Manipulación de programas

En el activo de información SISTEMAS EXTERNOS

- 2.- Fugas de información
- 6.- Suplantación de la identidad del usuario
- 10.- Degradación de los soportes de almacenamiento de la información
- 11.- Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones
- 12.- Hacking no ético

Al hacer uso del proceso, Entrega, Servicio y Soporte (DSS) – 05. Gestionar servicios de seguridad, esta responde a las metas de TI que podemos ver en el anexo 5 y además se analizó cada métrica identificada para poder hacer el uso de buenas prácticas - actividades de los sub procesos del DSS 05 que nos brinda COBIT 5 para poder mitigar las estimaciones de riesgo y amenazas que fueron encontradas.

CAPÍTULO 4 – Resultados

4.1 Comprobación de la prospectiva.

Se espera que en un futuro la CACSDG agencia Sicuani ya pueda implementar esta propuesta de un modelo de gestión de seguridad de la información basado en el marco de referencia de COBIT 5 y así poder mitigar y corregir todos los riesgos detectados en la empresa, además de salvaguardar lo más importante que es la información.

En cuanto a la gestión de la seguridad de la información, se deberá regir mediante el modelo de gestión de la seguridad propuesto, donde inicialmente se hizo un mapeo detallado sobre las metas relacionadas con TI y las metas corporativas-financieras de COBIT 5. Con este modelo de gestión de la seguridad de la información la CACSDG agencia Sicuani, tendrá la capacidad de saber actuar antes, durante y después de producido un ataque a sus activos de información.

Una vez obtenidas nuestras metas relacionadas con TI, se hizo un mapeo detallado entre estas y los procesos de COBIT 5 para poder analizar la relación principal y secundaria que estas tenían, y así poder obtener los procesos de COBIT 5 que se usarán para proponer un modelo de gestión de seguridad de la información.

Para el modelo propuesto se identificaron los activos de información con los que cuenta la CACSDG agencia Sicuani, para ello se entrevistó a los responsables del área de TI. Identificados los activos de información se aplicó la metodología MAGERIT para poder identificar las amenazas existentes y la probabilidad de ocurrencia. Seguidamente, se evaluó cada activo de información, mediante sus amenazas, probabilidad de ocurrencia, degradación e impacto para obtener su estimación de riesgo en confidencialidad, integridad y disponibilidad, mediante una escala de Bajo, Medio y Alto. Luego, se evaluó los activos de información, con cada amenaza encontrada y su estimación de riesgo en confidencialidad, integridad y disponibilidad, para poder hacer un mapeo detallado con nuestros procesos y sub procesos de COBIT 5. Finalmente, se seleccionó entre los sub procesos que tenían una relación principal y las amenazas a mitigar para poder hacer el uso de las buenas prácticas que COBIT 5 nos brinda.

De acuerdo a las conclusiones a las que llegaron en el antecedente “PLAN DE MEJORA DE LA SEGURIDAD DE INFORMACIÓN Y CONTINUIDAD DEL CENTRO DE DATOS DE LA GERENCIA REGIONAL DE EDUCACIÓN LA LIBERTAD APLICANDO LINEAMIENTOS ISO 27001 Y BUENAS PRÁCTICAS COBIT” – Tesis de pre grado de la Universidad Privada Antenor Orrego – Trujillo. Dice, “De implantarse un Sistema de Gestión de Seguridad de la Información y la instalación de un ambiente de prueba, estos impactarán significativamente sobre la calidad de los sistemas de información.”

Se coincide con la conclusión a la que llega el investigador en el antecedente antes mencionado, ya que la aplicación del modelo de gestión de seguridad de la información basado en el marco de referencia COBIT 5, que se propone tendrá un impacto significativo y positivo sobre los niveles de confidencialidad, integridad y disponibilidad de la información en todos los activos de información identificados de la Cooperativa de Santo Domingo de Guzmán agencia Sicuani.

4.2 Cumplimiento de objetivos.

El trabajo desarrollado en la investigación, propone un modelo de gestión para la seguridad de la información de la CACSDG agencia Sicuani, que está basado en el marco de referencia de COBIT 5. El proceso de identificación de los activos de información fue soportada por la metodología MAGERIT, que permitió identificar las amenazas existentes y la probabilidad de ocurrencia, por cada activo de información.

Al proponer un modelo de gestión para la seguridad de la información de la CACSDG agencia Sicuani usando el marco de referencia de COBIT 5, se realizó un diagnóstico de la situación actual en cuanto a la seguridad de su información, se aplicó una entrevista a los trabajadores de TI de la sede central y a los de la agencia Sicuani

Después de terminar la entrevista se identificó que los activos de información eran estos:

- Equipos informáticos
- Servidores
- Equipos red local
- Periféricos y pendrives
- Portátiles, tabletas y móviles
- Oficinas
- Personal propio
- Aplicaciones informáticas
- Gestores de bases de datos

Al obtener los activos de información se hizo un análisis de los resultados en base a la metodología MAGERIT que permitió identificar las amenazas y estimar el nivel de riesgo que podría tener los activos de información en los niveles de confidencialidad integridad y disponibilidad.

Se aplicó el método en cascada de COBIT para identificar las metas de TI y las metas corporativas-financieras para la Cooperativa Santo Domingo de Guzmán agencia Sicuani, una vez obtenidas nuestras metas relacionadas con TI, se hizo un mapeo detallado entre las metas relacionadas con TI y los procesos de COBIT 5 para poder analizar la relación principal y secundaria que estas tenían, y así poder obtener los procesos de COBIT 5 que se usarán para proponer el modelo de la gestión de seguridad de su información.

De acuerdo a las matrices desarrolladas, y a los procesos de COBIT 5, se logró seleccionar las buenas prácticas de COBIT 5, que permitirán mitigar las amenazas de cada uno de los activos de información analizados en el modelo.

4.3 Contribuciones (impacto).

La información es uno de los bienes más preciados que tiene toda empresa, el mal uso de esta, robo, extorsión, manipulación entre otros riesgos hace que existan modelos de seguridad para poder corregir estos errores, la capacidad de reacción que ahora la CACSDG agencia Sicuani en cuanto a estas y muchas otras amenazas aumenta ya que antes no contaban con ningún modelo propuesto, con esta investigación podemos contribuir al mejor uso de la seguridad de la información, y así la empresa podrá tener una mejor solides corporativa y estar mejor relacionada con las TIC's.

En cuanto a seguridad de su integridad, confidencialidad y disponibilidad se espera que esta empresa se posicione de mejor manera y tenga mejores referentes en cuanto a clientes y proveedores, y así también poder captar mayor socias para la Cooperativa.

Los sistemas de información se basan más que todo en tres grandes dimensiones las cuales son:

Organización
Los sistemas de información automatizan los procedimientos formalmente establecidos por la estructura organizacional, la comunicación informal, la que no está documentada dentro de los manuales de organización y de procedimientos de la empresa generalmente no se representa debido a las grandes variaciones de estas.

Personas
Una organización es tan buena como las personas que la conforman y trabajan dentro de ella, las personas son el recurso más importante de cualquier organización, ya que estas son las que fabrican y producen la sinergia que finalmente se convertirá en utilidades para la empresa

Tecnología
La tecnología está compuesta por todos los recursos de hardware, software, redes y telecomunicaciones que la empresa implementa para soportar la comunicación y producción de la información.

Teniendo en cuenta estas tres dimensiones, la propuesta del modelo de gestión de seguridad de la información aglomera dichas dimensiones.

Glosario

IT. - Information Technology

Framework. - Marco de referencia.

Auditoria.- Instrumento útil para analizar el patrimonio tecnológico de una organización.

Networking.- Hace referencia a eventos, tanto de tipo formal como informal, en los que puedes construir una red de contactos que te ayuden a generar oportunidades tanto de negocio como laborales.

Firewalls.- Es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Malware.- Hace referencia a cualquier tipo de software malicioso que trata de infectar un ordenador o un dispositivo móvil.

Endpoint.- Sirven para descubrir, gestionar y controlar los dispositivos que solicitan acceso a la red corporativa de nuestra empresa.

Hackeo.- Hace referencia a las actividades que buscan comprometer los dispositivos digitales, como ordenadores, teléfonos inteligentes, tabletas e incluso redes enteras.

Phishings.- Conocido como suplantación de identidad, es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta.

Spamming.- Es el abuso de cualquier tipo de sistema de mensajes electrónicos y, por extensión, cualquier forma de abuso en otros medios como spam en mensajería instantánea, en foros, en blogs, en buscadores, en mensajes en teléfonos móviles, etc.

ISO.- Organización Internacional de Normalización.

ITIL.- Biblioteca de Infraestructura de Tecnologías de Información.

SGSI.- Sistema de Gestión de Seguridad de la Información.

Val iT.- Es un conjunto de documentos que proveen un marco de trabajo para el gobierno de las inversiones en TI, creado por el Instituto de Gobierno de las TI (ITGI, por sus siglas en inglés).

ITAF.- Es un marco de trabajo de prácticas profesionales para auditoría y aseguramiento de SI, proporciona múltiples niveles de dirección.

BCP. - Business Continuity Plan

CUBIT.- Control Objectives for Information and related Technology

Conclusiones

1) El uso de COBIT 5 en entidades financieras permite manejar de mejor manera el uso de la tecnología ya que esta desempeña un rol fundamental en las acciones que desarrolla la Cooperativa Santo Domingo de Guzmán agencia Sicuani, además que COBIT 5 es un enfoque robusto para el gobierno y la gestión de la seguridad de la información, sobre la base de las políticas, procesos y estructuras de la organización.

2) MAGERIT es una herramienta eficiente para la evaluación de ocurrencia de las amenazas en la primera etapa de creación de la matriz de riesgos.

3) El modelo propuesto para la Cooperativa Santo Domingo de Guzmán agencia Sicuani es una adaptación de los procesos de COBIT 5 seleccionados tomando en consideración las características de gestión de la información de la organización.

Recomendaciones

1. Se recomienda implementar el modelo de gestión para la seguridad de la información de la Cooperativa Santo Domingo de Guzmán agencia Sicuani usando el marco de referencia de COBIT 5 presentado.
2. Se recomienda realizar estudios que permitan ampliar la flexibilidad de MAGERIT para incorporar mayor cantidad de tipos de amenazas, dado que los tipos considerados son limitados.
3. Se recomienda la implantación de sistemas que permitan automatizar las tareas de gestión de tecnologías de información bajo el marco de trabajo de COBIT 5.

Referencias

Bibliografía

Dangel, A. D. (24 de Febrero de 2010). *Econlink*. Obtenido de https://www.econlink.com.ar/sistemas-informacion/definicion

Desconocido. (26 de Marzo de 2017). *blogspot*. Obtenido de http://cobitmmatiasc.blogspot.com/2017/03/dominios-y-procesos-de-cobit.html

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid: © Ministerio de Hacienda y Administraciones Públicas.

ESAN. (1 de Junio de 2016). *ConexinoESAN*. Obtenido de https://www.esan.edu.pe/apuntes-empresariales/2016/06/los-cinco-principios-de-cobit-5/

Espitia, D. S. (10 de Febrero de 2015). *Reporte Digital*. Obtenido de https://reportedigital.com/seguridad/la-seguridad-de-la-informacion/

G2. (07 de Marzo de 2019). *gedos*. Obtenido de http://www.gedos.es/servicios-2/modelos-gestion/

Gelbstein, E. (2011). *Gobernanza de Internet*. Malta: DiploFundation.

Gomez, A. (2007). *Enciclopedia de la seguridad informatica*. RA-MA Editorial.

INSPQ. (12 de Octubre de 1998). *Instut national de santé publique Québec*. Obtenido de https://www.inspq.qc.ca/es/centro-collaborador-oms-de-quebec-para-la-promocion-de-la-seguridad-y-prevencion-de-traumatismos/definicion-del-concepto-de-seguridad

ISOTools. (06 de Mayo de 2015). *ISOTools*. Obtenido de PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE LA EXCELENCIA: https://www.isotools.org/2015/08/06/en-que-consiste-una-matriz-de-riesgos/

Mendoza, M. A. (4 de Agosto de 2015). *welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2015/08/04/practicas-cobit-seguridad-organizaciones/

Navarrete, C. R. (19 de Enero de 2002). *Tecnologias de Informacion y su utilidad en la empresa*. Obtenido de gestiopolis: https://www.gestiopolis.com/tecnologias-de-informacion-y-su-utilidad-en-la-empresa/

Ramirez Vera, M. A. (1 de Octubre de 2015). *Informatica Empresarial*. Obtenido de blospot.pe: http://iemiguelangelramirez.blogspot.pe/p/definicion-de-informatica-empresarial-y.html

Securityinabox. (20 de Mayo de 2018). *securityinabox*. Obtenido de https://securityinabox.org/es/guide/malware/

SGSI. (28 de Julio de 2015). *Blog especializado en Sistemas de Gestión de Seguridad de Informacion*. Obtenido de https://www.pmg-ssi.com/2015/07/que-es-sgsi/

Universitat de Barcelona. (23 de Abril de 2019). *OBS Business School*. Obtenido de https://www.obs-edu.com/int/blog-investigacion/sistemas/seguridad-de-la-informacion-un-conocimiento-imprescindible

Pérez-Montoro Gutiérrez, Mario (ed.) y Golkhosravi, Mehrad (2010). "Gestión de la información". Díaz Nafría, José María; Pérez-Montoro, Mario y Salto Alemany, Francisco (eds.) (2010). Glosario de conceptos, metaforas, teorías y problemas en torno a la información. Leon: Universidad de León.

Ccesa, M. (2017). Diseño de un sistema de gestión de seguridad de la información balo la NTP ISO/IEC 27001:2014 para la municipalidad provincial de Huamanga, 2016. Publicación Universidad Nacional San Cristóbal del Huamanga.