Modelo unificado para identificación y valoración de los riesgos de los activos de información en una organización

PROYECTO DE GRADO

Fernando Caviedes Sanabria
Bertulfo A. Prado Urrego

Asesor
Ingrid Lucía Muñoz Periñán
Msc. en Gestión de Informática y Telecomunicaciones

FACULTAD DE INGENIERÍA
DEPARTAMENTO ACADÉMICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
MAESTRÍA EN GESTIÓN INFORMÁTICA Y TELECOMUNICACIONES
SANTIAGO DE CALI
2012

Modelo unificado para identificación y valoración de los riesgos de los activos de información en una organización

Fernando Caviedes Sanabria
Bertulfo A. Prado Urrego

Trabajo de grado para optar al título de
Máster en Gestión de Informática y Telecomunicaciones con énfasis en Gerencia de Tecnologías de Información y Telecomunicaciones

Asesor
Ingrid Lucía Muñoz Periñán
Msc. en Gestión de Informática y Telecomunicaciones

FACULTAD DE INGENIERÍA
DEPARTAMENTO ACADÉMICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
MAESTRÍA EN GESTIÓN INFORMÁTICA Y TELECOMUNICACIONES
SANTIAGO DE CALI
2012

DEDICATORIA

A la Vida,
A quienes me la dieron,
A quienes me han acompañado a vivirla
Y en especial a Felipe por prestarme los
Sábados para ir a la universidad.

Fernando Caviedes Sanabria

Dedico este trabajo a las tres personas que me han dado vida:

Mis padres, Noé y María de los Ángeles, que han estado dispuestos a entregar la suya por mí.

A esa personita, de tan solo 5 años, que me enseña algo nuevo cada día, mi hijo Juan Camilo.

Bertulfo A. Prado Urrego

AGRADECIMIENTOS

Un agradecimiento muy especial a la ing. Ingrid Lucía Muñoz Periñán por "robarle" tiempo a sus hijos para dedicarlo a la lectura y corrección de nuestras propuestas. Todos sus regaños fueron producto del alto nivel de compromiso con el cual afrontó la dirección de nuestro proyecto.

Fernando Caviedes Sanabria - Bertulfo A. Prado Urrego

Gracias a aquellos que de una u otra manera me han ofrecido su apoyo en todos los instantes de mi vida, sobre todo en los menos buenos…

Bertulfo A. Prado Urrego

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Santiago de Cali, 25 de junio de 2012

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

LISTA DE FÓRMULAS

RESUMEN

En el país hay sectores, como el financiero y el asegurador, donde existen reglamentaciones que obligan a las empresas a establecer esquemas para mantener la seguridad de la información; desafortunadamente esta situación no es regla sino excepción y se observa que la mayoría de las empresas no tienen claridad sobre el tema y normalmente confunden seguridad de la información con seguridad informática, como ha sido evidenciado por la Asociación Colombiana de Ingenieros de Sistemas (ACIS) en varios de los estudios realizados tanto a nivel nacional como latinoamericano.

En los últimos años la sensación de inseguridad se ha incrementado y a hoy se han hecho comunes los ataques de comunidades de hackers a empresas y estamentos gubernamentales dentro y fuera del país, que muestran que a nivel global existen altos grados de vulnerabilidad en la protección de la información.

También existen entidades públicas y privadas que, desde años atrás, han hecho estudios para el manejo de la información y los riesgos a los que está expuesta; como resultado de los estudios han propuestos marcos de trabajo tales como COBIT, RiskIT, ISO27000, O-ISM3, ITIL, MoR, MagerIT, entre otras; que muestran qué se debe hacer para asegurar los activos de información, pero no indican cómo hacerlo y que, además, generan cierta confusión porque no se tienen o se desconocen, por parte de las empresas, los elementos de juicio que permita determinar cuál o cuáles aplicar o cómo articular estas diferentes propuestas a las condiciones de cada una.

Como respuesta a la problemática planteada y la diversidad de marcos de referencia existentes, se ha fijado como objetivo desarrollar un modelo que unifique las mejores prácticas de los *frameworks* más conocidos, para ser integrado en los sistemas de gestión de seguridad de la información de las organizaciones. Debido a lo extenso del tema, para efectos de este trabajo se ha delimitado el alcance de dicho objetivo a la identificación y valoración de los riesgos de los activos de información.

In Colombia there are sectors such as the financial and the insurer, where there are regulations that require enterprises to establish schemes to maintain the security of the information; unfortunately this is not a rule but exception and is observed that the majority of the companies have no clarity on the subject and usually confused with computer security the information security, as it has been evidenced by the Colombian Association of Engineers of Systems (ACIS - by its acronym in Spanish) in several of the studies both nationally and Latin American area.

In recent years the feeling of insecurity has increased and today have become common hacker attacks communities and government sites to companies inside and abroad, showing that overall there are high levels of vulnerability in protecting the information.

There are also public and private entities, since years ago, made studies for the management of information and the risks to which it is exposed; as a result of the studies have proposed frameworks such as COBIT, RiskIT, ISO27000, O-ISM3, ITIL, MoR, MagerIT, among others; show what should be done to ensure information assets, but do not indicate how to do it and which, furthermore, generate confusion because they don't have or are unknown, by enterprises, the elements of judgment to determine which ones apply or how to articulate these different proposals to the conditions of each.

In response to the issues raised and the diversity of existing frameworks, has set a goal to develop a model that unifies the best practices of the most popular frameworks to be integrated into management systems information security of organizations . Due to the extensiveness of the topic, for purposes of this work has delimited the scope of this objective the identification and and valuation of the risks of information assets.

1. INTRODUCCIÓN

1.1 CONTEXTO DE TRABAJO

Tomando como marco de referencia el entorno país, donde los sectores regularizados y vigilados por entidades de control con herramientas suficientes para influir sobre la voluntad de las empresas para acoger las reglamentaciones emitidas alrededor de la seguridad de la información son pocos[1]; podemos encontrarnos que al momento de hablar de seguridad de la información, en la mayoría de las empresas, se confunde con seguridad informática y, aún más, se termina centrado en controles sin tener idea clara de qué debe protegerse, por qué debe protegerse o cómo debe protegerse.

Es claro que cada empresa, independiente del sector económico, tiene como responsabilidad velar por los intereses y expectativas de los diferentes actores relevantes (accionistas, clientes, empleados, gobierno, comunidad, proveedores) y proteger de la manera debida los activos de información, buscando el balance entre la seguridad y las necesidades de información necesarias para el cumplimiento de las tareas que deba ejecutar cada uno de estos actores para el cabal cumplimiento de sus funciones dentro del engranaje de la organización.

Las empresas, como dueñas de la información y para verificar que se esté dando cumplimiento a esta responsabilidad, tienen el apoyo de las entidades de control internas y externas, que a través de sus evaluaciones y diagnósticos presentan las recomendaciones al respecto, dejando sentadas, normalmente las falencias y de manera genérica las necesidades de mejora. Con este panorama, la administración de las empresas debe escoger entre dar respuesta puntual a cada uno de los informes emitidos por los entes de control o establecer un sistema de gestión que mediante el establecimiento de procesos normalizados, controle de manera eficiente la causa raíz de los aspectos vulnerables en la seguridad de la información y minimice o evite que vuelvan a repetirse los incidentes, tal vez con componentes diferentes, pero con causas comunes.

Por otro lado, eventos de amplia difusión pública de incidentes como la divulgación de los correos diplomáticos de las embajadas americanas (difundidos por la red *Wikileaks*), la sustracción de información de más 75.000 usuarios de los servicios de juegos en línea de la multinacional SONY y el ataque a los sitios web estatales en Colombia (por parte del grupo *Anonymus*[2] a raíz de la promoción de

[1] En el aspecto de emisión de reglamentación tendiente a mejorar la seguridad de la información sobresalen los sectores financiero y asegurador.

[2] Seudónimo utilizado mundialmente por diferentes grupos e individuos que, poniéndose o no de acuerdo con otros, realizan acciones o publicaciones (individuales o concertadas) en protesta a favor de la libertad de expresión, de la independencia de Internet y en contra de diversas organizaciones, entre ellas, sociedades de derechos de autor.

la llamada ley Lleras) o a sitios del gobierno de los Estados Unidos por el anuncio de las leyes SOPA[3] y PIPA[4]; son solo una pequeña muestra del incremento vertiginoso de las amenazas a la seguridad de la información. Amenazas que han llevado a las empresas a preocuparse por los niveles de protección de sus activos de información y a preguntarse si éstos están **correctamente identificados y valorados**.

Si bien, existen propuestas metodológicas y marcos de referencia como COBIT, RiskIT, ITIL, ISO27000, O-ISM3 y otras; no es fácil para las organizaciones establecer de manera práctica la forma de acometer la identificación de sus activos de información y establecer su valor intrínseco dentro de sus procesos críticos, para realizar un correcto y efectivo análisis de riesgo de tales activos dentro de un sistema de gestión de seguridad de la información (SGSI).

En el informe "Uso de la TI en empresas de América Latina" publicado en marzo de 2011 por la consultora Axentian [1] se muestra la gran importancia que le dan las organizaciones a la aplicación de soluciones de tecnologías de información orientadas a atender los requerimientos de usuarios y gerencia y gestión del intercambio de información entre diferentes áreas (Figura 1). Se observa que aspectos como retorno de la inversión de un proyecto, adopción rápida de tecnologías e integración de sistemas nuevos con el *legacy* poseen menos importancia que aquellos en los cuales se hace manejo de la información, permitiendo concluir que herramientas de identificación y aseguramiento de activos de la información serían rápidamente acogidas debido a la importancia y criticidad de éstos.

El Dr. Jeimy Cano y el Magister Andrés Almanza, en junio del 2007 durante la presentación de resultados de la VII Encuesta Nacional de Seguridad Informática (en el marco de la VII jornada de seguridad informática promovida por ACIS[5]), mostraron que las empresas Colombianas[6] al enfrentar temas relacionados con la seguridad de la información encuentran dificultades crecientes para afrontar el proceso por aspectos como (ver Figura 2):

- Inexistencia de las políticas de seguridad.

[3] La Ley SOPA (*Stop Online Piracy Act*) o Ley H.R. 3261; es un proyecto de ley presentado en la Cámara de Representantes de los Estados Unidos el 26 de octubre de 2011 por el Representante Lamar S. Smith que tiene como finalidad expandir las capacidades de la ley estadounidense para combatir el tráfico de contenidos con derechos de autor y bienes falsificados a través de Internet.
[4] PIPA (acrónimo en inglés de *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act* o *PROTECT IP Act*) es un a propuesta de Ley presentada en la Cámara del Senado de Estados Unidos, le daría al gobierno el poder de apagar de internet *websites* y censurar motores de búsqueda después que una reclamación a una infracción de los derechos de autor sea hecha por el propietario del contenido actual.
[5] Acrónimo de Asociación Colombiana de Ingenieros de Sistemas.
[6] De diferentes sectores de la economía

- Bajo entendimiento del tema.
- Falta de colaboración entre las áreas.

Figura 1. Importancia de Objetivos en la Gestión (www.axentian.com) [1]

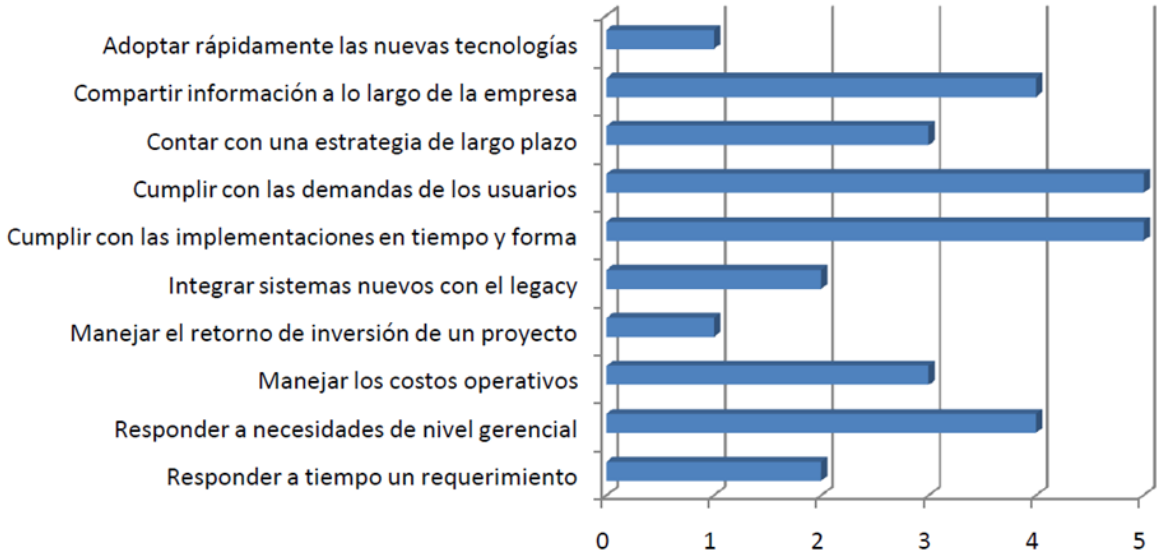
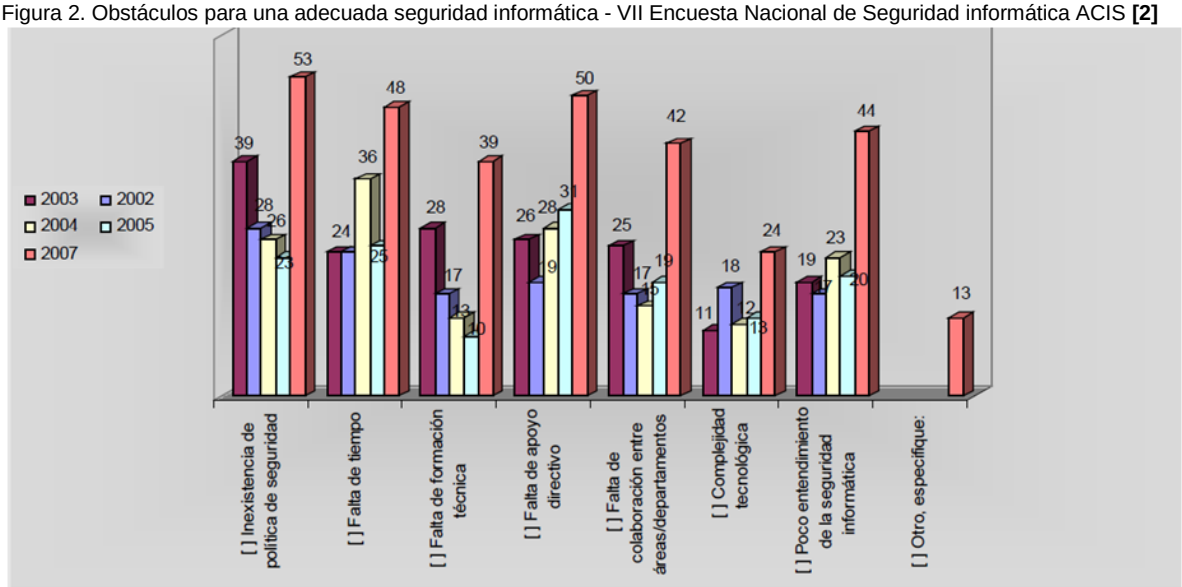


Figura 2. Obstáculos para una adecuada seguridad informática - VII Encuesta Nacional de Seguridad informática ACIS **[2]**



En los resultados de la III Encuesta Latinoamericana de Seguridad de la Información (realizada en el año 2011) presentada por el mismo Dr. Jeimy Cano en la XI Jornada de Seguridad Informática, se evidencia que la falta de colaboración entre áreas de la organización y el poco entendimiento de la

seguridad informática (Figura 3) son los mayores obstáculos para el entendimiento de la seguridad informática; los cuales se han mantenido vigentes a pesar de las nuevas tecnologías y la actualización continua de los marcos de referencia.

Figura 3. Obstáculos para implementar la seguridad - III Encuesta Latinoamericana de Seguridad de la Información ACIS 2011 **[3]**

Gartner en [4], describen lo que para ellos son las cuatro etapas de su modelo de seguridad de la información como:

- Dichosa ignorancia
- Conciencia
- Correctivo
- Excelencia Operacional

En este reporte Gartner [4] plantea que la equivocación más común incurrida por las empresas encuestadas que se encuentran en la etapa de ***Dichosa ignorancia***, es creer que todo está bien en el mundo y no realizar ninguna acción. En las etapas de ***Conciencia*** y ***Correctivo***, el error más grande es creer que con lo realizado se ha terminado, relajándose en los esfuerzos remediadores de la seguridad y comprometiendo la integralidad de la información del negocio. Finalmente, en la fase ***Excelencia Operacional***, los clientes se centran en los procesos y se llega a una superabundancia de procedimientos de seguridad, muchas veces para los procesos que no requieren tal protección.

Con el desarrollo del trabajo sugerido en este documento se hará una propuesta que, tomando los elementos que se ofrecen en los marcos de referencia y metodologías existentes, defina un modelo unificado que permita a las empresas resolver los interrogantes esbozados.

Para validar la viabilidad y eficiencia del modelo propuesto, se propondrá la aplicación del modelo resultante en la unidad de tecnología informática de la matriz de un grupo empresarial colombiano, del que los autores conocen se presentan estas situaciones y pueden tener acceso a la información necesaria para su aplicación.

1.2 PLANTEAMIENTO DEL PROBLEMA

Con los antecedentes presentados, nos atrevemos a deducir que al momento de iniciar el proceso de establecimiento de un sistema de seguridad de la información, las empresas a pesar de que pueden contar con una serie de marcos de referencia y metodologías de clase mundial como son COBIT, RiskIT, la familia ISO27000, O-ISM3, ITIL, entre otras; deben enfrentarse con la problemática de definir cuál de estos marcos de referencia utilizar o cómo articularlos para lograr el tratamiento eficiente de sus activos de información y su evaluación de riesgos.

En los grupos corporativos, con empresas en más de un sector económico, diferentes regulaciones y entes de control, con niveles de exigencia disímiles; la selección del modelo de evaluación de activos de información dentro de su sistema de gestión de seguridad de la información se hace aún más complejo y se requiere de modelos que permitan la identificación y valoración de activos para la realización de procesos de análisis de riesgo adaptados a las condiciones particulares de cada una.

La propuesta a desarrollar parte de la premisa que ya existen marcos de referencia donde se presentan prácticas que se han evaluado con suficiente profundidad y propiedad en su eficacia y eficiencia y que el modelo centrará su aplicación alrededor de estas prácticas y buscará apoyar los procesos que deben dar como resultado el aseguramiento de la información en sus tres componentes básicos: confidencialidad, integridad y disponibilidad y, finalmente, entregará un modelo unificado que, partiendo de las definiciones del marco de la familia ISO27000, permita la identificación y valoración de los activos de información en la organización conforme las prácticas seleccionadas de los marcos de referencia que mejor y de manera más práctica aborden esta labor y que sirvan de introducción a un posterior análisis de riesgo. Este modelo se someterá a prueba en una unidad de servicios de tecnología de un grupo corporativo, aplicándolo a un par de unidades de negocio o empresas.

1.3 OBJETIVOS

1.3.1 Objetivo General.

Desarrollar un modelo unificado para la identificación y valoración de los riesgos de los activos de información dentro de un sistema de gestión de seguridad de la información para cualquier tipo de empresa.

1.3.2 Objetivos Específicos:

- Revisar, evaluar y seleccionar las mejores prácticas de los marcos de referencia para la identificación y valoración de activos dentro de un sistema de gestión de seguridad de la información.

- Revisar, evaluar y seleccionar las mejores prácticas de los marcos de referencia para la identificación y valoración de riesgos dentro de un sistema de gestión de seguridad de la información

- Caracterizar y articular las prácticas y estándares seleccionados para conformar el modelo global para identificación y valoración de activos y riesgos de información.

- Validar el modelo propuesto en Coomeva.

1.4 RESUMEN DEL MODELO PROPUESTO

El modelo propuesto se construye a partir de dos premisas:

- La primera es que la empresa en que se vaya a aplicar tiene un sistema de gestión basado en procesos con una madurez suficiente para integrar dentro de su Sistema de Gestión de Seguridad de la Información (SGSI) un ciclo que, partiendo de los elementos de la estrategia de negocio, conduzca el proceso de identificación y valoración de activos y de identificación y valoración de los riesgos a los que estos están expuestos.
- Segunda, que existen unos marcos de referencia o de mejores prácticas que han sido suficientemente probados en su pertinencia, de los cuales se pueden tomar los elementos que se articulan para generar el modelo.

Este modelo en su construcción refleja las mejores prácticas que se proponen a través de los marcos de referencia de mayor aplicación a nivel global como la familia ISO 27000, ITIL, COBIT, MagerIT, MoR y la Norma Técnica Colombiana NTC 5254, articuladas de una manera sencilla y práctica, de forma que permita a una empresa realizar el proceso de identificación y valoración de los riesgos a los que están expuestos los activos más críticos que soportan los procesos que apalancan el éxito del negocio.

El ciclo del modelo propuesto está compuesto por tres grandes fases: Evaluación alineación organizacional, Evaluación de activos y Evaluación de riesgos.

Evaluación alineación organizacional: corresponde a la revisión y priorización de los procesos productivos que van a ser objeto de aseguramiento y requieren que sus activos y riesgos asociados sean identificados y valorados.

En esta fase se identifica el nivel de participación que sobre el logro de los objetivos de negocio tenga cada uno de los procesos de la cadena de valor de la empresa, aplicando para su valoración el criterio que mejor refleje esta participación sobre el principal objetivo de la organización. El resultado es un vector de procesos con la participación porcentual estimada para cada uno de ellos en el logro de los principales objetivos, que en la siguiente fase del ciclo ayudará a priorizar los activos que quedan incluidos dentro del alcance del análisis de riesgo.

Evaluación de activos: presenta las actividades y mecanismos que permitan a la organización identificar los activos que intervienen en sus procesos productivos y priorizarlos conforme a los criterios que dan valor a la información que intrínsecamente representan.

Esta fase está compuesta por dos etapas: Identificación de activos y valoración de activos.

Para la identificación de los activos se realiza una entrevista con el dueño o el funcionario que mayor conocimiento tenga de la operación de cada proceso incluido en el alcance del análisis de riesgos, diligenciando para cada uno de ellos la tabla de inventario de activos propuesta por el modelo, donde queda consignada la información necesaria para las etapas de valoración de los mismos y para la fase de identificación y valoración de los riesgos a que cada uno de ellos está expuesto.

Cada uno de los activos se clasifica dentro de uno de los seis grupos de activos propuestos (Información, Aplicaciones, Infraestructura, Personas, Servicios y Capital financiero) para facilitar su tratamiento en la fase de evaluación de riesgos.

Una vez levantado el inventario de los activos involucrados en cada uno de los procesos dentro del alcance del análisis de riesgo, se realiza la etapa de valoración de estos activos, donde para cada activo se valora el impacto, en una escala de uno a cinco según los posibles escenarios considerados en el modelo, que puede tener sobre el resultado u objetivo a alcanzar por parte del negocio si el activo es vulnerado en cualquiera de los cuatro atributos considerados por el modelo (Confidencialidad, Integridad, Disponibilidad y Confiabilidad).

La etapa final de esta fase es la estimación del valor de cada activo, aplicando una fórmula de valoración que toma, para los activos de cada proceso, la sumatoria de los impactos estimados para cada atributo, multiplicado por la participación porcentual de cada proceso estimado en la fase anterior.

El resultado de la fase es el inventario de activos valorados.

Para la siguiente fase se sugiere continuar con un porcentaje de los activos con mayor valor.

Evaluación de riesgos: una vez obtenida la relación de activos y definido su valor dentro del proceso productivo, se presentan las herramientas que permiten identificar el grado de exposición y el impacto que puede generar en la organización la violación a la seguridad de estos activos críticos.

Esta última fase tiene tres etapas: Identificación de riesgos, Identificación de controles y Valoración de riesgos.

En la primera etapa, basados en una propuesta ampliada de MagerIT, para cada activo, se identifican las amenazas a que está expuesto según el grupo de activos (Información, Aplicaciones, Infraestructura, Personas, Servicios y Capital financiero) al que pertenezca, dando prioridad a aquellas que pueden afectar el atributo con mayor peso (Confidencialidad, Integridad, Disponibilidad o Confiabilidad) según la valoración realizada en la fase anterior.

La segunda etapa de esta tercera fase asume la existencia de un proceso en la organización para la definición, diseño y seguimiento de controles dentro del tratamiento de los riesgos, que permita evaluar las salvaguardas o controles ya implementados y que puedan mitigar el riesgo o impacto de cada una de las amenazas identificadas en la primera etapa de esta fase.

Si existen salvaguardas se valora la eficiencia de estos controles, con una escala cualitativa (Muy adecuado, Adecuado, Moderado, Débil y Muy débil), que posteriormente el modelo cuantifica para dar sendos valores de eficiencia entre el 90% y el 10% y de la marginalidad correspondiente entre 0.1 y 0.9. Para la valoración de eficiencia de las salvaguardas se consideran la fortaleza del control

establecido, el grado de automatización del mismo y si se tienen o no registros o certeza de la eficiencia de este control.

En la tercera etapa de esta fase se hace la valoración de riesgos considerando dos variables: la probabilidad de que la amenaza identificada se haga realidad y el impacto o nivel de degradación que esto resultaría sobre el activo evaluado.

Para estimar la probabilidad de ocurrencia el modelo propone basarse en el conocimiento previo y conforme a la frecuencia histórica valorar cualitativamente esta probabilidad (Nada frecuente, Poco frecuente, Normal, Frecuente y Muy frecuente). El modelo asigna para cada nivel cualitativo un valor cuantitativo entre 0.2 y 1.

Para estimar el nivel de degradación que generaría sobre el activo la ocurrencia de una amenaza, se plantean escenarios que valoran cualitativamente (Insignificante, Menor, Moderado, Mayor y Catastrófico) el daño y la consecuencia sobre el proceso que signifique el evento sobre el activo. El modelo igualmente asigna un valor numérico a cada uno de los niveles de esta escala entre 0.2 y 1.

Una vez estimados los anteriores valores se procede a calcular tanto el riesgo inherente, que es igual al producto de la probabilidad o frecuencia de ocurrencia de la amenaza por el impacto o degradación del activo y el riesgo marginal, que corresponde al producto del riesgo inherente por el valor de marginalidad calculado para las salvaguardas estimadas en el paso anterior.

El resultado final de esta fase y por lo tanto del ciclo es una tabla que servirá de guía para continuar con el proceso de Gestión de riesgos, donde se deberá establecer la respuesta a cada uno de los riesgos identificados y se deberá hacer seguimiento a la eficiencia de estas respuestas y posteriormente volver a repetir el ciclo de alineamiento, evaluación de activos y evaluación de riesgos propuestos en este modelo.

1.5 RESUMEN DE RESULTADOS OBTENIDOS

La aplicación del modelo en el macro proceso de Infraestructura y Telecomunicaciones (Telco) de la Unidad de Tecnología Informática de Coomeva, simulado para tres de sus servicios, arrojó el vector de procesos y las matrices de activos y riesgos valorados que se muestran en la Figura 4.

Figura 4. Vector de procesos de Telecomunicaciones priorizado **[5]**

Proceso	Adecuación de redes	Montaje de redes	Soporte y continuidad	TOTAL
Participación	50%	30%	20%	100%

Aunque no se incluye en la documentación del modelo, el ejercicio aplicado utilizó la colorimetría inmersa en la hoja electrónica de uso común en la organización que entregó el inventario priorizado y ordenado de los activos de los procesos dentro del alcance de la evaluación (Figura 5).

Figura 5. Inventario (parcial) de activos de Telco valorados **[5]**

ID ACTIVO	IDENTIFICACIÓN	TIPO ACTIVO						ADECUACIÓN DE REDES				MONTAJE DE REDES				SOPORTE Y CONTINUIDAD				VALOR ACTIVO	COMENTARIO
								Peso			50%	Peso			30%	Peso			20%		
	Nombre activo	Infomación	Aplicaciones	Infraestructura	Personas	Servicios	Capital financiero	Confidencilidad	Integridad	Disponibilidad	Confiabilidad	Confidencilidad	Integridad	Disponibilidad	Confiabilidad	Confidencilidad	Integridad	Disponibilidad	Confiabilidad		
13	Redes WAN			X				4	4	4	4	2	3	2	3	5	4	4	5	14.6	Medios de comunicaciones que permiten la interconexión entre los nodos y el sitio central
11	Equipos de telecomunicaciones			X				4	4	3	4	1	3	3	3	4	4	5	5	14.1	Hardware para la prestación de los servicios telemáticos
5	Esquemas de red	X						4	3	4	3	3	3	4	2	3	5	4	3	13.6	Planos físicos y lógicos del esquema de red de un sitio o nodo
19	Servidor de Gestión			X				3	4	3	3	2	3	3	3	3	4	4	4	12.8	Servidor en el cual se almacena la información relacionada con el servicio telemático
14	Red LAN - Wireless			X				4	3	4	3	3	2	2	2	4	4	3	4	12.7	Medios de comunicaciones que permiten la interconexión de equipos.
10	Servicio de Share Point			X				3	4	3	3	3	3	2	3	3	4	4	3	12.6	Repositorio de información donde residen copias del sistema operativo de los equipos de telecomunicaciones y servidor de gestión de telecomunicaciones
6	Proveedores de telecomunicaciones					X		1	4	3	4	1	4	4	4	1	2	5	5	12.5	Terceros que prestan el servicio trasnporte de datos y de equipos de telecomunicaciones
1	Ingenieros de Telemática				X			4	4	3	2	1	4	2	2	4	4	4	3	12.2	Recurso humano del area de telecomunicaciones que desempeña el rol de administrador de infraestructura de telco
7	Proveedores servicios de telefonia					X		1	4	3	3	2	4	3	3	1	2	4	4	11.3	Terceros que prestan el servicio y equipos de telefonia
12	Equipos de telefonía			X				3	3	3	3	1	2	2	2	3	3	4	4	10.9	Hardware para la prestación de los servicios de telefonía
17	Planes de continuidad	X						3	4	2	2	2	3	2	1	3	4	4	4	10.9	Foma de operación ante una eventual falla para garantizar la continuidad en la prestación de los servicios
4	Carpeta Solicitud de Servicios	X						2	4	3	2	3	4	1	1	2	4	3	3	10.6	Documentación red con servicios telemáticos implementados
2	Analistas de telemática				X			4	3	2	2	1	3	1	2	4	3	3	3	10.2	Recurso humano del area de telecomunicaciones que desempeña el rol de operador de infraestructura de telco
21	Software de monitoreo		X					2	3	3	3	1	2	2	2	2	4	4	3	10.2	Herramienta para el control y seguimiento de los servicios telemáticos
8	Contratos	X						3	3	1	1	3	4	3	2	3	4	3	1	9.8	Contratos firmados con los proveedores para la prestación de los servicios

Igualmente se creó el mapa de riesgos priorizado para cada uno de estos activos, tanto para el riesgo inherente como para el riesgo residual, con una escala de colores independiente para cada una de las dos variables, tal como se muestra en la Figura 6.

Figura 6. Ejemplo de riesgos priorizados para un activo **[5]**

ID ACTIVO	IDENTIFICACIÓN	VALOR CONSOLIDADO ACTIVO					AMENAZAS		SALVAGUARDAS			RIESGOS					
	Nombre activo	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	TOTAL	ID	DESCRIPCIÓN	Posee un control	Solidez del control	Nivel de mitigación	Probabilidad (Frecuencia)	Impacto (Degradación)	Valor probabilidad	Valor impacto	Riesgo Inherente	Riesgo Marginal
13	Redes WAN	3.6	3.7	3.4	3.9	14.6	A12	Análisis de tráfico	Si	Moderado	0.5	Muy frecuente	Mayor	1.0	0.8	0.8	0.4
							A14	Interceptación de información (escucha)	Si	Moderado	0.5	Muy frecuente	Mayor	1.0	0.8	0.8	0.4
							I11	Emanaciones electromagnéticas	No	No existente	0.0	Nada frecuente	Moderado	0.2	0.6	0.12	0.12
							A25	Robo	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
							A27	Ocupación no autorizada	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
							E2	Errores del administrador	Si	Muy Adecuado	0.9	Normal	Mayor	0.6	0.8	0.48	0.048
							A4	Manipulación de la configuración	Si	Muy Adecuado	0.9	Normal	Mayor	0.6	0.8	0.48	0.048
							E14	Escapes de información	Si	Adecuado	0.7	Nada frecuente	Moderado	0.2	0.6	0.12	0.036
							E4	Errores de configuración	Si	Muy Adecuado	0.9	Poco frecuente	Mayor	0.4	0.8	0.32	0.032
							E9	Errores de re-encaminamiento	Si	Muy Adecuado	0.9	Nada frecuente	Mayor	0.2	0.8	0.16	0.016
							A5	Suplantación de la identidad del usuario	Si	Muy Adecuado	0.9	Nada frecuente	Mayor	0.2	0.8	0.16	0.016
							A6	Abuso de privilegios de acceso	Si	Muy Adecuado	0.9	Nada frecuente	Mayor	0.2	0.8	0.16	0.016
							A9	Re-encaminamiento intencional de mensajes	Si	Muy Adecuado	0.9	Nada frecuente	Mayor	0.2	0.8	0.16	0.016
							A11	Acceso no autorizado	Si	Muy Adecuado	0.9	Nada frecuente	Mayor	0.2	0.8	0.16	0.016

A partir de este resultado el macro proceso de Infraestructura y Telecomunicaciones podrá definir o mejorar los controles de una manera ordenada y guiada por la criticidad de cada uno de los activos considerados dentro de los procesos evaluados y la criticidad de los riesgos a que cada uno de ellos está expuesto y volver a aplicar el ciclo propuesto por el modelo.

1.6 ORGANIZACIÓN DEL DOCUMENTO

A continuación se presenta una descripción de la estructura del presente documento para dar a los lectores un entendimiento de la manera en que se abordó el proyecto de grado.

1. **Introducción.** En este capítulo se describe el contexto tanto nacional como internacional que motivó el tema del proyecto de grado y se plantea el problema a resolver y los objetivos definidos para construir una propuesta de solución.

2. **Marco teórico.** En este capítulo se describen diferentes *frameworks* existentes para gestionar la seguridad de la información en las empresas. Dado el alcance establecido para el proyecto de grado, la descripción de los *frameworks* seleccionados se centra en los capítulos de gestión de activos de la información y gestión de riesgos.

3. **Análisis comparativo marcos evaluados.** El capítulo presenta comparación de los marcos de trabajo en las dos perspectivas analizadas: gestión de activos de información y gestión de riesgos. Durante la comparación se destaca la importancia que tienen todos los puntos comunes para alimentar el modelo a proponer.

4. **Modelo propuesto.** Tomando como base la comparación y análisis del capítulo anterior, en este se propone un modelo que toma las prácticas de los frameworks revisados considerando además aquellas que a pesar de no ser comunes o poco implementadas aportan claridad y riqueza a la propuesta.

5. **Validación de la propuesta.** El capítulo hace una presentación del método seguido para evaluar el modelo propuesto y los datos o hechos obtenidos como resultado de la evaluación.

6. **Resultados obtenidos.** En este capítulo los valores o hechos obtenidos de la validación del modelo propuesto dejan de ser datos aislados y se articulan para que brinden información que permita determinar la validez y utilidad del modelo.

7. **Conclusiones y futuro trabajo.** Finalmente, en este capítulo, se compilan las lecciones aprendidas en la elaboración del modelo propuesto, se declara la utilidad, validez y viabilidad de implementación del modelo y se plantean interrogantes o inquietudes que pueden ser material para la realización de futuros proyectos.

2. MARCO TEÓRICO

2.1 Sistema de Gestión de Seguridad de la Información

2.1.1 ¿Qué es un sistema de gestión de seguridad de la información?

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es una herramienta que ayuda a las empresas a establecer políticas, procedimientos y controles alineados con los objetivos de negocio de la misma, con el fin de mantener el riesgo por debajo del nivel definido por la propia organización. A los responsables de la entidad les entrega una visión global sobre el estado de sus sistemas de información, las medidas de seguridad que se están aplicando y los resultados que se están obteniendo de dicha aplicación y les permite soportar la toma de decisiones sobre la estrategia a seguir sobre las inversiones que requiera para este aspecto.

El objetivo de un SGSI es garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, minimizados y gestionados por la organización de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la organización, los riesgos, el entorno y las tecnologías a lo largo del tiempo.

La implementación de un Sistema de Gestión de Seguridad de la Información permite establecer un proceso de mejora continua a través del seguimiento de un modelo PHVA (Planear, Hacer, Verificar, Actuar), para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad de la información, con unas responsabilidades claras y el compromiso manifiesto por parte de directivas.

2.1.2 ¿Qué son activos de información?

Un activo de información es cualquier componente, humano, tecnológico, tangible o intangible que interviene en uno o más procesos de negocios de la empresa y que representa algún valor por contener información importante. Estos activos suelen agruparse según su naturaleza para determinar el tratamiento que debe dárseles dentro de un sistema de gestión de seguridad de la información; a manera de ilustración, la Tabla 1 muestra una clasificación típica.

Tabla 1. Ejemplo clasificación de activos de información **[6]**

Activos fuentes de información	Bases de datos y archivos, archivos de configuración de un sistema, manuales de usuarios, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, planes de recuperación.
Activos de software	Software de aplicación, software del sistema, herramientas y programas de desarrollo, herramientas de ofimática.
Activos de procesos	Prácticas empresariales y actividades de negocio
Activos físicos	Servidores y sus componentes externos, equipos de comunicaciones (*switches* y enrutadores de datos, equipos de telefonía, máquinas de fax), medios magnéticos (discos y cintas), equipos de soporte (planta eléctrica, unidades de aire acondicionado), instalaciones, muebles, etc.
Servicios	Servicios telefonía, computo y comunicaciones, servicios generales (agua, luz, aire acondicionado).
Personas	Conocimiento, experiencia, cualificación y destrezas.
Otros activos	Imagen, objetivos, planes, estrategias, credibilidad, reputación.

2.1.3 ¿Cómo se relacionan los activos de información con SGSI?

Una vez identificados los procesos críticos de la organización y los sistemas informáticos que los soportan, cada uno de estos procesos contiene activos de información que a su vez dependen de otros componentes críticos como software, hardware, infraestructura diversa, personas, información diseñados para sostener de forma eficiente dichos procesos críticos. La identificación de los activos y componentes críticos es esencial para conocer qué debe protegerse al clasificarlos mediante criterios como su confidencialidad, integridad y disponibilidad.

2.1.4 Marcos de referencia más representativos para apoyar la gestión de activos de información

Existen muchos marcos y metodologías donde se proponen prácticas que puedan ser aplicadas para realizar la gestión de activos de información como COBIT, RiskIT, ISO27000, O-ISM3, ITIL, entre otras; pero no es fácil seleccionar cuál es la más conveniente en el entorno particular de una empresa o si es más viable una mezcla de ellas; y de ser así, qué se debe tomar de cada una, por qué y cómo hacer para articularlas entre sí considerando que cada uno de los modelos o marcos de referencia tiene implícita o explícitamente una orientación hacia determinado objetivo de control o seguridad: p.e RisktIT para manejo de vulnerabilidades y escenarios de riesgo, COBIT para el análisis de relevancia estratégica de la información o cumplimiento normativo; ITIL para la gestión de los servicios, ISO 27000 u O-ISM3 para estructurar su sistema de gestión de seguridad en general. Aquí se propondrá un modelo unificado tomando las

prácticas presentadas en los marcos de referencia más divulgados a nivel mundial.

2.1.4.1 Familia ISO 27000.

Las normas más destacadas de esta familia son:

2.1.4.1.1 ISO 27001.

Estándar Internacional preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI. Permite a una organización evaluar su riesgo e implementar controles apropiados para preservar la confidencialidad, la integridad y la disponibilidad del valor de la información. El objetivo fundamental es proteger la información de su organización para que no caiga en manos incorrectas o se pierda.

2.1.4.1.2 ISO 27002.

Código de buenas prácticas para la gestión de la seguridad que contiene recomendaciones sobre qué medidas tomar para asegurar los sistemas de información de una organización y describe los objetivos de control (aspectos a analizar para garantizar la seguridad de la información) y especifica los controles recomendables a implantar (medidas a tomar). Anteriormente conocida como ISO 17799, basado en estándar BS 7799 (en España norma UNE-ISO 17799).

2.1.4.1.3 ISO 27005.

Publicada el 4 de Junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información.

2.1.4.2 COBIT.

Objetivos de Control para la información y Tecnologías relacionadas (COBIT siglas en inglés de *Control Objectives for Information and Related Technology*) es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA).

2.1.4.3 ITIL.

Biblioteca de Infraestructura de Tecnologías de Información (ITIL siglas en inglés de *Information Technology Infrastructure Library*), es un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. ITIL da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI. ITIL fue publicado como un conjunto de libros, cada uno dedicado a un área específica dentro de la Gestión de TI. Los nombres ITIL e *IT Infrastructure Library* ('Biblioteca de infraestructura de TI') son marcas registradas de la *Office of Government Commerce* ('Oficina de comercio gubernamental', OGC), que es una división del Ministerio de Hacienda del Reino Unido.

2.1.4.4 O-ISM3.

Estándar abierto y publicado bajo la licencia *Creative Commons*, puede ser descargado de Internet desde la página de ISECOM (*Institute for Security and Open Methodologies*) y su implementación es compatible con ISO 17799 y BS 7799-2. Asimismo, está diseñado para que sea interoperable con OSSTMM (*Open Source Security Testing Methodology Manual*[7]), un estándar de auditorías de seguridad para BS7799, también de ISECOM.

Ayuda a los administradores de seguridad de la información a evaluar sus ambientes de trabajo y planear los procesos de administración para que sean consistentes con los objetivos del negocio.

[7] Manual de la Metodología Abierta de Testeo de Seguridad.

2.1.4.5 RiskIT.

Marco de Riesgos de TI (*The Risk IT Framework*) es producto de la investigación y aporte de la experiencia conjunta de un equipo global de especialistas dirigidos por ISACA, cuya misión fue la de facilitar a la alta Gerencia, una administración efectiva de los riesgos de TI relacionados con el negocio, a partir de su identificación y evaluación; para ello proporciona un marco de referencia que permite identificar, gobernar y gestionar los riesgos.

2.1.4.6 MoR.

Administración del riesgo, MoR (siglas en inglés de Management of Risk), fue diseñada para ser usada por la UK Goverment y es propiedad de OGC. Hoy día es usada tanto en el sector público como privado en el reino unido.

Asiste en el control efectivo de los riesgos, asumiendo éstos como cualquier acción o evento que provenga del exterior de la organización.

2.1.4.7 MagerIT.

Metodología de análisis y gestión de riesgos de los sistemas de información elaborada por el Consejo Superior de Administración Electrónica de España para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información (IT) en las Administraciones Públicas.

2.2 Identificación y Valoración de Activos de Información

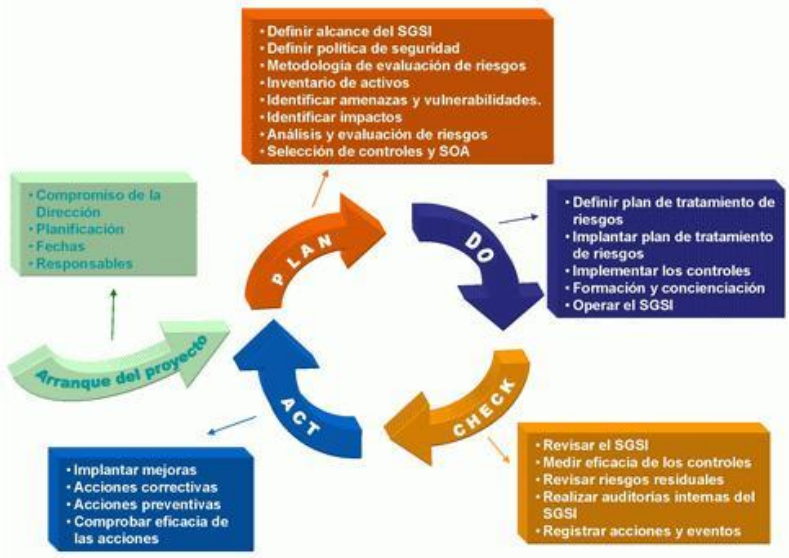
Como se enuncia en la sección anterior, un activo de información es cualquier componente, humano, tecnológico, tangible o intangible que interviene en uno o más procesos de negocios de la empresa y que representa algún valor por contener información importante; deben ser correctamente identificados para posteriormente establecer de qué manera deben protegerse según criterios como la confidencialidad, integridad y disponibilidad de la información que intrínsecamente cada uno de ellos representa.

Cada marco de referencia propone prácticas para la gestión de los activos de información de donde se tomarán las que conformarán el modelo unificado a proponer.

2.2.1 Propuesta ISO27000

La serie ISO27000 muestra en su norma fundamental la ISO27001 que está fundamentada en el ciclo PHVA y presenta las fases que se muestran en la Figura 7.

Figura 7. Modelo PHVA aplicado a los procesos de un SGSI **[7]**



En su estándar ISO/IEC 17799:2005 o 27002 donde establece las guías y principios generales para la iniciación, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información en una organización presenta 11 dominios o cláusulas de control de seguridad (Tabla 2), que en conjunto contienen 39 categorías principales de seguridad y una clausula introductoria para evaluación y tratamiento de riesgos.

Para efectos del desarrollo del modelo unificado a proponer, este documento se enfocará en el dominio Gestión de Activos.

2.2.1.1 Identificación de activos

La ISO27001 que es la norma principal de la serie 27000 y que contiene los requisitos del sistema de gestión de seguridad de la información, respecto a la identificación de activos de información, dedica en su anexo A (ISO 27002) el Dominio A.7 a la gestión de activos, con su objetivo de control A.7.1, con 3 controles asociados (7.1.1, 7.1.2, 7.1.3) incluyendo su propuesta de clasificación y

uso aceptable, cuyo objetivo es “Alcanzar y mantener una protección adecuada de los activos de la Organización”.

Tabla 2. Clausulas o Dominios de la ISO/IEC 17799:2005 **[6]**

Clausula o Dominios	**Categorías de seguridad incluidas**
Política de Seguridad	1
Organización de Seguridad de la Información	2
Gestión de activos	2
Seguridad del recurso humano	3
Seguridad física y medioambiental	2
Gestión de comunicaciones y operaciones	10
Control de accesos	7
Adquisición, desarrollo y mantenimiento de sistemas de información	6
Gestión de Incidentes de seguridad de la información	2
Gestión de continuidad de negocio	1
Cumplimiento	3

La estructura de este punto de la norma en lo que concierne a la identificación de activos se muestra en la Tabla 3.

Tabla 3. Control A.7 Gestión de Activos: Responsabilidad sobre los activos **[6]**

A.7 Gestión de Activos		
A.7.1 Responsabilidad sobre los activos. Objetivo: Alcanzar y mantener una protección adecuada de los activos de la Organización		
A.7.1.1	Inventario de activos.	Control Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.
A.7.1.2	Responsable de los activos.	Control Toda la información y activos asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.
A.7.1.3	Acuerdos sobre el uso aceptable de los activos.	Control Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.

La norma en su información adicional indica que existen muchos tipos de activos (Tabla 4).

En junio de 2008 se publicó la ISO/IEC 27005:2008 (*Information technology, Security techniques, Information security risk management*) que proporciona una guía para la gestión del riesgo en un sistema de seguridad de la información, soporta los conceptos definidos en la ISO/IEC 27001 y está diseñado para ayudar

a la implementación de un sistema de seguridad de la información basado en la gestión del riesgo. El proceso del análisis de riesgo definido en el estándar indica la necesidad de identificar activos de la información bajo riesgo y propone en su anexo informativo B la clasificación mostrada en la Tabla 5.

Tabla 4. Tipos de Activos según ISO27002 **[6]**

Información	Bases de datos y archivos de datos, contratos y acuerdos, documentación del sistema, información sobre investigación, manuales de usuario, material de formación, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos de recuperación, registros de auditoría e información archivada.
Activos de software	Software de aplicación, software del sistema, herramientas de desarrollo y utilidades.
Activos físicos	Equipos de computación, equipos de comunicaciones, medios removibles y otros equipos.
Servicios	Servicios de computación y comunicaciones, servicios generales como por ejemplo iluminación, calefacción, energía y aire acondicionado.
Personas	Sus calificaciones, habilidades y experiencia.
Intangibles	Como reputación e imagen de la organización.

Tabla 5. Clasificación de activos según ISO27005 **[8]**

Activos primarios	Actividades y procesos del negocio
	Información
Activos de soporte	Hardware
	Software
	Redes
	Personal
	Sitio
	Estructura de la organización

2.2.1.2 Valoración de activos

En la sección anterior se muestra que la ISO27001 que es la norma principal de la serie 27000 y que contiene los requisitos del sistema de gestión de seguridad de la información, respecto a la identificación de activos de información, dedica en su anexo A el dominio A.7 a la gestión de activos, con su objetivo de control A.7.2 con 2 controles asociados 7.2.1, 7.2.2, incluyendo su propuesta de clasificación y uso aceptable, cuyo objetivo es “Alcanzar y mantener una protección adecuada de los activos de la Organización”.

La estructura de este punto de la norma respecto a la valoración de activos se muestra en la Tabla 6.

Tabla 6. Control A.7 Gestión de Activos: Clasificación de la información **[6]**

A.7 Gestión de Activos		
A.7.2 Clasificación de la información. Objetivo: Asegurar que la información recibe el nivel de protección adecuado.		
A.7.2.1	Directrices clasificación.	Control La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la Organización.
A.7.2.2	Marcado y tratamiento de la información	Control Se debe desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y manejo de la información, de acuerdo con el esquema de clasificación adoptado por la Organización.

En la guía de implementación de la [9], para las directrices de clasificación se indica que la clasificación y los controles de protección asociados para la información deben tener en cuenta las necesidades de los negocios para compartir o restringir información y el impacto en el negocio asociado a tales necesidades, identificando los impactos que la pérdida de confidencialidad, integridad y disponibilidad pueda tener sobre estos activos. Igualmente hace referencia a otros controles asociados que deben ser considerados al momento de la clasificación de los activos Tabla 7.

Tabla 7. Controles asociados a la clasificación de activos **[6]**

A.11.1.1	Política de control de accesos	Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.
A.7.1.2	Responsable de los activos	Toda la información y activos asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.
A.10.7.2	Eliminación de soportes	Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales.

Advierte que debe prestarse atención al número de categorías de clasificación y los beneficios que pueden obtenerse de su uso, que sistemas excesivamente complejos pueden ser incómodos y antieconómicos de utilizar o resultar poco prácticos y que debe tenerse cuidado en la interpretación de etiquetas de clasificación de documentos de otras organizaciones, que pueden tener diferentes definiciones para etiquetas de nombre igual o similar.

Adicionalmente hace ver que el nivel de protección puede evaluarse mediante el análisis de la confidencialidad, integridad y disponibilidad y cualesquiera otros requisitos para la información considerada; que la Información a menudo deja de ser sensible o crítica tras un determinado período de tiempo, por ejemplo, cuando

la información ha sido hecha pública. Estos aspectos deben tenerse en cuenta como sobre-clasificación que puede conducir a la aplicación de controles innecesarios, resultando en gastos adicionales; que tener en cuenta y juntar documentos con requisitos de seguridad similares al momento de asignar niveles de clasificación podría ayudar a simplificar la tarea de clasificación. Y que de manera general, la clasificación dada a la información es una forma abreviada de determinar cómo es manejada y protegida esta información.

En la misma guía, para el marcado y tratamiento de la información, indica que los procedimientos para el etiquetado de la información necesitan cubrir los activos de información en formatos físicos y electrónicos; que la salida de sistemas que contiene información que es clasificada como sensible o crítica debe llevar una etiqueta de clasificación adecuada (en la salida). El etiquetado debe reflejar la clasificación de acuerdo con las reglas establecidas en el control 7.2.1. Para esta consideración se incluyen elementos como informes impresos, salidas en pantalla, soportes grabados (por ejemplo, cintas, discos, CDs), mensajes electrónicos, y transferencias de archivos.

Finalmente sugiere que los acuerdos con otras organizaciones que incluyan el intercambio de información deben considerar los procedimientos para identificar la clasificación de la información e interpretar etiquetas de clasificación de la otra organización.

2.2.2 Propuesta COBIT

2.2.2.1 Identificación de activos

COBIT brinda un modelo de procesos genéricos que representa los que normalmente se encuentran en las funciones de TI, ofreciendo un modelo de referencia común entendible para los gerentes operativos de TI y del negocio.

Una de las premisas de COBIT es que las organizaciones deben satisfacer la calidad, los requerimientos fiduciarios y de seguridad de su información, así como de todos sus activos y aclara que las buenas prácticas que propone representan el consenso de los expertos, están enfocadas fuertemente en el control y menos en la ejecución dentro del siguiente principio básico, “Para proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita invertir en, y administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que provean los servicios que entregan la información empresarial requerida.” (Figura 8).

Los recursos de TI identificados en COBIT[10] se pueden definir según la Tabla 8.

Figura 8. Principio básico de COBIT **[11]**

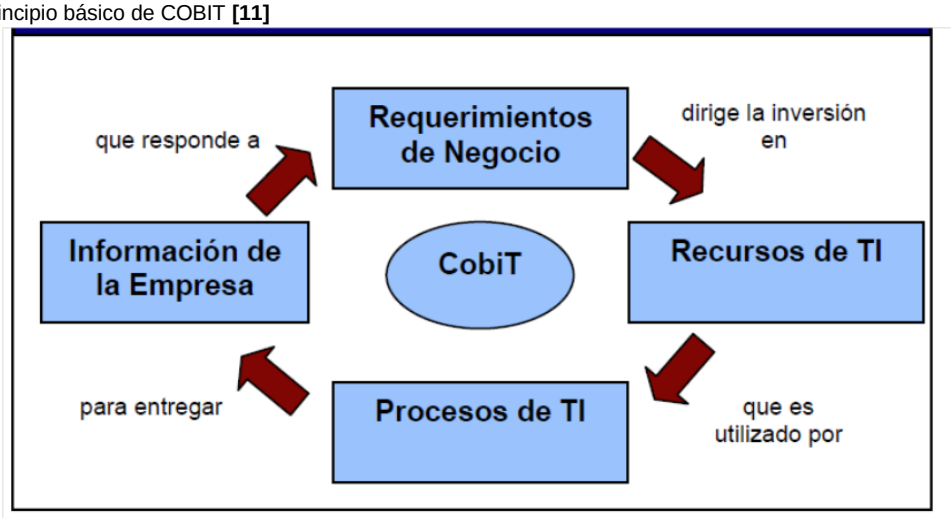
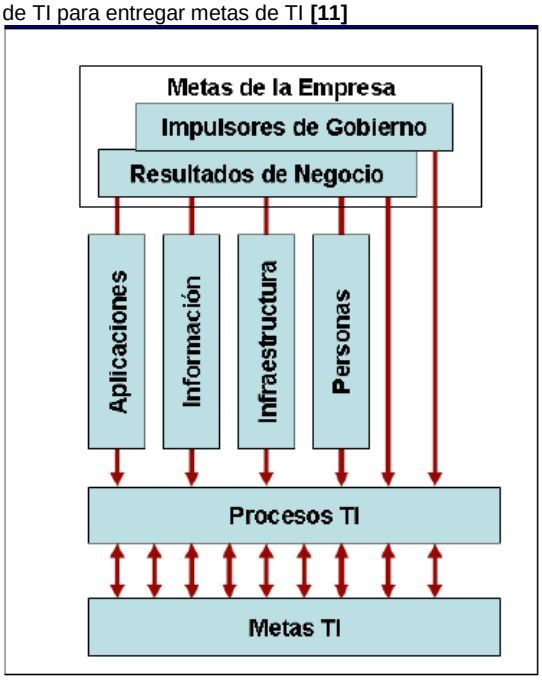


Tabla 8. Recursos de TI según COBIT **[10]**

Recursos	**Descripción**
Aplicaciones	Incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.
Información	Son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.
Infraestructura	Es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.
Personas	Corresponde al personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por *outsourcing* o contratadas, de acuerdo a como se requieran.

En la Figura 9 se resume la propuesta de COBIT para la gestión de estos recursos, de manera que estén alineados con las metas de negocio.

Figura 9. Gestión de los recursos de TI para entregar metas de TI **[11]**



En el marco de trabajo propuesto por COBIT [10], en la sección 1 de cada uno de los 34 procesos de TI identificados se muestra el mapeo del proceso con los recursos de TI (Figura 10), además indica con una **P** la relación primaria y con una **S** la secundaria con las áreas de enfoque de gobierno de TI (Figura 11), entre otras.

Figura 10. Mapeo recursos en procesos de TI **[11]**

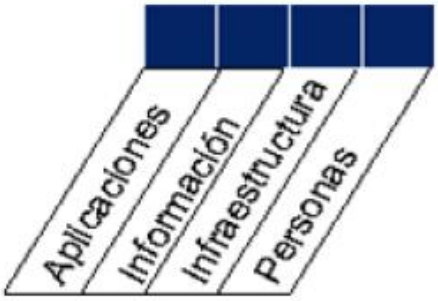
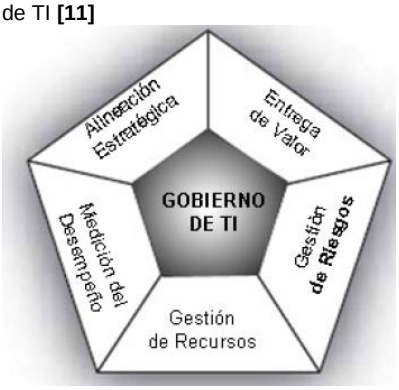


Figura 11. Áreas de enfoque de gobierno de TI **[11]**



La Tabla 9 muestra los 4 dominios y los 34 procesos; además especifica el tipo de relación con el área de enfoque de gobierno de TI “Gestión de Recursos”. De este mapeo se evaluarán los procesos que apoyen la identificación de activos para integrar el modelo unificado y en el siguiente capítulo se explorarán los que tengan énfasis en la valoración de los mismos.

Tabla 9. Mapeo procesos contra recursos según COBIT **[10]**[8]

Enfoque Gestión de Recursos	PROCESO		RECURSOS DE TI			
			APLICACIONES	INFORMACIÓN	INFRAESTRUCTURA	PERSONAS
DOMINIO PLANEAR Y ORGANIZAR						
S	PO1	Definir un Plan Estratégico de TI	**X**	**X**	**X**	**X**
P	PO2	Definir la Arquitectura de la Información	**X**	**X**		
P	PO3	Determinar la Dirección Tecnológica	**X**		**X**	
P	PO4	Definir los Procesos, Organización y Relaciones de TI				**X**
S	PO5	Administrar la Inversión en TI	**X**		**X**	**X**
	PO6	Comunicar las Aspiraciones y la Dirección de la Gerencia		**X**		**X**
P	PO7	Administrar Recursos Humanos de TI				**X**
	PO8	Administrar la Calidad	**X**	**X**	**X**	**X**
	PO9	Evaluar y Administrar los Riesgos de TI	**X**	**X**	**X**	**X**
S	PO10	Administrar Proyectos	**X**		**X**	**X**
DOMINIO ADQUIRIR E IMPLEMENTAR						
S	AI1	Identificar soluciones automatizadas	**X**		**X**	
	AI2	Adquirir y mantener software aplicativo	**X**			
P	AI3	Adquirir y mantener infraestructura tecnológica			**X**	
S	AI4	Facilitar la operación y el uso	**X**		**X**	**X**
P	AI5	Adquirir recursos de TI	**X**	**X**	**X**	**X**
P	AI6	Administrar cambios	**X**	**X**	**X**	**X**
S	AI7	Instalar y acreditar soluciones y cambios	**X**	**X**	**X**	**X**
DOMINIO ENTREGAR Y DAR SOPORTE						
P	DS1	Definir y administrar los niveles de servicio	**X**	**X**	**X**	**X**
S	DS2	Administrar los servicios de terceros	**X**	**X**	**X**	**X**
P	DS3	Administrar el desempeño y la capacidad	**X**		**X**	
S	DS4	Garantizar la continuidad del servicio	**X**	**X**	**X**	**X**
	DS5	Garantizar la seguridad de los sistemas	**X**	**X**	**X**	**X**
P	DS6	Identificar y asignar costos	**X**	**X**	**X**	**X**
S	DS7	Educar y entrenar a los usuarios				**X**
	DS8	Administrar la mesa de servicio y los incidentes	**X**			**X**
P	DS9	Administrar la configuración	**X**	**X**	**X**	
	DS10	Administrar los problemas	**X**	**X**	**X**	**X**
P	DS11	Administrar los datos		**X**		
S	DS12	Administrar el ambiente físico			**X**	
P	DS13	Administrar las operaciones	**X**	**X**	**X**	**X**
DOMINIO MONITOREAR Y EVALUAR						
S	ME1	Monitorear y Evaluar el Desempeño de TI	**X**	**X**	**X**	**X**
	ME2	Monitorear y Evaluar el Control Interno	**X**	**X**	**X**	**X**
	ME3	Garantizar el Cumplimiento Regulatorio	**X**	**X**	**X**	**X**
P	ME4	Proporcionar Gobierno de TI	**X**	**X**	**X**	**X**

2.2.2.2 Valoración de activos

Los activos tienen valor para las organizaciones en la medida en que contribuyan con su información intrínseca en el logro de los objetivos. Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT[10] como requerimientos de

[8] Creada con base en la información recopilada del documento referenciado.

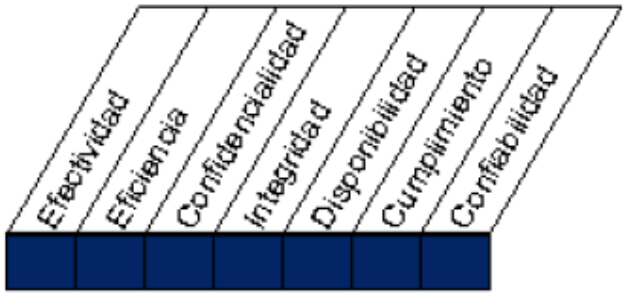
información del negocio. Con base en los requerimientos más amplios de calidad, fiduciarios y de seguridad, se definen siete criterios de información (Tabla 10).

Tabla 10. Criterios de Información **[10]**[9]

Criterio	**Descripción**
Efectividad	Tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
Eficiencia	Consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.
Confidencialidad	Se refiere a la protección de información sensitiva contra revelación no autorizada.
Integridad	Está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
Disponibilidad	Se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.
Cumplimiento	Tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.
Confiabilidad	Se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

De manera global los 4 dominios y sus 34 procesos presentan las relaciones mostradas en la tabla “Mapeo de procesos, recursos y criterios (Figura 12) según COBIT”, donde se incluye una P en la columna Dominio, si el proceso tiene una relación primaria con el área de enfoque de gobierno de TI “Gestión de Riesgos” propuesto por COBIT.

Figura 12. Criterios de Información **[11]**



De este mapeo se evaluarán los procesos que apoyen la identificación de activos para integrar el modelo unificado (Tabla 11).

[9] Creada con base en la información recopilada del documento referenciado.

Tabla 11. Mapeo de procesos, recursos y criterios según COBIT **[10]**[10]

Enfoque Gestión de Recursos	Enfoque Gestión de Riesgo	PROCESO		RECURSOS DE TI				CRITERIOS DE INFORMACIÓN						
				APLICACIONES	INFORMACIÓN	INFRAESTRUCTURA	PERSONAS	EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD
DOMINIO PLANEAR Y ORGANIZAR														
S	S	PO1	Definir un Plan Estratégico de TI	X	X	X	X	P	S					
P	S	PO2	Definir la Arquitectura de la Información	X	X			S	P	S	P			
P	S	PO3	Determinar la Dirección Tecnológica	X		X		P	P					
P	P	PO4	Definir los Procesos, Organización y Relaciones de TI				X	P	P					
S		PO5	Administrar la Inversión en TI	X		X	X	P	p					S
	P	PO6	Comunicar las Aspiraciones y la Dirección de la Gerencia		X		X	P					P	
P	S	PO7	Administrar Recursos Humanos de TI				X	P	P					
	S	PO8	Administrar la Calidad	X	X	X	X	P	P		S			S
	P	PO9	Evaluar y Administrar los Riesgos de TI	X	X	X	X	S	S	P	P	P	S	S
S	S	PO10	Administrar Proyectos	X		X	X	P	P					
DOMINIO ADQUIRIR E IMPLEMENTAR														
S	S	AI1	Identificar soluciones automatizadas	X		X		P	S					
	S	AI2	Adquirir y mantener software aplicativo	X				p	p		S			S
P		AI3	Adquirir y mantener infraestructura tecnológica			X		S	P		S	S		
S	S	AI4	Facilitar la operación y el uso	X		X	X	P	P		S	S	S	S
P		AI5	Adquirir recursos de TI	X	X	X	X	S	P				S	
P		AI6	Administrar cambios	X	X	X	X	P	P		P	P		S
S	S	AI7	Instalar y acreditar soluciones y cambios	X	X	X	X	P	S		S	S		
DOMINIO ENTREGAR Y DAR SOPORTE														
P		DS1	Definir y administrar los niveles de servicio	X	X	X	X	P	P	S	S	S	S	S
S	P	DS2	Administrar los servicios de terceros	X	X	X	X	P	P	S	S	S	S	S
P	S	DS3	Administrar el desempeño y la capacidad	X		X		P	P			S		
S	P	DS4	Garantizar la continuidad del servicio	X	X	X	X	P	S			P		
	P	DS5	Garantizar la seguridad de los sistemas	X	X	X	X			P	P	S	S	S
P		DS6	Identificar y asignar costos	X	X	X	X		P					P
S	S	DS7	Educar y entrenar a los usuarios				X	P	S					
		DS8	Administrar la mesa de servicio y los incidentes	X			X	P	P					
P	S	DS9	Administrar la configuración	X	X	X		P	S			S		S
	S	DS10	Administrar los problemas	X	X	X	X	P	P			S		
P	P	DS11	Administrar los datos		X						P			P
S	P	DS12	Administrar el ambiente físico			X					P	P		
P		DS13	Administrar las operaciones	X	X	X	X	P	P		S	S		
DOMINIO MONITOREAR Y EVALUAR														
S	S	ME1	Monitorear y Evaluar el Desempeño de TI	X	X	X	X	P	P	S	S	S	S	S
	P	ME2	Monitorear y Evaluar el Control Interno	X	X	X	X	P	P	S	S	S	S	S
	P	ME3	Garantizar el Cumplimiento Regulatorio	X	X	X	X						P	S
P	P	ME4	Proporcionar Gobierno de TI	X	X	X	X	P	P	S	S	S	S	S

2.2.3 Propuesta ITIL

2.2.3.1 Identificación de activos

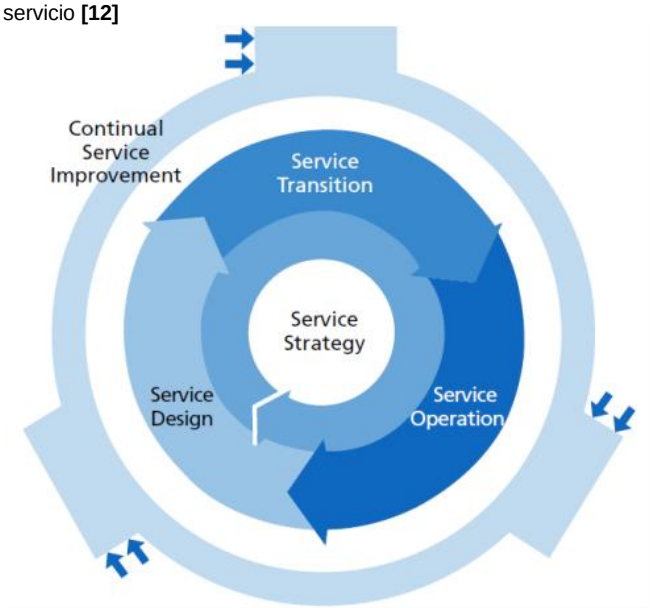
ITIL ofrece un enfoque sistemático para la entrega de calidad de los servicios de TI. Ofrece una detallada descripción de la mayoría de los principales procesos de una organización de TI e incluye listas de chequeo para tareas, procedimientos y responsabilidades que pueden utilizarse como base para adaptar a las necesidades de distintas organizaciones.

En la versión 3, ITIL ha elegido un nuevo enfoque de gestión de servicio no centrado alrededor de procesos, si no centrado en el ciclo de vida del servicio en donde la estrategia de servicio es el eje alrededor del cual corren las demás fases (ver Figura 13); estas son, la fase de formulación de políticas y objetivos, las

[10] Creada con base en la información recopilada del documento referenciado.

fases de diseño del servicio, transición del servicio y estrategia de operación de este servicio, su tema constante es adaptación y cambio. La fase de mejora del servicio continua significa aprender y mejorar y abarca todas las fases del ciclo.

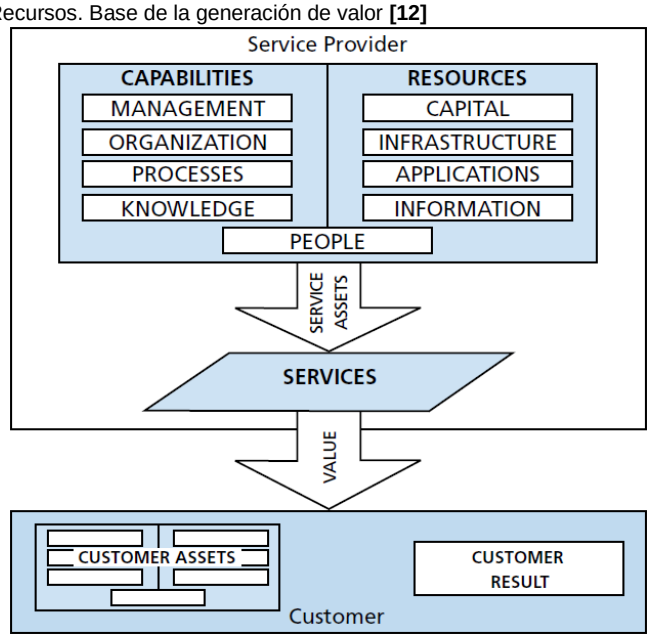
Figura 13. Ciclo de vida del servicio **[12]**



En el capítulo 3 de [12], Fase del Ciclo de Vida: Estrategia del Servicio; donde se tratan la definición del concepto de estrategia, activos de servicio, catálogos de servicio, aplicación de la estrategia a través del ciclo de vida de servicio, varios tipos de proveedores de servicios, gestión financiera, administración del portafolio de servicios, desarrollo organizacional, y riesgos estratégicos; establece que la misión de la fase de estrategia del servicio es desarrollar la capacidad para lograr y mantener una ventaja estratégica y que uno de sus objetivos asociados es la creación de activos estratégicos. En este mismo capítulo se definen los activos de servicio e identifica Recursos y Capacidades como tipos de activos que son utilizados por las organizaciones para crear valor en la forma de productos o servicios.

Los Recursos comprenden la entrada directa para la producción; administración, organización, personas y conocimientos que convierten recursos en valor. Las Capacidades representan la habilidad de una organización para coordinar, administrar y aplicar los recursos a fin de producir valor. Concluyendo que Capacidades y Recursos juntos forman la base del valor de un servicio (Figura 14).

Figura 14. Capacidades y Recursos. Base de la generación de valor **[12]**



Para ampliar el concepto se listan los tipos de activos (Tabla 12).

Más adelante se resalta que la comprensión de los clientes es esencial en administración del servicio, enfatizando que se debe conocer el rendimiento de los activos de los clientes. Sin una visión de estos activos no hay ninguna base determinar el valor de un servicio. Los activos del cliente son el contexto en el que se crea valor porque son el vínculo con los resultados de negocio que el cliente desea. En la siguiente sección revisaremos que se propone en ITIL para la valoración de estos activos.

2.2.3.2 Valoración de activos

Para efectos de valoración en [12], en el capítulo 3.2 Conceptos básicos, se define que: “Valor no sólo es perceptible en los resultados del negocio del cliente, sino también, depende en gran medida, de la percepción del cliente. Esto se refiere a la diferencia entre el valor económico y la percepción económica. La percepción depende de la propia imagen del cliente, los atributos de valor, y la experiencia personal. Es importante recordar que la definición y diferenciación de valor están principalmente en la mente del cliente. Valor económico no tiene que corresponder automáticamente con las percepciones económicas del cliente.”, y define dos conceptos para valorar un servicio:

Tabla 12. Tipos de activos **[12]**

Tipo	Descripción
Gestión	Gestión es un sistema que incluye liderazgo, administración, política, rendimiento, regulaciones e incentivos; esta capa cultiva, coordina y supervisa los otros tipos de activos.
Organización	Los activos organizacionales son configuraciones activas de las personas, procesos, aplicaciones e infraestructuras que implementan todas las actividades de la organización; esta capa incluye las jerarquías funcionales, grupos de redes sociales, equipos y personas y todos los sistemas que se utilicen para trabajar juntos hacia objetivos colectivos.
Procesos	Los activos de proceso consisten en algoritmos, métodos, procedimientos y rutinas que impulsan la implementación y administración de las actividades y las interacciones
Conocimiento	Los activos de conocimiento son acumulaciones de realizaciones, experiencia, información, conocimiento y propiedad intelectual que están asociadas con actividades específicas y contextos.
Personas	Las personas como activos representan la capacidad de análisis, percepción, creatividad, educación, evaluación, liderazgo, comunicación, coordinación, empatía y confianza.
Información	Los activos de información son colecciones, patrones y abstracciones significativas de datos que se aplican en el contexto de los clientes, contratos, servicios, eventos, proyectos y producción.
Aplicaciones	Los activos de aplicación son muy variados en tipo e incluyen artefactos, automatización y herramientas para apoyar el desempeño de otros tipos de activos; las aplicaciones derivan su valor de sus relaciones con otros activos.
Infraestructura	Los activos de infraestructura existen en forma de capas que se definen por sus relaciones de apoyo a otros activos (personas y aplicaciones, en particular).
Capital financiero	Los activos financieros son necesarios a fin de apoyar la propiedad o el uso de todo tipo de activos.

- **Utilidad**: Aptitud para el propósito. Corresponde a los atributos del servicio que tienen un efecto positivo sobre el rendimiento de las actividades, los objetos y las tareas con un resultado específico. Utilidad representa el aumento de una posible ganancia.
- **Garantía**: Idoneidad para el uso. Disponibilidad y confiabilidad en la continuidad y seguridad. Soportes de garantía para la disminución de posibles pérdidas.

“La utilidad es lo que recibe el cliente y la garantía afirma cómo se entregará”.

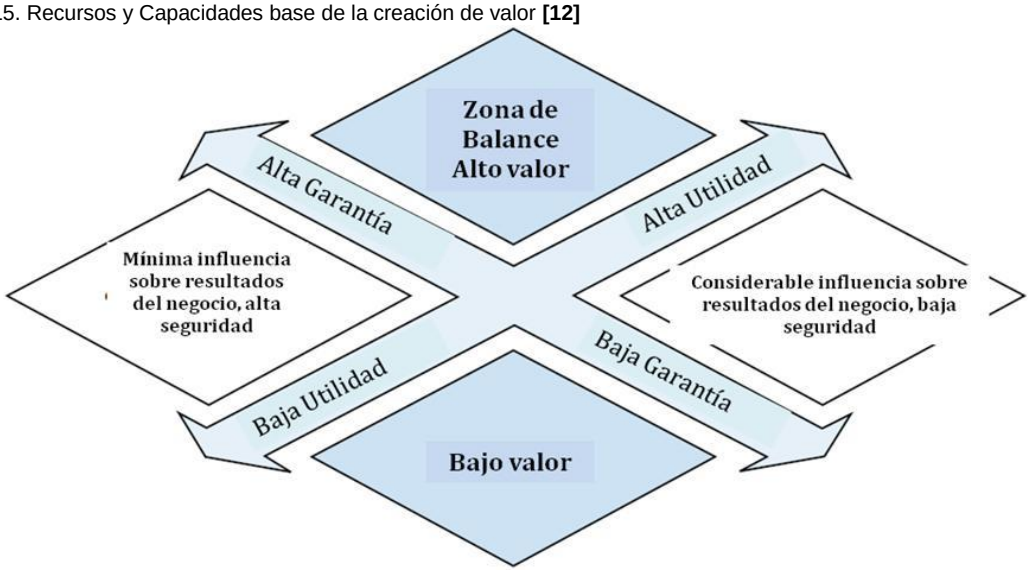
Aclara que la utilidad de un servicio se entrega mediante el apoyo de ciertos resultados o impidiendo algunos riesgos y costos y que la gestión de los activos deben buscar balance entre los recursos financieros puestos en ellos y evitando su escasez.

Considerando la imposibilidad de utilizar los servicios que no son aptos para su uso, la garantía asegura la utilidad de un servicio haciendo que esté disponible y que ofrezca suficiente capacidad, continuidad y seguridad.

- **Disponibilidad**: La disponibilidad es el aspecto más fundamental en la prestación de servicios a un cliente. Ofrece al cliente la garantía de que los servicios están disponibles según las condiciones acordadas.
- **Capacidad**: Sin la supervisión efectiva de los problemas de capacidad, los proveedores de servicios no se encuentran en condiciones de ofrecer la utilidad de la mayoría de los servicios.
- **Continuidad**: La continuidad garantiza que el servicio soporta al negocio incluso durante momentos de gran dificultad o en condiciones de desastre.
- **Seguridad**: Garantiza a los clientes que pueden hacer uso del servicio de manera segura.

ITIL afirma que la creación de valor (Figura 15) es una combinación de los efectos de utilidad y garantía, que ambos son necesarios para la creación de valor para el cliente y muestra en el siguiente gráfico el efecto de la combinación de utilidad y garantía sobre los activos del cliente.

Figura 15. Recursos y Capacidades base de la creación de valor **[12]**



Aunque esta propuesta está dirigida a la generación de valor a través de servicios de tecnología, para la concepción del modelo unificado se extrapolará para aplicarla a la valoración de activos, buscando acoger y respetar la recomendación de este marco que dice “La correcta sincronización entre el contexto de creación

de valor (activos de cliente) y los conceptos de creación de valor (arquetipo de servicio) ayuda a prevenir deficiencias en el rendimiento.”.

En [12], en el capítulo 4: Fase de diseño de servicio del ciclo de vida se hace especial énfasis en la importancia de los datos y su gestión y presenta varias oportunidades que permiten valorarlos:

- **Valorando datos por su disponibilidad**: Este enfoque mira qué procesos del negocio se afectarían si no se dispusiera de una porción determinada de los datos, y que costo le representaría esto a la Organización.
- **Valoración de pérdida de datos**: Este enfoque examina el costo de tener que reemplazar los datos si se pierden o son destruidos.
- **Valorando datos teniendo en cuenta el ciclo de vida**: Este enfoque se centra en cuestiones tales como cómo se crean los datos, cómo se hacen disponibles, y cómo se archivan; el ciclo de vida difiere (y por lo tanto, también lo hacen los costos) dependiendo de la demanda, o si estos pasos pueden ser realizados por un parte interna o externa.

Y propone clasificarlos en tres niveles:

- **Datos operacionales:** Estos son los datos necesarios para el funcionamiento de la organización y son menos específicos.
- **Datos tácticos**: Estos son los datos necesarios para la línea o administración superior; entre otros las cosas, esto se refiere a los datos periódicos, analizados a partir de los sistemas de información de gestión.
- **Datos estratégicos**: Se refiere a las tendencias a largo plazo en comparación con información externa (mercado).

Otro aporte que hace ITIL respecto a la medición y que podemos aplicar para efectos de valorar los activos se encuentra en el capítulo 10.4 Gestión de Disponibilidad de [12] donde advierte “La medición es extremadamente importante. Esta puede ser realizada desde tres perspectivas”:

- **Perspectiva del negocio:** Mira la disponibilidad de TI en términos de su contribución o impacto en las funciones vitales del negocio.
- **Perspectiva del usuario:** Ve la disponibilidad de los servicios de TI como una combinación de tres factores: frecuencia, alcance en duración e impacto (cuántos usuarios o partes de la organización son afectados) y también tiempos de respuesta.
- **Perspectiva del proveedor de servicio de IT:** Ve la disponibilidad de los servicios y sus componentes desde el punto de vista de disponibilidad, confiabilidad y mantenibilidad.

ITIL en su gestión de activos y configuración ofrece una visión completa de los activos, en el capítulo 11.3 de [12] Administración de la configuración garantiza que todos los componentes de los ítems de configuración (CIs, por su sigla en inglés) que forman parte del servicio o producto se identifican, son provistos de una línea de base (configuración básica) y son mantenidos. Administra todos los cambios relativos a estos componentes y formalmente aprueba nuevas versiones. El proceso también proporciona un modelo lógico de todos los servicios, bienes, la infraestructura física y las relaciones mutuas. Igualmente muestra los métodos procesos y técnicas para mantener la base de datos de configuración (CMDB, por su sigla en inglés), donde define el conjunto de atributos que debe tener cada uno de los ítems o elementos de configuración.

2.2.4 Propuesta O-ISM3

2.2.4.1 Identificación de activos

O-ISM3 es independiente de la tecnología. Define un número manejable pero integral de procesos de seguridad de la información suficientes para las necesidades de la mayoría de las organizaciones, con los controles de seguridad pertinentes, identificándolos dentro de cada proceso como un conjunto esencial de ese proceso. Es totalmente compatible con los estándares 27000:2009, COBIT e ITIL ISO/IEC establecidos en este campo.

Este marco plantea la definición de una política de seguridad de TI que apoye y aplique a su política corporativa para proteger sus activos, principalmente su activo más valioso, sus datos.

En el apéndice B de [13]. Términos y definiciones, B.2 Componentes de un sistema de información, define: “Los sistemas de información son complejos y tienen una variedad de componentes tangibles e intangibles. Los componentes de un sistema pueden ser clasificados en un nivel seleccionado de abstracción de acuerdo a sus características estructurales y transaccionales”.

Con respecto a las características estructurales indica que un sistema de información puede estar construido por:

- **Repositorios:** Cualquier almacenamiento temporal o permanente de información, incluyendo RAM, bases de datos, sistemas de archivos y cualquier clase de medios portátiles.
- **Interfaces:** Cualquier dispositivo de entrada/salida, tal como pantallas, impresoras y sistemas de fax.

- **Canales:** Caminos físicos o lógicos para el flujo de mensajes, incluyendo buses, LAN, redes, etc., Una red es un conjunto dinámico de canales.
- **Fronteras:** Define los límites del sistema.
- Los dispositivos físicos pueden hospedar uno o más componentes lógicos. Los objetos estructurales existen en cualquier nivel lógico o físico.

Las características transaccionales son dadas por los diversos recursos que un sistema de información utiliza para producir resultados reales:

- **Servicios:** Cualquier proveedor de valor en un sistema de información, incluidos los servicios prestados por el BIOS, sistemas operativos y aplicaciones. Un servicio puede colaborar con otros servicios o servicios de nivel inferior para completar una tarea que proporciona valor, como por ejemplo el acceso a la información de un repositorio.
- **Sesiones:** Una relación temporal de confianza entre servicios. El establecimiento de esta relación puede requerir el intercambio de credenciales.
- **Mensajes:** Cualquier información significativa intercambiada entre dos servicios o un usuario y una interfaz.

Los activos transaccionales son dinámicos, tal como correr un proceso, mover un mensaje o una sesión en vivo. Los activos estáticos tales como correo, archivos de programas o credenciales almacenadas en un repositorio no son considerados ni mensajes, ni servicios. Los objetos transaccionales existen tanto en el nivel lógico como físico.

Respecto al proceso de gestión de activos de información y particularmente sobre su identificación O-ISM3 define …en el capítulo 2 Conceptos, en el numeral 2.4 Procesos, 2.4.1.4 Procesos operacionales específicos…; la responsabilidad de "Identificar y proteger los activos dentro del ciclo de vida" y más adelante …en el capítulo 3.5 Definición O-ISM3 – en el contexto de seguridad…, aclara que "O-ISM3 se centra en el logro de los objetivos de negocio y de seguridad. La protección de los activos es importante en la medida en que promueve el logro de los objetivos de seguridad".

En el capítulo 4 Modelo de procesos O-ISM3; 4.5 Procesos específicos: gestión operativa, 4.5.3 Control al ciclo de vida…, define el proceso OSP-3 Gestión de inventario como lo muestra la Tabla 13.

Tabla 13. OSP-3: Gestión de Inventario **[13]**

Proceso	**OSP-3 Gestión de Inventario**
Descripción	Este proceso identifica, clasifica y valora los activos (repositorios, interfaces, servicios y canales) a proteger. Debe identificar: • El propietario del sistema de información para cada sistema de información, el dominio de TI gestionada al que pertenece y el estado actual dentro de tal dominio de TI gestionada. • La audiencia autorizada de los principales repositorios extraíbles manteniendo un inventario de las copias y sus propietarios. • El licenciamiento del software instalado y desinstalado • El licenciamiento de la información con derechos de autor utilizada. Mantener un inventario totalmente exacto puede ser costoso y extremadamente difícil en grandes organizaciones. O-ISM3 reconoce esta dificultad, por lo que este proceso puede realizarse como un proceso periódico o un proceso en tiempo real (detección).
Valor	La Operación del sistema de gestión de seguridad de información (en inglés *Information Security Management System* - ISMS) depende de la identificación de los activos críticos a proteger y de una clasificación adecuada utilizando, por ejemplo, el lenguaje de marcado de aseguramiento de la información (en inglés *Information Assurance Markup Language* - IAML).
Documentación	OSP-031: Procedimiento de inventario OSP-032: Política para nombrar activos OSP-033: Procedimiento para etiquetado de activos TSP-032: Clasificación y requisitos de la información
Entradas	Hardware conocido Software conocido Otros repositorios de información conocidos Informe de limpieza (OSP-6)
Salidas	Inventario de activos (múltiples procesos) Repositorios y mensajes clasificados Interfaces, servicios y canales priorizados Calidad y durabilidad repositorios agrupados Informe de métricas (TSP-4)
Responsabilidades	Supervisor: TSP-14 Propietario de proceso Propietario de proceso: Administración de sistemas de información
Procesos relacionados	TSP-3: Definir objetivos de Seguridad OSP-4: Control de cambios a sistemas de información en dominios de IT gestionados.
Metodologías relacionadas	No aplicable.

2.2.4.2 Valoración de activos

O-ISM3[13] “evita conceptos tradicionales de seguridad, tales como la confidencialidad, disponibilidad e integridad, porque hay una tentación para usarlas como taquigrafía, y que lleva a malentendidos. Mientras que los objetivos de seguridad son necesariamente específicos y detallados, el uso de términos operacionales contribuye a eliminar la ambigüedad y el potencial de malentendido” y en su capítulo…2.4 Procesos, 2.4.1 niveles, 2.4.1.3 Procesos Tácticos específicos… define que la gestión táctica responde ante la gestión estratégica por el desempeño del ISMS y por el uso de recursos y establece dentro de su objetivos y responsabilidades definir el entorno para la gestión operativa, incluyendo dentro de esta los objetivos de seguridad y la clasificación de activos, para lo que propone el proceso TSP-3 Definir objetivos de seguridad que regirá los procesos operativos OSP (Tabla 14).

Tabla 14. TSP-3: Definir Objetivos de seguridad **[13]**

Proceso	**OSP-6 Definir objetivos de seguridad**
Descripción	Este proceso especifica los objetivos de seguridad para los objetivos de negocio específicos, los objetivos de seguridad por dominio de TI administrado asociado y relacionados con las políticas y normas. Se tienen en cuenta negocios, cumplimiento de normas, personal, control de acceso, prioridad, durabilidad, calidad de la información y requisitos relacionados con la técnica.
Valor	La definición de los objetivos de seguridad y los objetivos de seguridad por dominio de TI administrado proporciona la base para la construcción de los procesos de los ISMS.
Documentación	TSP-031: Plantilla de objetivos de seguridad de información TSP-032: Plantilla de requerimientos de información y de clasificación GP-01E: Plantilla de política de uso aceptable TSP-034: Plantilla de directiva de acuerdo de código de conexión con terceros GP-017: Política de control del ciclo de vida
Entradas	Política de seguridad de la información (GP-024, GP-3)
Salidas	Objetivos de seguridad de información (TSP-4 GP-3, 2 OSP, OSP-8, OSP-9, OSP-20) Requerimientos de información y clasificación (documentación) Política de uso aceptable (TSP-10, TSP-11) Informe de métricas (TSP-4)
Responsabilidades	Supervisor: Propietario del proceso GP-3 Propietario del proceso: CIO
Procesos relacionados	GP-3: Diseño y evolución del ISM
Metodologías relacionadas	No aplicable

Como se mostró en la sección anterior, en el capítulo 4 de [13] …Modelo de procesos O-ISM3, 4.5 Procesos específicos: gestión operativa, 4.5.3 Control al ciclo de vida…, define el proceso OSP-3 Gestión de inventario, donde se indica que este “Este proceso identifica, clasifica y valora los activos (repositorios, interfaces, servicios y canales) a proteger” y los procesos OSP-4 Control de cambios al dominio de IT Gestionado Sistemas de Información, OSP-5 Dominio de TI gestionado Parcheo, OSP-6 Dominio de TI gestionado Limpieza y OSP-7 Dominio de TI gestionado Endurecimiento en mayor grado contemplan la gestión de valor de los activos y definen su estado dentro del ciclo de vida que propone O-ISM3. Todo lo anterior se define desde el proceso fundamental de O-ISM3 GP-3 Diseño y Evolución del ISM (Tabla 15).

Tabla 15. GP-3: Diseño y Evolución del ISM **[13]**

Proceso	**GP-3 Diseño y Evolución del ISM**
Descripción	Este proceso valida si el proceso operacional existente coincide (o no coincide) con la organización, las necesidades y objetivos de cumplimiento de normas expresados en los objetivos de negocio. También valida si el proceso se realiza mejor y más eficiente que el caso anterior. El alcance incluye las siguientes áreas: • Medio ambiente y misión organizacional • Cumplimiento de normas legales y reglamentarias • Protección de la privacidad , tanto de empleados como de clientes • Protección de la propiedad intelectual Este proceso selecciona los procesos operacionales más adecuados para lograr los objetivos de seguridad. Hay una variedad de técnicas disponibles para ayudar en las decisiones que deben incluirse en los procesos de seguridad para permitir el logro de los objetivos de seguridad. Los modelos organizacionales son útiles para hacer la evaluación de riesgo, amenaza, vulnerabilidad e impacto en el negocio. Dependiendo del alcance y profundidad de la evaluación, son útiles los modelos de los siguientes tipos: • Modelo de sistema de información • Modelo financiero • Modelo logístico (transporte, suministros, residuos) • Modelo de infraestructura (energía, espacio, condiciones ambientales) • Modelo de personal y las responsabilidades • Modelo de reputación organizacional Estas técnicas deben agregar valor produciendo resultados reproducibles de manera rentable. Las unidades más pequeñas, consideradas por una evaluación de riesgos centrada en O-ISM3 son los objetivos de negocio, los objetivos de seguridad, y dominios de TI administrados.
Valor	El desarrollo de los objetivos específicos del negocio requiere una comprensión estratégica del medio ambiente y objetivos de negocios de la organización. Los objetivos de negocio constituyen la base de la política de seguridad de la información y los objetivos de seguridad de la información. Cada organización tiene objetivos de seguridad diferentes, actúa en diferentes dominios de TI administrados y tiene diferentes recursos. Una selección adecuada de procesos dará un buen retorno de la inversión en seguridad. La eficiencia de los procesos y su eficacia puede disminuir con el tiempo a menos que exista un esfuerzo continuo de la organización hacia mayores niveles de capacidad.

Tabla 15. GP-3: Diseño y Evolución del ISM **[13]** (Continuación)

Proceso	**GP-3 Diseño y Evolución del ISM**
Documentación	GP-030: Plantilla de amenazas internas y externas, vulnerabilidades a los objetivos del negocio y objetivos seguridad por dominio de TI administrado. GP-031: Plantilla de inversión recomendada en procesos de ISM nuevos y existentes por dominio de TI administrado. GP-032:Metodología de diseño y evolución del ISM GP-01G: Política de gestión de riesgo GP-033: Plantilla de directiva de seguridad de información
Entradas	*Estrategia y objetivos de la organización* GP-017: Política de control del ciclo de vida GP-024: Política de seguridad de información Objetivos de seguridad de información (TSP-3) Asignar recursos para la seguridad de la información (SSP-6) Inventario de activos (OSP-3) Informes de incidentes (OSP-24) Informes de intrusión (OSP-24) Informes de análisis forense (OSP-25) Informe de pruebas de copias de seguridad (OSP-10) Mayor confiabilidad y disponibilidad prueba informe (OSP-26) Informe de prueba de continuidad de operaciones (OSP-15) Informe de capacidades de los atacantes potenciales (TSP-14) Informe de contraespionaje de los atacantes potenciales (TSP-14)
Salidas	Amenazas internas y externas, vulnerabilidades a los objetivos del negocio y objetivos seguridad por dominio de TI administrado. Nivel aceptable de amenazas internas y externas, vulnerabilidades a los objetivos del negocio y objetivos seguridad por dominio de TI administrado. Informe de amenazas para asegurar (TSP-13). Inversión recomendada en procesos de ISM nuevos y existentes por dominio de TI administrado (SSP-6). Definición de procesos de gestión seguridad de la información (incluyendo las prioridades y las inversiones necesarias). Políticas de procesos de seguridad: • GP-033: Política de seguridad de la información • GP-017: Política de Control del ciclo de vida • GP-018: Política de acceso y control medioambiental • GP-019: Política de gestión de disponibilidad • GP-01C: Política de pruebas y auditoría • GP-01B: Política de monitoreo y control • GP-01A: Política de gestión de incidentes • GP-01D: Política de gestión de personal Informe de métricas (TSP-4)
Responsabilidades	Supervisor: CEO y representantes de las partes interesadas Propietario del proceso: CIO

Tabla 15. GP-3: Diseño y Evolución del ISM **[13]** (Continuación)

Proceso	**GP-3 Diseño y Evolución del ISM**
Procesos relacionados	SSP-4: Definir la División de normas de derechos SSP-6: Asignar recursos para la seguridad de la información TSP-3: Definir objetivos de seguridad TSP-13: Gestión de seguros OSP-3: Gestión de inventario OSP-24: Gestión de incidentes OSP-25: Forense OSP-20: Emulación de incidente OSP-19: Auditoría técnica interna
Metodologías relacionadas	ISO 544R (paquete de soporte para ISO 9001:2000) Evaluación de Impacto en el Negocio (BIA) Evaluación de riesgos, evaluación de amenazas, evaluación de la vulnerabilidad: Como / NZS 4360, CRAMM, EBIOS, ISO/IEC 27005:2008, MAP MAGERIT, CLUSIF MEHARI, OCTAVE, NIST SP 800-30, el estándar técnico de taxonomía de riesgo de Open Group

2.3 Identificación y Valoración de Riesgos.

Una vez identificados, clasificados y valorados los activos de información que soportan la operación crítica de los negocios, se debe determinar cómo deben ser protegidos para garantizar la estabilidad del proceso; para esto se deberá identificar en nivel de exposición y grado de afectación de sus atributos en caso de ser vulnerados. Los diferentes marcos de referencia proponen prácticas para la gestión de los riesgos de los activos de información que se referenciarán para acoger aquellas que conformarán el modelo unificado a proponer.

2.3.1 Propuesta ISO27000

La norma ISO/IEC 27001[11] define lo siguiente, respecto a la identificación y valoración de riesgos, para el establecimiento del SGSI:

c) Definir el enfoque organizacional para la valoración del riesgo
   1) Identificar una metodología de valoración del riesgo que sea adecuada al SGSI y a los requisitos reglamentarios, legales y de seguridad de la información del negocio, identificados.
   2) Desarrollar criterios para la aceptación de riesgos, e identificar los niveles de riesgo aceptables.

d) Identificar los riesgos

[11] Numeral 4.2.1 literales c), d) y e).

1) Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios.
2) Identificar las amenazas en relación a los activos.
3) Identificar las vulnerabilidades que podrían ser aprovechadas por dichas amenazas.
4) Identificar los impactos que la pérdida la confidencialidad, integridad y disponibilidad puede tener sobre estos activos.

e) Analizar y evaluar los riesgos

1) Valorar el impacto de negocios que podría causar una falla en la seguridad, sobre la organización, teniendo en cuenta las consecuencias de la pérdida de confidencialidad, integridad o disponibilidad de los activos.
2) Valorar la posibilidad realista de que ocurra una falla en la seguridad, considerando las amenazas, las vulnerabilidades, los impactos asociados con estos activos, y los controles implementados actualmente.
3) Estimar los niveles de los riesgos.
4) Determinar la aceptación de riesgo o la necesidad de su tratamiento a partir de los criterios establecidos en el numeral 4.2.1, literal c)

La misma norma ISO/IEC 27001 especifica que los controles implementados dentro del alcance, los límites y el contexto de SGSI se deben basar en el riesgo. La aplicación de un proceso de gestión del riesgo en la seguridad de la información puede satisfacer este requisito.

La ISO/IEC 27005:2008 (*Information technology, Security techniques, Information security risk management*) [14] dice textualmente en su introducción: “Esta norma proporciona directrices para la gestión del riesgo en la seguridad de la información en una organización, dando soporte particular a los requisitos de un sistema de gestión de seguridad de la información (SGSI) de acuerdo con la norma ISO/IEC 27001. Sin embargo, esta norma no brinda ninguna metodología específica para la gestión del riesgo en la seguridad de la información. Corresponde a la organización definir su enfoque para la gestión del riesgo, dependiendo por ejemplo del alcance de su SGSI, del contexto de la gestión del riesgo o del sector industrial. Se puede utilizar una variedad de metodologías existentes bajo la estructura descrita en esta norma para implementar los requisitos de un sistema de gestión de seguridad de la información.”. Sin embargo amplía los términos y definiciones de las normas ISO/IEC 27001 e ISO/IEC 27002, entre otras con las siguientes, que hacen referencia al tópico que nos interesa:

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados.

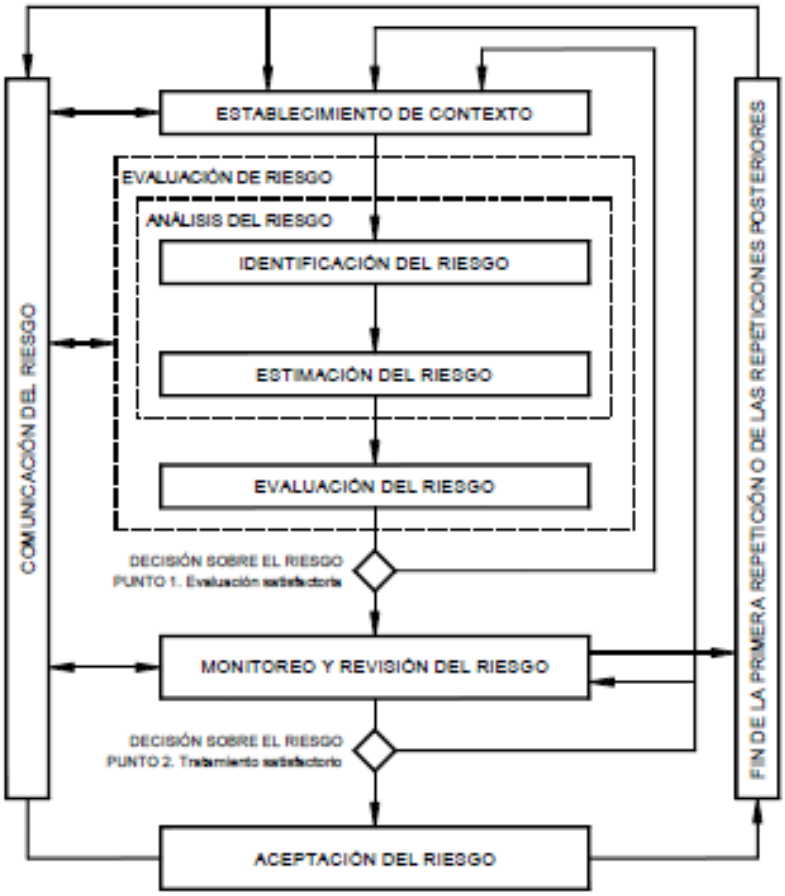
Riesgo en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Anotando que se mide en términos de una combinación de la probabilidad de que suceda un evento y sus consecuencias.

Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Igualmente establece que la gestión del riesgo en la seguridad de la información ha de ser un ciclo continuo que conste de: Establecimiento del contexto, evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo y monitoreo y revisión del riesgo; como se muestra en la gráfica "Proceso de gestión del riesgo en la seguridad de la información" (Figura 16).

Figura 16. Proceso de gestión del riesgo en la seguridad de la información **[14]**



2.3.1.1 Identificación de riesgos

Dentro de la fase de Establecimiento del contexto, la norma sugiere hacer las siguientes definiciones:

Criterios de evaluación del riesgo

Recomienda desarrollar criterios para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la organización, teniendo en cuenta los siguientes aspectos:

- El valor estratégico del proceso de información del negocio.
- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, confidencialidad e integridad para las operaciones y el negocio.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación.

De igual modo, los criterios de evaluación del riesgo se pueden utilizar para especificar las prioridades para el tratamiento del riesgo.

Criterios de Impacto

Recomienda desarrollar criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la organización, causados por un evento de seguridad de la información, considerando los siguientes aspectos:

- Nivel de clasificación de los activos de información impactados.
- Brechas en la seguridad de la información (por ejemplo, pérdida de confidencialidad, integridad y disponibilidad).
- Operaciones deterioradas (partes internas o terceras partes).
- Pérdida del negocio y del valor financiero.
- Alteración de planes y fechas límites.
- Daños para la reputación.
- Incumplimiento de los requisitos legales, reglamentarios o contractuales.

La norma ISO/IEC 27005:2008 dedica su numeral 8 a la evaluación del riesgo, en sus fases de identificación (de la Tabla 16 a la Tabla 26), estimación y evaluación (de la Tabla 27 a la Tabla 36).

Tabla 16. Descripción general de la valoración del riesgo en la seguridad de la información **[6]**

8. VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN	
8.1 DESCRIPCIÓN GENERAL DE LA VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN	
Entrada	Criterios básicos, el alcance y los límites, y la organización establecida para el proceso de la gestión del riesgo en la seguridad de la información.
Acción	Los riesgos se deberían identificar, describir cuantitativa o cualitativamente y priorizar frente a los criterios de evaluación del riesgo y los objetivos relevantes para la organización.
Guía para la implementación	Un riesgo es una combinación de las consecuencias que se presentarían después de la ocurrencia de un evento indeseado y de su probabilidad de ocurrencia. La valoración del riesgo cuantifica o describe cualitativamente el riesgo y permite a los directores priorizar los riesgos de acuerdo con su gravedad percibida u otros criterios establecidos. La valoración del riesgo consta de las siguientes actividades: - Análisis del riesgo (véase el numeral 8.2) el cual consiste en: - Identificación del riesgo (véase el numeral 8.2.1). - Estimación del riesgo (véase el numeral 8.2.2). - Evaluación del riesgo (véase el numeral 8.3). La valoración del riesgo determina el valor de los activos de información, identifica las amenazas y vulnerabilidades aplicables que existen (o que podrían existir), identifica los controles existentes y sus efectos en el riesgo identificado, determina las consecuencias potenciales y, finalmente, prioriza los riesgos derivados y los clasifica frente a los criterios de evaluación del riesgo determinados en el contexto establecido. Con frecuencia, la valoración del riesgo se lleva a cabo en dos (o más) iteraciones. En primer lugar, se realiza una valoración general para identificar riesgos potencialmente altos que ameriten posterior valoración. La siguiente iteración puede implicar una consideración adicional en profundidad de los riesgos potencialmente altos revelados en la iteración inicial. Cuando estas actividades suministran información que no es suficiente para evaluar el riesgo, entonces se realiza un análisis más detallado, probablemente en partes del alcance total y, tal vez, utilizando un método diferente. Depende de la organización seleccionar su propio enfoque para la valoración del riesgo con base en los objetivos y la meta de esta valoración. En el Anexo E (de la norma) se puede encontrar la discusión sobre los enfoques para la valoración del riesgo en la seguridad de la información.
Salida	Una lista de los riesgos valorados, con prioridad de acuerdo con los criterios de evaluación del riesgo.

Tabla 17. Análisis del riesgo **[6]**

8. VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN	
8.2 ANÁLISIS DEL RIESGO	
8.2.1 Identificación del riesgo	
8.2.1.1 Introducción a la identificación del riesgo	El propósito de la identificación del riesgo es determinar qué podría suceder que cause una pérdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida. Los pasos que se describen en los siguientes numerales de la sección 8.2.1 deberían recolectar datos de entrada para la actividad de estimación del riesgo.
8.2.1.2 Identificación de los activos	
Entrada	Alcance y límites para la valoración del riesgo que se va a realizar, lista de los componentes con sus propietarios, ubicación, funciones, etc.
Acción	Se deberían identificar los activos dentro del alcance establecido (se relaciona con la norma NTC-ISO/IEC 27001, numeral 4.2.1 d) 1)).
Guía para la implementación	Un activo es todo aquello que tiene valor para la organización y que, por lo tanto, requiere de protección. Para la identificación de los activos se recomienda tener en cuenta que el sistema de información consta de más elementos que sólo hardware y software. La identificación de los activos se debería llevar a cabo con un nivel adecuado de detalle, que proporcione información suficiente para la valoración del riesgo. El nivel de detalle utilizado en la identificación de los activos tendrá influencia en la cantidad total de información recolectada durante la valoración del riesgo. Este nivel se puede mejorar en iteraciones posteriores de la valoración del riesgo. Se debería identificar al propietario de cada activo, para asignarle la responsabilidad y rendición de cuentas sobre éste. El propietario del activo puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la organización (véase el numeral 8.2.2.2 con relación a la valoración del activo). El límite de la revisión es el perímetro definido de los activos de la organización que debe ser gestionado por parte del proceso de gestión del riesgo en la seguridad de la información. Mayor información sobre la identificación y la valoración de los activos con relación a la seguridad de la información se puede obtener en el Anexo B (de la norma).
Salida	Una lista de los activos que van a estar sometidos a gestión del riesgo, y una lista de los procesos del negocio relacionados con los activos y su importancia.

Tabla 18. Identificación de las amenazas **[6]**

8. VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN	
8.2 ANÁLISIS DEL RIESGO	
8.2.1 Identificación del riesgo	
8.2.1.3 Identificación de las amenazas	
Entrada	Información sobre las amenazas obtenida de los propietarios de los activos, de los usuarios, de la revisión de incidentes, y de otras fuentes, incluidos los catálogos de amenazas externas.
Acción	Se deberían identificar las amenazas y sus orígenes (se relaciona con la norma ISO/IEC 27001, numeral 4.2.1 d) 2)).
Guía para la implementación	Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a las organizaciones. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Es recomendable identificar tanto los orígenes de las amenazas accidentales como de las deliberadas. Una amenaza puede tener su origen dentro o fuera de la organización. Las amenazas se deberían identificar genéricamente y por tipo (por ejemplo, acciones no autorizadas, daño físico, fallas técnicas) y, cuando sea adecuado, las amenazas individuales dentro de la clase genérica identificada. Esto significa que ninguna amenaza se pasa por alto, incluidas las inesperadas, pero teniendo en cuenta que el volumen de trabajo requerido es limitado. Algunas amenazas pueden afectar a más de un activo. En tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados. La entrada para la identificación de las amenazas y la estimación de la probabilidad de ocurrencia (véase el numeral 8.2.2.3) se puede obtener de los propietarios o los usuarios del activo, del personal de recursos humanos, del administrador de las instalaciones y de especialistas en seguridad de la información, expertos en seguridad física, área jurídica y otras organizaciones que incluyen organismos legales, bien sea autoridades, compañías de seguros y autoridades del gobierno nacional. Los aspectos ambientales y culturales se deben tener en cuenta cuando se consideran las amenazas. La experiencia interna obtenida de los incidentes y las valoraciones anteriores de las amenazas, se deberían tomar en consideración en la valoración actual. Podría ser valioso consultar otros catálogos de amenazas (pueden ser específicas para una organización o un negocio) para completar la lista de amenazas genéricas, cuando sea pertinente. Los catálogos y las estadísticas sobre las amenazas están disponibles en organismos industriales, del gobierno nacional, organizaciones legales, compañías de seguros, etc. Cuando se utilizan catálogos de amenazas o los resultados de valoraciones anteriores de las amenazas, es conveniente ser consciente de que existe un cambio continuo de las amenazas importantes, en especial si cambia el ambiente del negocio o los sistemas de información. Mayor información sobre los tipos de amenazas puede encontrar en el Anexo C (de la norma).
Salida	Una lista de las amenazas con la identificación del tipo y el origen de la amenaza.

Tabla 19. Identificación de los controles existentes **[6]**

8. VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN	
8.2 ANÁLISIS DEL RIESGO	
8.2.1 Identificación del riesgo	
8.2.1.4 Identificación de los controles existentes	
Entrada	Documentación de los controles, planes para la implementación del tratamiento del riesgo.
Acción	Se deberían identificar los controles existentes y los planificados.
Guía para la implementación	Se debería realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo en la duplicación de los controles. Además, mientras se identifican los controles existentes es recomendable hacer una verificación para garantizar que los controles funcionan correctamente - una referencia a los reportes de auditoría del SGSI ya existente debería limitar el tiempo que tarda esta labor. Si el control no funciona como se espera, puede causar vulnerabilidades. Es recomendable tomar en consideración la situación en la que el control seleccionado (o la estrategia) falla en su funcionamiento y, por lo tanto, se requieren controles complementarios para tratar de manera eficaz el riesgo identificado. En un SGSI, de acuerdo con ISO/IEC 27001, se tiene como soporte la revisión de la eficacia del control. Una forma de estimar el efecto del control es ver la manera en que reduce la probabilidad de ocurrencia de la amenaza y la facilidad de explotar la vulnerabilidad, o el impacto del incidente. Las revisiones por parte de la dirección y los reportes de auditoría también suministran información acerca de la eficacia de los controles existentes. Los controles que se planifican para implementar de acuerdo con los planes de implementación del tratamiento del riesgo, se deberían considerar en la misma forma que aquellos ya implementados. Un control existente o planificado se podría identificar como ineficaz, insuficiente o injustificado. Si es injustificado o insuficiente, se debería revisar el control para determinar si se debe eliminar, reemplazar por otro más adecuado o si debería permanecer, por ejemplo, por razones de costos. Para la identificación de los controles existentes o planificados, las siguientes actividades pueden ser útiles: • Revisión de los documentos que contengan información sobre los controles (por ejemplo, los planes de implementación del tratamiento del riesgo). Si los procesos de la gestión de la seguridad de la información están bien documentados, todos los controles existentes o planificados y el estado de su implementación deberían estar disponibles; • Verificación con las personas responsables de la seguridad de la información (por ejemplo, el funcionario a cargo de la seguridad de la información y el funcionario a cargo de la seguridad del sistema de información, el administrador de la instalación o el director de operaciones) y los usuarios, en cuanto a qué controles están realmente implementados para el proceso de información o el sistema de información que se considera; • Efectuar una revisión en el sitio de los controles físicos, comparando aquellos implementados con la lista de los controles que deberían estar, y verificando aquellos implementados con respecto a si funcionan correctamente y de manera eficaz, o; • Revisión de los resultados de las auditorías internas.
Salida	Una lista de todos los controles existentes y planificados, su estado de implementación y utilización.

Tabla 20. Identificación de las vulnerabilidades **[6]**

8. VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN	
8.2 ANÁLISIS DEL RIESGO	
8.2.1 Identificación del riesgo	
8.2.1.5 Identificación de las vulnerabilidades	
Entrada	Lista de las amenazas conocidas, lista de los activos y los controles existentes.
Acción	Se deberían identificar las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos o la organización (se relaciona con ISO/IEC 27001, numeral 4.2.1 d) 3)).
Guía para la implementación	Se pueden identificar vulnerabilidades en las siguientes áreas: • Organización; • Procesos y procedimientos; • Rutinas de gestión; • Personal; • Ambiente físico; • Configuración del sistema de información; • Hardware, software o equipo de comunicaciones; • Dependencia de partes externas. La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza correspondiente puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla para determinar los cambios. Conviene anotar que un control implementado de manera incorrecta o que funciona mal, o un control que se utiliza de modo incorrecto podrían por sí solo constituir una vulnerabilidad. Un control puede ser eficaz o ineficaz dependiendo del ambiente en el cual funciona. Por el contrario, una amenaza que no tiene una vulnerabilidad correspondiente puede no resultar en un riesgo. Las vulnerabilidades pueden estar relacionadas con las propiedades de los activos que se pueden usar de una manera, o para un propósito, diferente del previsto cuando se adquirió o se elaboró el activo. Las vulnerabilidades que se originan desde fuentes diferentes se deben considerar, por ejemplo, aquellas intrínsecas o extrínsecas al activo. Ejemplos de vulnerabilidades y métodos para la valoración de la vulnerabilidad se pueden encontrar en el Anexo D (de la norma).
Salida	Una lista de las vulnerabilidades con relación a los activos, las amenazas y los controles; una lista de las vulnerabilidades que no se relacionen con ninguna amenaza identificada para revisión.

Tabla 21. Identificación de las consecuencias **[6]**

8. VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN	
8.2 ANÁLISIS DEL RIESGO	
8.2.1 Identificación del riesgo	
8.2.1.6 Identificación de las consecuencias	
Entrada	Una lista de los activos y una lista de los procesos del negocio, una lista de las amenazas y las vulnerabilidades, cuando corresponda, con respecto a los activos y su pertinencia.
Acción	Se deberían identificar las consecuencias que pueden tener las pérdidas de confidencialidad, integridad y disponibilidad de los activos (véase la norma ISO/IEC 27001, 4.2.1 d) 4)).
Guía para la implementación	Una consecuencia puede ser la pérdida de la eficacia, condiciones adversas de operación, pérdida del negocio, reputación, daño, etc. Esta actividad identifica los daños o las consecuencias para la organización que podrían ser causadas por un escenario de incidente. Un escenario de incidente es la descripción de una amenaza que explota una vulnerabilidad determinada o un conjunto de vulnerabilidades en un incidente de seguridad de la información (véase la norma ISO/IEC 27002, sección 13). El impacto de los escenarios de incidente se determina tomando en consideración los criterios del impacto que se definen durante la actividad de establecimiento del contexto. Puede afectar a uno o más activos o a una parte de un activo. De este modo, los activos pueden tener valores asignados tanto para su costo financiero como por las consecuencias en el negocio, si se deterioran o se ven comprometidos. Las consecuencias pueden ser de naturaleza temporal o permanente como es el caso de la destrucción de un activo. NOTA La norma ISO/IEC 27001 describe la ocurrencia de escenarios de incidente como "fallas de la seguridad". Las organizaciones deberían identificar las consecuencias operativas de los escenarios de incidentes en términos de (pero no limitarse a): • Tiempo de investigación y reparación; • Pérdida de tiempo (trabajo); • Pérdida de oportunidad; • Salud y seguridad; • Costo financiero de las habilidades específicas para reparar el daño; • Imagen, reputación y buen nombre. Detalles sobre la valoración de las vulnerabilidades críticas se pueden encontrar en el literal B.3 (de la norma), Valoración del impacto.
Salida	Una lista de los escenarios de incidente con sus consecuencias relacionadas con los activos y los procesos del negocio.

2.3.1.2 Valoración de riesgos

Tabla 22. Estimación del riesgo **[6]**

8. VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN	
8.2 ANÁLISIS DEL RIESGO	
8.2.2 Estimación del riesgo	
8.2.2.1 Metodologías para la estimación del riesgo	
	A continuación se describen los detalles de las metodologías para la estimación: a) Estimación cualitativa: La estimación cualitativa utiliza una escala de atributos calificativos para describir la magnitud de las consecuencias potenciales (por ejemplo, alta, intermedia y baja) y la probabilidad de que ocurran dichas consecuencias. Una ventaja de la estimación cualitativa es su facilidad de comprensión por parte de todo el personal pertinente, mientras que una desventaja es la dependencia en la selección subjetiva de la escala. Estas escalas se pueden adaptar o ajustar para satisfacer las circunstancias y se pueden utilizar descripciones diferentes para riesgos diferentes. La estimación cualitativa se puede utilizar: • Como una actividad de tamizado inicial para identificar los riesgos que requieren un análisis más detallado; • Cuando este tipo de análisis es adecuado para tomar decisiones; • Cuando los datos numéricos o los recursos no son adecuados para una estimación cuantitativa. El análisis cualitativo debería utilizar información con base en hechos y datos, cuando estén disponibles. b) Estimación cuantitativa: La estimación cuantitativa utiliza una escala con valores numéricos (a diferencia de las escalas descriptivas utilizadas en la estimación cualitativa) tanto para las consecuencias como para la probabilidad, utilizando datos provenientes de varias fuentes. La calidad del análisis depende de lo completos y exactos que sean los valores numéricos, y de la validez de los modelos utilizados. En la mayoría de los casos, la estimación cuantitativa utiliza datos históricos sobre los incidentes, dando como ventaja que ésta pueda relacionarse directamente con los objetivos de seguridad de la información y los intereses de la organización. Una desventaja es la falta de tales datos sobre riesgos nuevos o debilidades en la seguridad de la información. Una desventaja del enfoque cuantitativo se puede presentar cuando no se dispone de datos basados en los hechos que se puedan auditar, creando así una ilusión del valor y la exactitud de la valoración del riesgo. La forma en la cual se expresan las consecuencias y la probabilidad, y las formas en las cuales se combinan para proveer el nivel del riesgo varían de acuerdo con el tipo de riesgo y el propósito para el cual se va a utilizar la salida de la valoración del riesgo. La incertidumbre y la variabilidad tanto de las consecuencias como de la probabilidad se deberían ser consideradas en el análisis y comunicarse de manera eficaz.

Tabla 22. Estimación del riesgo **[6]** (Continuación)

8. VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN	
8.2 ANÁLISIS DEL RIESGO	
8.2.2 Estimación del riesgo	
8.2.2.2 Evaluación de las consecuencias	
Entrada	Una lista de los escenarios de incidentes pertinentes, que incluya la identificación de las amenazas, las vulnerabilidades, los activos afectados, las consecuencias para los activos y los procesos del negocio.
Acción	Se debería evaluar el impacto en el negocio de la organización que pueda resultar de incidentes posibles o reales en la seguridad de la información, teniendo en cuenta las consecuencias de una brecha en la seguridad de la información, por ejemplo la pérdida de confidencialidad, integridad o disponibilidad de los activos (se relaciona con ISO/IEC 27001, numeral 4.2.1 e) 1)).
Guía para la implementación	Después de identificar todos los activos bajo revisión, se deberían tener en cuenta los valores asignados a estos activos en la evaluación de las consecuencias. El valor del impacto del negocio se puede expresar de manera cualitativa y cuantitativa, pero cualquier método para asignar valor monetario en general puede suministrar más información para la toma de decisiones y, por tanto, facilitar un proceso más eficiente de toma de decisiones. La valoración de activos empieza con la clasificación de los activos de acuerdo con su criticidad, en términos de la importancia de los activos para cumplir los objetivos de negocio de la organización. La valoración se determina entonces utilizando dos medidas: • El valor de reemplazo del activo: el costo de la limpieza de recuperación y de reemplazo de la información (si es posible); • Las consecuencias para el negocio por la pérdida o compromiso de los activos, tales como consecuencias adversas potenciales para el negocio y/o consecuencias legales o reglamentarias por la divulgación, modificación, no disponibilidad y/o destrucción de la información, y otros activos de información. Esta valoración se puede determinar a partir del análisis del impacto del negocio. El valor, determinado por las consecuencias para el negocio, es en general significativamente superior al simple costo del reemplazo, dependiendo de la importancia del activo para la organización en el cumplimiento de los objetivos del negocio La valoración de activos es un factor clave en la evaluación del impacto de un escenario de incidente, porque el incidente puede afectar a más de un activo (por ejemplo activos independientes) o únicamente una parte de un activo. Diferentes amenazas y vulnerabilidades tendrán impactos diferentes en los activos, por ejemplo la pérdida de confidencialidad, integridad o disponibilidad. La evaluación de las consecuencias, por tanto, se relaciona con la valoración de activos con base en el análisis del impacto en el negocio. • Las consecuencias del impacto del negocio se pueden determinar mediante el modelado de los resultados de un evento o grupo de eventos, o mediante la extrapolación a partir de estudios experimentales o datos anteriores. • Las consecuencias se pueden expresar en términos de criterios monetarios, técnicos o del impacto humano, u otros criterios pertinentes para la organización. En algunos casos, se requiere más que un valor numérico para especificar las consecuencias para diferentes tiempos, lugares, grupos o situaciones. • Las consecuencias en el tiempo y las finanzas se deberían medir con el mismo enfoque utilizado para la probabilidad de amenaza y vulnerabilidad. Se debe mantener la consistencia en el enfoque cuantitativo o cualitativo. Mayor información tanto de la valoración de activos como de la evaluación del impacto se puede obtener en el Anexo B (de la norma).

Tabla 22. Estimación del riesgo **[6]** (Continuación)

8. VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN	
8.2 ANÁLISIS DEL RIESGO	
8.2.2 Estimación del riesgo	
8.2.2.2 Evaluación de las consecuencias	
Salida	Una lista de las consecuencias evaluadas de un escenario de incidente, expresadas con respecto a los activos y los criterios del impacto.

Tabla 23. Evaluación de la probabilidad de incidentes **[6]**

8. VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN	
8.2 ANÁLISIS DEL RIESGO	
8.2.2 Estimación del riesgo	
8.2.2.3 Evaluación de la probabilidad de incidentes	
Entrada	Una lista de los escenarios de incidentes pertinentes, que incluya la identificación de las amenazas, los activos afectados, las vulnerabilidades explotadas y las consecuencias para los activos y los procesos del negocio. Además, listas de todos los controles existentes y planificados, su eficacia, implementación y estado de utilización.
Acción	Se debería evaluar la probabilidad de los escenarios de incidente (se relaciona con ISO/IEC 27001, numeral 4.2.1 e) 2)).
Guía para la implementación	Después de identificar los escenarios de incidentes, es necesario evaluar la probabilidad de cada escenario y el impacto de que ocurra, utilizando técnicas de estimación cualitativas o cuantitativas. Se deberían tomar en consideración la frecuencia con la que ocurren las amenazas y la facilidad con que las vulnerabilidades pueden ser explotadas, teniendo en cuenta: • La experiencia y las estadísticas aplicables para la probabilidad de la amenaza; • Para fuentes de amenaza deliberada: la motivación y las capacidades, las cuales cambiarán con el tiempo, y los recursos disponibles para los posibles atacantes, así como la percepción de atracción y vulnerabilidad de los activos para un posible atacante; • Para fuentes de amenaza accidental: factores geográficos como proximidad a plantas químicas o de petróleo, la probabilidad de condiciones climáticas extremas, y factores que pudieran tener influencia en los errores humanos y el mal funcionamiento del equipo; • Vulnerabilidades, tanto individuales como en conjunto; • Controles existentes y qué tan eficazmente reducen las vulnerabilidades. Por ejemplo, un sistema información puede tener una vulnerabilidad para las amenazas de enmascaramiento de la identidad del usuario y mala utilización de los recursos. La vulnerabilidad de enmascaramiento de la identidad del usuario puede ser alta debido a la falta de autentificación del usuario. Por otra parte, la probabilidad de mala utilización de los recursos puede ser baja, a pesar de la falta de autentificación del usuario, dado que las formas para el mal uso de los recursos son limitadas. Dependiendo de la necesidad de exactitud, los activos se podrían agrupar o podría ser necesario dividir los activos en sus elementos y relacionar los escenarios con los elementos. Por ejemplo, a través de lugares geográficos, la naturaleza de las amenazas para los mismos tipos de activos puede cambiar, o puede variar la eficacia de los controles existentes.
Salida	Probabilidad de los escenarios de incidente (cuantitativa o cualitativa).

Tabla 24. Nivel de estimación del riesgo **[6]**

8. VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN	
8.2 ANÁLISIS DEL RIESGO	
8.2.2 Estimación del riesgo	
8.2.2. 4 Nivel de estimación del riesgo	
Entrada	Una lista de los escenarios de incidente con sus consecuencias relacionadas con los activos y los procesos del negocio, y su probabilidad (cuantitativa o cuantitativa).
Acción	Se deberían estimar el nivel de riesgo para todos los escenarios de incidente pertinentes (se relaciona con ISO/IEC 27001, numeral 4.2.1 e) 4).
Guía para la implementación	La estimación del riesgo asigna valores a la probabilidad y las consecuencias de un riesgo. Estos valores pueden ser cuantitativos o cualitativos. La estimación del riesgo se basa en las consecuencias evaluadas y la probabilidad. Además, la estimación puede considerar el beneficio de los costos, los intereses de las partes involucradas y otras variables, según correspondan para la evaluación del riesgo. El riesgo estimado es una combinación de la probabilidad de un escenario de incidente y sus consecuencias. Ejemplos de diferentes métodos o enfoques para la estimación del riesgo en la seguridad de la información se pueden encontrar en el Anexo E (de la norma).
Salida	Una lista de los riesgos con niveles de valor asignado.

Tabla 25. Evaluación del riesgo **[6]**

8. VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN	
8.3 EVALUACIÓN DEL RIESGO	
Entrada	Una lista de los riesgos con niveles de valor asignado y criterios para la evaluación del riesgo.
Acción	Se deberían comparar los niveles de riesgo frente a los criterios para la evaluación del riesgo y sus criterios de aceptación[12].

[12] Se relaciona con ISO/IEC 27001, numeral 4.2.1

Tabla25. Evaluación del riesgo **[6]** (Continuación)

8. VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN	
8.3 EVALUACIÓN DEL RIESGO	
Guía para la implementación	La naturaleza de las decisiones pertinentes para la evaluación del riesgo y los criterios de evaluación del riesgo que se utilizarán para tomar dichas decisiones, deben haber sido determinados durante el establecimiento del contexto. Estas decisiones y el contexto se deberían revisar con mayor detalle en esta etapa cuando se sabe más acerca de los riesgos particulares identificados. Con el fin de evaluar los riesgos, las organizaciones deberían comparar los riesgos estimados (utilizando métodos o enfoques seleccionados, tal como se discute en el Anexo E (de la norma)) con los criterios de evaluación del riesgo que se definieron durante el establecimiento del contexto. Los criterios de evaluación del riesgo utilizados para tomar decisiones deberían ser consistentes con el contexto definido para la gestión del riesgo en la seguridad de la información externa e interna y deberían tomar en consideración los objetivos de la organización, los puntos de vista de las partes interesadas, etc. Las decisiones, tal como se toman en la actividad de evaluación del riesgo, se basan principalmente en el nivel aceptable de riesgo. Sin embargo, también es recomendable considerar las consecuencias, la probabilidad y el grado de confianza en la identificación y el análisis del riesgo. La agrupación de múltiples riesgos bajos o medios puede dar como resultado riesgos globales mucho más altos y es necesario tratarlos según corresponda. Las consideraciones deberían incluir: • Propiedades de la seguridad de la información: si un criterio no es pertinente para la organización (por ejemplo la pérdida de confidencialidad), entonces todos los riesgos que tienen impacto sobre este criterio pueden no ser pertinentes; • La importancia de los procesos del negocio o de la actividad sustentada por un activo particular o un conjunto de activos: si se determina que el proceso tiene importancia baja, los riesgos asociados con él deberían tener una consideración más baja que los riesgos que tienen impacto en procesos o actividades más importantes. La evaluación del riesgo utiliza la comprensión del riesgo que se obtiene mediante el análisis del riesgo para tomar decisiones sobre acciones futuras. Las decisiones deberían incluir: • Si se debería realizar una actividad; • Prioridades para el tratamiento de los riesgos considerando los valores estimados de ellos.
Salida	Una lista de los riesgos con prioridad de acuerdo con los criterios de evaluación del riesgo, con relación a los escenarios de incidente que llevan a tales riesgos.

2.3.2 Propuesta COBIT

Como se muestra en la sección anterior, COBIT[10] dedica el proceso PO9 a la evaluación del riesgo estableciendo seis objetivos de control, aunque sin ahondar en el cómo de la implementación del proceso y el logro de estos objetivos dada su orientación enfocada fuertemente en el control y menos en la ejecución.

2.3.2.1 Identificación de riesgos

La identificación de los riesgos se muestra en la Tabla 26.

Tabla 26. P09. Evaluar y Administrar los Riesgos de TI – Identificación **[10]**[13]

P09. Evaluar y Administrar los Riesgos de TI.		
Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los Interesados (Stakeholders) y se debe expresar en términos financieros, para permitirles alinear los riesgos a un nivel aceptable de tolerancia**.**		
PO9.1	**Marco de Trabajo de Administración de Riesgos**	Establecer un marco de trabajo de administración de riesgos de TI que esté alineado al marco de trabajo de administración de riesgos de la organización.
PO9.2	**Establecimiento del Contexto del Riesgo**	Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos.
PO9.3	**Identificación de Eventos**	Identificar eventos (una amenaza importante y realista que explota una vulnerabilidad aplicable y significativa) con un impacto potencial negativo sobre las metas o las operaciones de la empresa, incluyendo aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto y mantener esta información. Registrar y mantener los riesgos relevantes en un registro de riesgos.

2.3.2.2 Valoración de riesgos

La valoración de los riesgos se muestra en la Tabla 27.

[13] Creada con base en la información recopilada del documento referenciado.

Tabla 27. P09. Evaluar y Administrar los Riesgos de TI – valoración **[10]**[14]

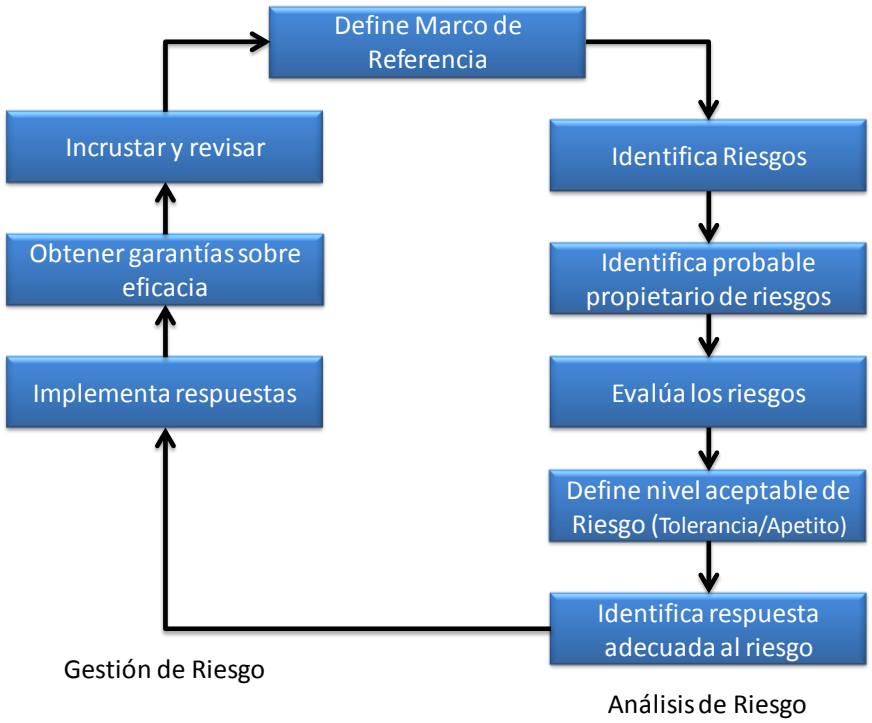
P09. Evaluar y Administrar los Riesgos de TI.		
Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los Interesados (Stakeholders) y se debe expresar en términos financieros, para permitirles alinear los riesgos a un nivel aceptable de tolerancia**.**		
PO9.4	**Evaluación de Riesgos de TI**	Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.
PO9.5	**Respuesta a los Riesgos**	Desarrollar y mantener un proceso de respuesta a riesgos diseñado para asegurar que controles efectivos en costo mitigan la exposición en forma continua. El proceso de respuesta a riesgos debe identificar estrategias tales como evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos.
PO9.6	**Mantenimiento y Monitoreo de un Plan de Acción de Riesgos**	Priorizar y planear las actividades de control a todos los niveles para implementar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Obtener la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas están a cargo del dueño (s) de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.

2.3.3 Propuesta ITIL

ITIL [12] define riesgo como: "**Riesgo** es un resultado incierto, o en otras palabras, una oportunidad positiva o una amenaza negativa". Y define que la tarea de la gestión de riesgo es asegurar que la organización hace uso, de una manera costo-efectiva, de un marco de referencia de riesgo que consiste de un conjunto de pasos bien definidos, como se muestra en la Figura 17.

[14] Creada con base en la información recopilada del documento referenciado.

Figura 17. Marco de referencia genérico para gestión de riesgo **[12]**



El objetivo de este ciclo es soportar una mejor toma de decisión a través del uso de un buen entendimiento de los riesgos y su probable impacto y platea dos fases: análisis de riesgos y gestión de riesgos.

Análisis de Riesgos: Tiene que ver con la recopilación de información sobre la exposición a riesgos para que la organización tome las decisiones correctas y supervise los riesgos en la forma apropiada.

Gestión de Riesgos: Asegura que haya procesos que se centran en la vigilancia de los riesgos, que haya información actualizada y fiable sobre los riesgos, que se aplica el balance de control adecuado para los riesgos remanentes, y que la toma de decisiones es apoyada por un marco de análisis y evaluación de riesgos.

Aunque ITIL indica que el análisis de riesgos y gestión de riesgos deben aplicarse a todo el ciclo de servicio y catálogo de servicios a fin de identificar, detener y mitigar los riesgos dentro de las fases del ciclo de vida, para efectos del modelo unificado a proponer sólo se evaluará su propuesta de análisis de riesgos.

2.3.3.1 Identificación de riesgos

ITIL a través de sus procesos de Gestión de Configuración y Gestión de Activos define las características de los activos para registrarlos en la base de datos de configuración (CMDB, por su sigla en inglés) y sugiere los siguientes atributos de seguridad para cada ítem de configuración.

- Confidencialidad
- Integridad / Confiabilidad
- Disponibilidad / Continuidad

Sugiere adicionalmente, desde el proceso de Control de Cambios que se realice un análisis de riesgos, sin especificar cómo hacerlo, donde se evalúe:

- Impacto sobre los procesos de negocio (bajo la responsabilidad del cliente) - dependencias.
- Impacto sobre la infraestructura de TI como un todo – Vulnerabilidades.
- Cuál es el nivel de seguridad requerido – Requisitos de nivel de servicio para seguridad.

ITIL reconoce las siguientes clases de riesgos:

Riesgos de contratos: (un contrato incluye acuerdos formal y legalmente vinculantes entre el negocio y los proveedores de servicios) – Los riesgos hagan imposible que el proveedor satisfaga los acuerdos contractuales, son riesgos estratégicos, porque no sólo amenazan la producción actual, sino también dañan la confianza para futuras interacciones. El impacto de los riesgos del contrato, los peligros subyacentes y sus debilidades no puede limitarse a una función específica del proceso. El cliente no hace distinción del origen de los riesgos. La coordinación durante todo el ciclo es necesaria a fin de administrar eficazmente los riesgos.

Riesgos de diseño: Los clientes esperan servicios para tener un impacto específico en el rendimiento de sus activos, lo que es una utilidad desde su perspectiva. Siempre existe el riesgo que los servicios alcancen resultados no deseados. Esto es un riesgo de rendimiento. Un pobre rendimiento generalmente es el resultado de un mal diseño.

Riesgos operacionales: Cada organización se ocupa de los riesgos operacionales. Visto desde una perspectiva de gestión de servicio, existen dos tipos de distinguir: los riesgos para las unidades de negocio y los riesgos para las unidades de servicio.

Riesgos de mercado: La gestión eficaz de servicio ayuda a reducir los riesgos competitivos mediante el aumento de la escala y el alcance de la demanda de un catálogo de servicios. Otro enfoque es modificar el contenido del catálogo de servicios para que los clientes puedan encontrar la profundidad y amplitud que están buscando. Pueden reducir los riesgos de mercado a través de:

- **Diferenciación**: desde la perspectiva del cliente, los activos que son escasos y complementarios son interesantes. Los proveedores de servicios pueden concentrarse en proporcionar activos importantes que no hayan sido proporcionados por terceros. Los mercados desatendidos y carentes de servicios ofrecen oportunidades atractivas.
- **Consolidación**: la consolidación de la demanda reduce los riesgos financieros para proveedores de servicios, así como los riesgos operacionales para el cliente.

2.3.3.2 Valoración de riesgos

En el capítulo 10.4 Gestión de Disponibilidad de [12], se define que la gestión de disponibilidad supervisa, mide, analiza e informa sobre los siguientes aspectos:

- **Disponibilidad**: El servicio o la capacidad del componente para funcionar según lo acordado con el cliente.
- **Confiabilidad**: El tiempo de que un servicio o componente puede funcionar sin interrupción conforme a los acuerdos.
- **Mantenibilidad**: La velocidad y la eficacia de la reparación de un componente o servicio después de una falla; en otras palabras, cuán rápido se reanudará el funcionamiento normal.
- **Servicio**: La capacidad de un proveedor externo para cumplir con los acuerdos de contrato.

Y establece que para asegurar estos aspectos, desde la fase de diseño del servicio se debe considerar al análisis y gestión de riesgo como una de sus actividades proactivas.

Más adelante en el capítulo 10.5 Gestión de continuidad del servicio de TI, define que el propósito de gestión de continuidad servicio de TI (ITSCM, por su sigla en inglés) es apoyar la continuidad del negocio al asegurar que las instalaciones de TI requeridas (sistemas informáticos, redes, etc.) puedan reanudarse dentro de los plazos acordados, con los siguientes objetivos:

- Mantener un conjunto de planes de continuidad y recuperación.
- Realizar regularmente análisis de impacto de negocios.
- Ejecutar ejercicios de gestión y estimaciones de riesgo.

- Asesorar a otras unidades de negocio sobre todas las cuestiones relacionadas con la recuperación y continuidad.
- Asegurar que los mecanismos necesarios de continuidad y recuperación estén listos para su uso.
- Investigar el impacto de los cambios en los planes de continuidad y recuperación.
- Aplicar medidas proactivas para mejorar la disponibilidad de servicios.
- Negociar acuerdos con los proveedores en relación con la capacidad de recuperación requeridos.

Para lo que ITSCM debe realizar:

- Acuerdos sobre alcance de ITSCM.
- Un análisis de impacto de negocio para calificar el impacto de calamidades.
- Análisis e identificación de riesgos (incluyendo medidas necesarias).
- La creación de una estrategia global de ITSCM basada en la gestión de continuidad de negocio.
- La creación de planes de continuidad del negocio.
- Pruebas de los planes.
- Mantenimiento continúo de los planes.

Para esto define dentro de las actividades, métodos y técnicas de este servicio unos requisitos y estrategias. Los requisitos incluyen la ejecución de un análisis de impacto de negocio y estimación riesgo, de la siguiente manera:

Requisito 2: Estimación de riesgo - Existen diversos métodos y análisis de riesgo. El análisis de riesgo es una evaluación de los riesgos que pueden producirse. La administración de riesgos identifica la respuesta y las contramedidas que pueden adoptarse. Puede utilizarse un método estándar como gestión de riesgos (MoR) para investigar y gestionar los riesgos. Este método consiste en:

- Principios de MoR.
- Enfoque MoR (organización del enfoque).
- Procesos de MoR (identificación, evaluación, planificación, implementación).
- Incrustación y revisión de MoR.
- Comunicación (suministro de información adecuada y actualizada).

2.3.4 Propuesta O-ISM3

2.3.4.1 Identificación de riesgos

Como se mostró en la sección de identificación y valoración de activos, O-ISM3 [13] “evita conceptos tradicionales de seguridad, tales como la confidencialidad, disponibilidad e integridad, porque hay una tentación para usarlas como taquigrafía, y que lleva a malentendidos. Mientras que los objetivos de seguridad son necesariamente específicos y detallados, el uso de términos operacionales contribuye a eliminar la ambigüedad y el potencial de malentendido” y plantea desde su introducción que la seguridad de la información es necesaria para proteger los sistemas de riesgos o amenazas que potencialmente puedan hacer daño y que para ello generalmente se establecen tres áreas:

- **Gestión de Riesgo:** Para identificar y estimar los niveles de exposición a la probabilidad de pérdida, para que los gerentes de negocios pueden tomar decisiones de negocios respecto a cómo administrar los riesgos de pérdida al aceptar el riesgo o mitigarlo, ya sea a través de invertir en medidas adecuadas de protección internas estimadas como suficientes para disminuir la pérdida potencial a un nivel aceptable, o invirtiendo en indemnización externa. Aquí las decisiones de los gerentes de negocios son establecidas como su política de seguridad, que describe cómo administrar su seguridad de TI.
- **Controles de Seguridad:** Una empresa crea y mantiene una política corporativa sobre las metas y objetivos que impulsan sus operaciones, y como parte de sus operaciones de TI-dependientes utiliza los resultados de la evaluación de riesgo para formular una política de seguridad de TI que apoya y aplica a su política corporativa para proteger sus activos (principalmente su activo más valioso: datos) y asegurar que sus operaciones sean tan seguras como deben ser para el nivel de protección requerido.
- **Gestión de Seguridad:** Para Apoyar la selección, el mantenimiento y la política de seguridad general de los controles de seguridad implementados en una empresa. En nuestro mundo cada vez más conectado también es un impulsor de negocios sólido para asociarse con otras organizaciones, proveedores, clientes y trabajadores móviles, y esto exige establecer arreglos de seguridad acordados mutuamente para compartir datos y aplicaciones. Otros aspectos de gestión de seguridad incluyen auditoría y registro y cumplimiento de normas.

2.3.4.2 Valoración de riesgos

Por ser independiente a la tecnología O-ISM3 no propone una técnica en particular e indica que utilizar cualquier técnica de protección “es adecuado para alcanzar

los objetivos del proceso y sus salidas. Así como los procesos de arquitectura de empresa definen la operación deseada de los sistemas de información, los procesos de gestión de seguridad definen métricas operacionales y sus variaciones permisibles".

O-ISM3 establece toda la estrategia de gestión de riesgo desde la definición del sistema de gestión a través del proceso GP-3, como se muestra en la Tabla 15. Aquí sugiere utilizar otras metodologías relacionadas para evaluación de riesgos, evaluación de amenazas, evaluación de la vulnerabilidad como AS/NZS 4360, CRAMM, EBIOS, ISO/IEC 27005:2008, MAP MAGERIT, CLUSIF MEHARI, OCTAVE, NIST SP 800-30 ó el estándar técnico de taxonomía de riesgo de *Open Group*.

En el mismo sentido en [13], se plantea como una de las características claves de O-ISM3 que "mientras muchos enfoques de gestión de seguridad de información consideran evaluación del riesgo como una primera etapa necesaria y como tal O-ISM3 puede utilizarse así como cualquier otra norma en este campo, no exige un enfoque basado en la evaluación de riesgo. En algunos casos, una empresa puede decidir que no es necesario hacer una evaluación del riesgo para encontrar que necesita un control de seguridad. Por ejemplo, los controles pueden elegirse en función de:

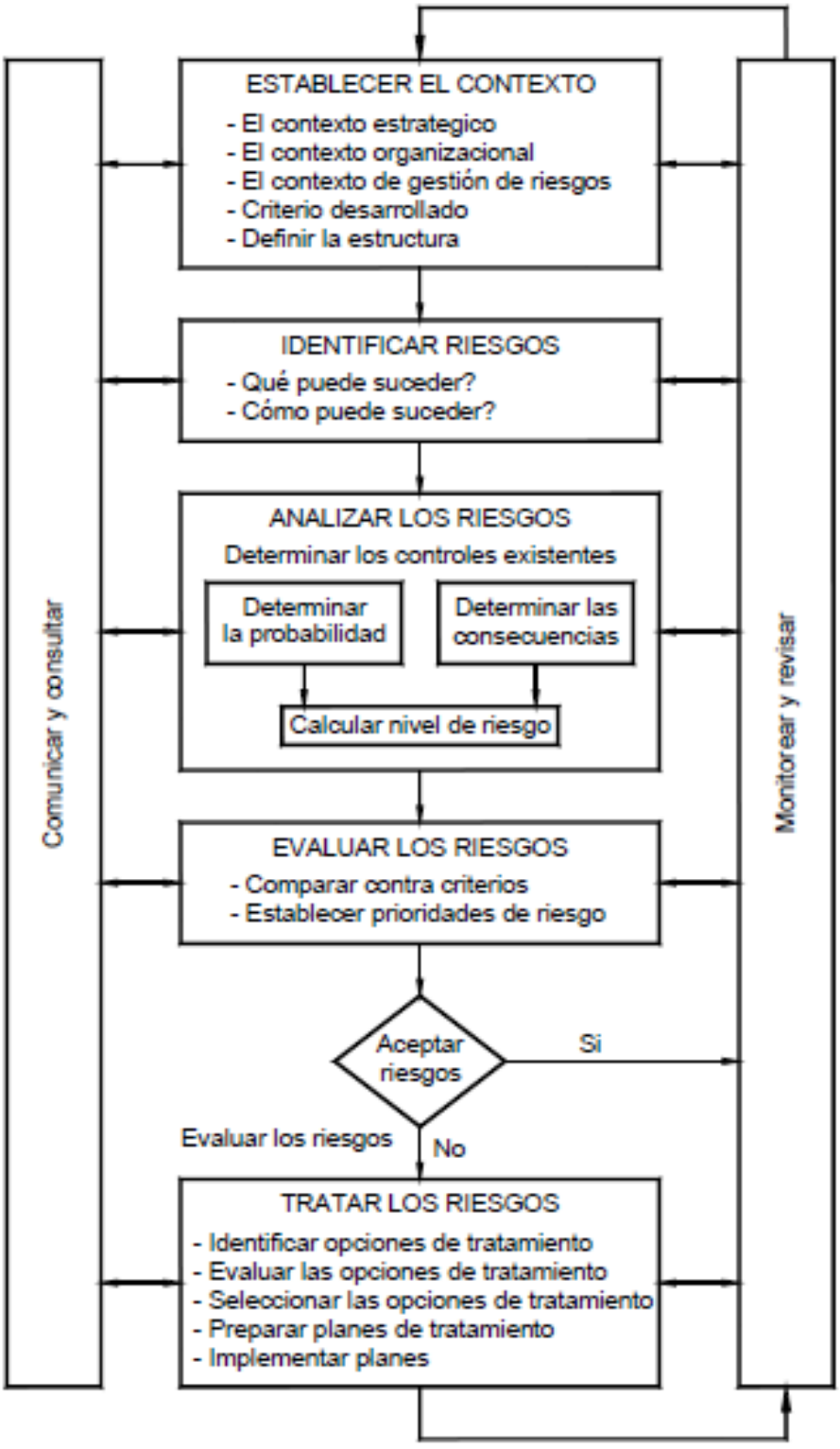
- Sentido común.
- Mejores prácticas (contraseñas)
- Aprendiendo de incidentes (tal vez un mejor *firewall* o antivirus)
- Un análisis centrado específicamente en vulnerabilidad o amenazas.
- Requisitos de cliente (No deseo que los usuarios del proyecto A tengan acceso a datos pertenecientes a mi proyecto).

El enfoque de O-ISM3 ofrece a las organizaciones la flexibilidad de elegir cualquier subconjunto de sus procesos de seguridad de la información basada en varios criterios."

2.3.5 Propuesta NTC 5254

Esta norma técnica Colombiana [15] es una adopción modificada (MOD), de la AS/NZ 4360:1999 *Risk Management* y tiene como objetivo proporcionar un marco genérico para establecer el contexto, la identificación, el análisis, la evaluación, el tratamiento, el seguimiento y la comunicación del riesgo. En este documento nos centraremos en la propuesta para la identificación, el análisis y evaluación del riesgo, según los pasos propuestos por la norma en la Figura 18.

Figura 18. Proceso general de gestión del riesgo según **[15]**



Identificar riesgos: Identificar qué, por qué y cómo pueden surgir elementos como base para análisis posterior.

Analizar riesgos: Determinar los controles existentes y analizar los riesgos en términos de **consecuencia** y **posibilidad** en el contexto de estos controles. El análisis debe considerar la gama de consecuencias potenciales y la posibilidad de que éstas ocurran. Se pueden combinar la consecuencia y la posibilidad para producir un nivel estimado de riesgo.

Evaluar los riesgos: Comparar los niveles estimados de riesgo, contra los criterios pre-establecidos. Esto posibilita que los riesgos sean clasificados de modo que se identifiquen prioridades de gestión. Si los niveles de riesgo establecido son bajos, entonces los riesgos pueden encajar en una categoría aceptable, y es posible que no se requiera tratamiento.

Los demás elementos del proceso propuesto se dejan a consideración para otro estudio posterior.

2.3.5.1 Identificación del Riesgo.

En este paso se busca identificar los riesgos que se van a gestionar. La identificación debe incluir todos los riesgos, sea que estén o no bajo el control de la organización.

2.3.5.1.1 ¿Qué puede suceder?

El objetivo es generar una lista global de eventos que podrían afectar cada elemento del sistema o proceso bajo gestión. Para el caso de estudio corresponde a los activos previamente identificados y valorados.

Para la identificación de las fuentes de riesgo la norma [15] en su anexo D propone las siguientes fuentes genéricas de riesgo:

a) Relaciones legales y comerciales al interior de la organización y con otras organizaciones, por ejemplo proveedores, subcontratistas, arrendatarios.;
b) Circunstancias económicas y de mercado, organizacionales, nacionales, e internacionales, así como factores que contribuyen a estas circunstancias, por ejemplo tasas de cambio;
c) Comportamiento humano de quienes están involucrados en la organización y de quienes no lo están;
d) Eventos naturales;

e) Circunstancias políticas: cambios legislativos y factores sociales que pueden influenciar otras fuentes de riesgo;
f) Tecnología y asuntos técnicos, tanto internos como externos, de la organización;
g) Actividades de gestión y control;
h) Actividades individuales.

Y complementa con otras clasificaciones como subconjuntos de las anteriores:

a) Enfermedades, afecciones humanas, de animales y plantas;
b) Económicas: fluctuaciones del dinero, tasas de interés, participación en el mercado;
c) Medioambientales: ruido y contaminación;
d) Financiero: riesgos contractuales, fraudes, malversación de fondos y multas;
e) Humanos: disturbios, ataques, sabotajes y errores
f) Riesgos naturales: condiciones climáticas, terremotos, incendios forestales, inundaciones, plagas y Actividad volcánica;
g) Salud ocupacional y seguridad: medidas inadecuadas de seguridad, deficiente gestión de seguridad;
h) Responsabilidad de un producto: error de diseño, control de calidad por debajo de la norma, ensayos inadecuados;
i) Responsabilidad profesional: mala asesoría, error de diseño, negligencia;
j) Daños en la propiedad: incendio, terremotos, inundaciones, contaminación, errores humanos;
k) Responsabilidad pública: ingreso y egreso de público, y seguridad;
l) Seguridad: disposición del dinero, vandalismo, robo, uso ilegal de la información, entrada ilegal;
m) Tecnológica: innovación, obsolescencia, explosiones y seguridad de funcionamiento.

2.3.5.1.2 ¿Cómo puede suceder?

Una vez que se haya identificado una lista global de eventos, es necesario considerar sus posibles causas y escenarios.

2.3.5.2 Análisis del Riesgo.

La norma propone textualmente: “Los objetivos del análisis consisten en separar los riesgos aceptables menores de los mayores, y proporcionar datos que sirvan

para la evaluación y el tratamiento de riesgos. El análisis del riesgo incluye considerar las fuentes de riesgo, sus consecuencias y la posibilidad de que estas consecuencias ocurran. Se pueden identificar los factores que afectan las consecuencias y la posibilidad. El riesgo se analiza mediante la combinación de estimaciones de consecuencias y posibilidad en el contexto de las medidas de control existentes".

2.3.5.2.1 Determinación de los controles existentes.

"Se deben identificar la gestión, los sistemas técnicos y procedimientos existentes para controlar el riesgo y evaluar sus fortalezas y debilidades".

Para esto la norma propone unas herramientas que pueden resultar apropiadas, lo mismo que métodos tales como inspecciones y técnicas de control por auto-evaluación ('CAE').

2.3.5.2.2 Consecuencia y posibilidad.

"Se evalúa la magnitud de las consecuencias de un evento, si ocurriera, y la posibilidad del evento y sus consecuencias asociadas, en el contexto de los controles existentes. Las consecuencias y la posibilidad se combinan para producir un nivel de riesgo. Las consecuencias y la posibilidad se pueden determinar a partir de análisis y cálculos estadísticos. Como alternativa, cuando no hay a disposición datos del pasado, se pueden hacer estimaciones subjetivas que reflejen el grado de creencia de un individuo o grupo con respecto a la probabilidad de ocurrencia de un evento o resultado particular".

Para disminuir la subjetividad, la norma [15] sugiere recurrir a las siguientes fuentes de información:

a) Registros pasados;
b) Experiencia pertinente;
c) Práctica y experiencia industrial;
d) Literatura publicada pertinente;
e) Marketing de ensayo e investigación de mercado;
f) Experimentos y prototipos;
g) Modelos económicos, de ingeniería y otros;
h) Juicios de especialistas y expertos.

Entre las técnicas, se emplean:

I. Entrevistas estructuradas con expertos en el área de interés;

II. Empleo de grupos de expertos multidisciplinarios;
III. Evaluaciones individuales empleando cuestionarios;
IV. Uso del computador y otros modelos;
V. Uso de árboles de falla y árboles de eventos.

2.3.5.2.3 Tipos de análisis.

“El análisis puede ser cualitativo, semicuantitativo, cuantitativo, o una combinación de estos, según las circunstancias”.

a) **Análisis cualitativo**: El análisis cualitativo emplea palabras o escalas descriptivas para describir la magnitud de las consecuencias potenciales y la posibilidad de que estas consecuencias ocurran.

Como ejemplo la norma en su anexo E presenta, entre otras, la Tabla 28 y la Tabla 29.

Tabla 28. Medidas cualitativas de la consecuencia o impacto **[15]**

Nivel	Descriptor	Descripción detallada de ejemplo
1	Insignificante	Ningún daño, pérdidas financieras pequeñas
2	Menor	Tratamiento de primeros auxilios, las descargas en el sitio son contenidas inmdiatamente, medianas pérdidas financieras.
3	Moderada	Requiere tratamiento médico, las descargas en el sitio son contenidas con ayuda externa, pérdidas financieras altas.
4	Mayor	Lesiones graves, pérdida de capacidad de producción, descargas fuera del sitio sin efectos perjudiciales, pérdida financiera importante.
5	Catastrófica	Muerte, liberación de tóxicos fuera del sitio con efecto perjudicial, enorme pérdida financiera
NOTA Las medidas tomadas deberían reflejar las necesidades y naturaleza de la organización y actividades bajo estudio.		

Tabla 29. Medidas cualitativas de las posibilidades **[15]**

Nivel	Descriptor	Descripción detallada de ejemplo
A	Casi Cierto	Se espera que ocurra en la mayoría de las circunstancias.
B	Probable	Puede probablemente ocurrir en la mayoría de las circunstancias.
C	Posible	Es posible que ocurra en algunas veces.
D	Improbable	Podría ocurrir en algunas veces.
E	Raro	Puede ocurrir solamente en circunstancias excepcionales.
NOTA Las tablas necesitan ajustarse para satisfacer las necesidades individuales de la organización.		

b) **Análisis semicuantitativo**: “Se asignan valores a escalas cualitativas como las descritas anteriormente. No es obligatorio que el número asignado a cada descripción tenga una relación exacta con la magnitud real de las consecuencias o posibilidad. Los números se pueden combinar mediante cualquier fórmula de entre una variedad de ellas, siempre y cuando el sistema usado para priorización sea compatible con el sistema escogido para asignar números y combinarlos. El objetivo es producir una priorización más detallada de la que se logra generalmente en el análisis cualitativo, y no sugerir cualquier valor realista del riesgo tal como se intenta en el análisis cuantitativo”.
c) **Análisis cuantitativo**: “El análisis cuantitativo emplea valores numéricos (en lugar de las escalas descriptivas empleadas en los análisis cualitativo y semi-cuantitativo), tanto para las consecuencias como para la posibilidad a partir de datos de una variedad de fuentes (tales como aquellos a los que se hace referencia en los literales (a) a (h) del numeral 2.4.5.2.2 (de la norma)). La calidad del análisis depende de la exactitud y de la integridad de los valores numéricos empleados”.

2.3.5.3 Evaluación del Riesgo.

“La evaluación del riesgo involucra la comparación del nivel de riesgo encontrado durante el proceso de análisis contra los criterios de riesgo previamente establecidos”.

El análisis del riesgo y los criterios contra los cuales se comparan los riesgos en la evaluación del riesgo se deben considerar sobre la misma base. Por tanto, la evaluación cualitativa involucra la comparación de un nivel cualitativo del riesgo contra los criterios cualitativos; y la evaluación cuantitativa involucra la comparación del nivel numérico del riesgo, contra los criterios que pueden expresarse como un número específico, como por ejemplo un valor que indique fatalidad, frecuencia o valor monetario.

El resultado de una evaluación del riesgo es una lista priorizada de riesgos, para tomar acciones posteriores.

2.3.6 Propuesta RiskIT

RiskIT establece las mejores prácticas para que las organizaciones cuenten con un marco que les permita identificar, gobernar y administrar los riesgos asociados a su negocio. RiskIT es utilizado para ayudar a implementar el gobierno de TI y complementa a COBIT en la gestión de los riesgos.

RiskIT establece una categorización de los riesgos de TI (Figura 19) entre las cuales se observan:

• **Beneficios/riesgos de TI**: Asociados con la ausencia de las oportunidades para utilizar la tecnología, con el fin de mejorar la eficiencia o efectividad de los procesos de negocio o como un facilitador para nuevas iniciativas organizacionales.
• **Programa de TI y el riesgo de ejecución de proyectos**: Asociado con la contribución de las TI para soluciones de negocios nuevos o mejorados, por lo general en la forma o los proyectos y programas. Esto se vincula a la gestión de las inversiones de cartera (como se describe en el marco de VAL IT[15]).
• **Las operaciones de TI y el riesgo de la prestación de servicios**: asociado con todos los aspectos del desempeño de TI y servicios del sistema, que puede ocasionar la destrucción o la reducción de valor para la organización.

Observando la Figura 19 se puede concluir:

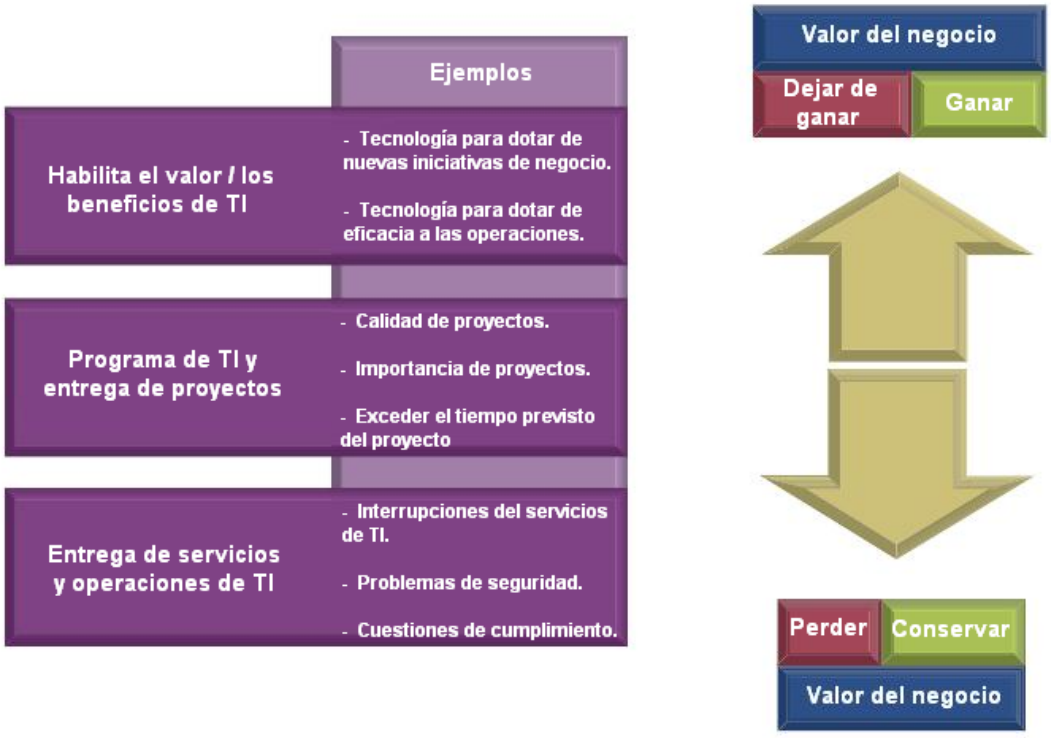
- Los riesgos de TI siempre existen estén o no detectados por la organización.
- Para todas las categorías de riesgo no existe un aspecto positivo equivalente; dado que cada decisión que se tome tiene dos dimensiones en las cuales se puede ganar (conservar) o perder (dejar de ganar) que apuntan a generar valor en la organización.

RiskIT se encarga de gestionar los riesgos de TI, pero se debe tener en cuenta que un riesgo de TI (debido a su carácter transversal) es también un riesgo del negocio (Figura 20) por lo que se concluye que este marco de trabajo está dirigido a todos los estamentos de la organización:

- Los principales ejecutivos y miembros del consejo que necesitan para establecer la dirección y seguimiento del riesgo a nivel de organización.
- Encargados de TI y de los departamentos de negocio que necesitan definir el proceso de la gestión de riesgos.
- Profesionales de la gestión de riesgos que necesitan la dirección específica en cuanto a los riesgos de TI.
- Entes externos.

[15] ValIT es otro marco de trabajo cuyo objetivo es responder a la necesidad en las organizaciones de optimizar la realización del valor de sus inversiones en TI.

Figura 19. Categorías de los riesgos de TI **[16]**



La Tabla 30 muestra la manera los beneficios o razones que pueden tener los diversos estamentos con el análisis de los riesgos.

Figura 20. Riesgos de TI en la jerarquía de riesgos **[16]**

Tabla 30. Público y ventajas del análisis de riesgos **[16]**

Papel	Beneficios de/ Razones para usar el marco de riesgos de TI
Junta y Dirección Ejecutiva	Mejor comprensión de sus responsabilidades y funciones con respecto a la gestión de riesgos de TI.
Gestores de Riesgos	Asistencia con la gestión de los riesgos de TI, de acuerdo con la organización generalmente aceptados por los principios de la gestión de riesgos.
Administrador de los riesgos Operacionales	Marco de su vinculación con los riesgos de TI, la identificación de las pérdidas operativas o el desarrollo de los principales indicadores de riesgo.
Dirección de TI	Mejor comprensión de cómo identificar y gestionar los riesgos y la forma de comunicar los riesgos a la toma de decisiones de negocios
Directores de servicios de TI	Mejora de su punto de vista sobre los riesgos relacionados con TI, los cuales deberían encajar en el conjunto global del marco de trabajo de la gestión de riesgos de IT.
Administrador de la continuidad de negocio	La alineación con la organización de gestión de riesgos (desde la evaluación de riesgo es un aspecto clave de su responsabilidad)
Administrador de seguridad de TI	Posicionamiento de los riesgos de seguridad, entre otras categorías de riesgo de IT
CFOs	Obtener una mejor visión de los riesgos relacionados con TI y sus implicaciones financieras
Oficiales del gobierno organizacional	Asistencia con su examen y la supervisión de las responsabilidades de gobierno y otras funciones de gobierno de TI.
Directores ejecutivos	La comprensión y la gestión de los riesgos es uno de los muchos riesgos de negocios, todos los cuales deben ajustarse.
Los auditores de TI	Mejor análisis de riesgo en apoyo de los planes de auditoría e informes
Reguladores	Apoyo de su evaluación de las organizaciones reguladas "enfoque de gestión de riesgos de TI
Auditores externos	Orientación adicional sobre las tecnologías relacionadas con los niveles de riesgo cuando se crea una opinión
Aseguradores	Apoyo en el establecimiento de cobertura de seguro adecuada de TI y la búsqueda de un acuerdo sobre los niveles de riesgo
Las agencias de calificación	En colaboración con aseguradores; una referencia para evaluar objetivamente y la tarifa como una organización se ocupa de los riesgos

Como los riesgos de TI afectan al negocio, la gestión de éstos se debe basar en unos principios (Figura 21, Tabla 31) que apunten a la organización.

Figura 21. Principios de los riesgos de TI **[16]**

Tabla 31. Principios de los riesgos de TI **[16]**[16]

Principios de los riesgos de TI	
La eficaz gestión de la organización de los riesgos de TI siempre se alinea con los objetivos de la organización	• El riesgo de TI es tratado como un riesgo de negocio, en contraposición a un tipo de riesgo, y el enfoque es integral y transversal; • La atención se centra en los resultados del negocio. Apoya la consecución de los objetivos del negocio y los riesgos de TI se expresan en el impacto que pueden tener en el logro de los objetivos de la organización o la estrategia. • Todo análisis de los riesgos de TI contiene una dependencia del análisis de cómo el negocio depende de la función de todas las capas subyacentes de la infraestructura de TI. • La gestión de riesgos de TI es un instrumento de negocio, no un inhibidor. El riesgo de negocio relacionado con TI es visto desde ambos ángulos: protección contra destrucción de valor y generación de valor.
El gobierno eficaz de la organización con respecto a los riesgos de TI alinea la gestión de riesgos de relacionados con TI con el riesgo organizacional en general con ERM[17]	• Los objetivos de negocio y la cantidad de riesgo que la organización está dispuesta a asumir están claramente definidos. • El proceso de toma de decisiones de la organización examina toda la gama de posibles consecuencias potenciales y oportunidades de los riesgos de TI. • El apetito de riesgo de la entidad refleja su filosofía de gestión del riesgo e influencia en la cultura y en el tipo de funcionamiento. • Los temas relativos a los riesgos están integrados en cada departamento de la organización, es decir, la visión del riesgo se comunica y expande a través de toda la estructura de la organización. • Certificado de los controles suministrados.
El gobierno eficaz de la organización con respecto a los riesgos de TI equilibra los costos y beneficios de la gestión del riesgo	• El riesgo es priorizado y dirigido en consonancia con el apetito del riesgo y la tolerancia. • Los controles se llevarán a cabo con respecto a un determinado riesgos y en base a un análisis sobre el coste-beneficio del mismo. En pocas palabras, los controles no se implementan por el hecho de tener controles. • Los controles existentes son aprovechados para hacer frente a múltiples riesgos o para hacer frente a los riesgos de manera más eficiente.
La dirección eficaz de los riesgos de TI promueve la comunicación abierta y justa de los riesgos de TI	• La información abierta, exacta, oportuna y transparente sobre riesgos de TI sirve como la base para todas las decisiones relacionadas con el riesgo. • Las tareas, principios y métodos de la gestión de riesgos se han integrado en toda la organización. • Las conclusiones técnicas son traducidas en términos de negocio relevante y comprensible.

[16] Creada con base en la información recopilada del documento referenciado.

[17] Acrónimo de *Enterprise Risk Management* (administración de riesgos empresariales): marco para la gestión de riesgos relacionados con el logro de los objetivos de las organizaciones. En este marco se realiza:

- Identificación de eventos o circunstancias relevantes para los objetivos de la organización (riesgos y oportunidades).
- Evaluación en términos de probabilidad y la magnitud del impacto.
- Determinación de una estrategia de respuesta y seguimiento de los progresos.

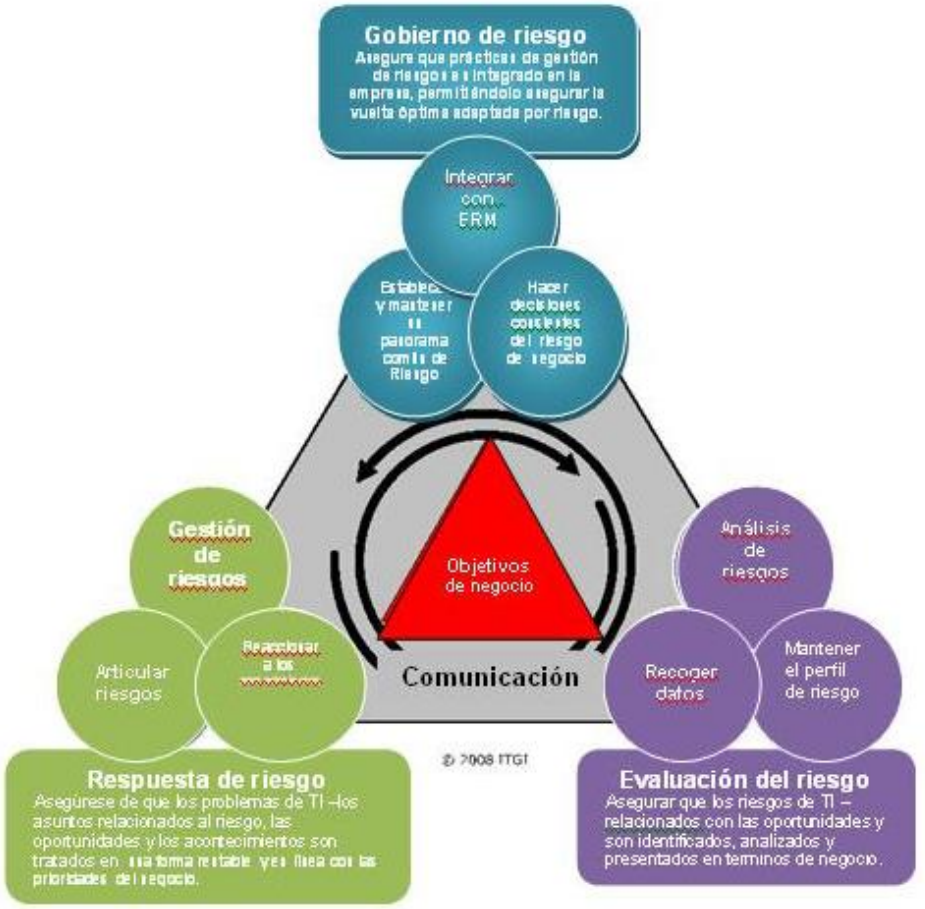
Tabla31. Principios de los riesgos de TI **[16]**[18] (Continuación)

Principios de los riesgos de TI	
La gestión eficaz de los riesgos de TI establece el tono correcto definiendo y estableciendo las responsabilidades personales para el funcionamiento dentro de los niveles de tolerancia aceptables y bien definidos	• Personas clave, por ejemplo personas influyentes, los dueños de negocios y el consejo de administración, se dedican a la gestión de riesgos de TI. • Hay una asignación clara aceptación de la propiedad del riesgo, incluyendo la rendición de cuentas, haciendo la medición del rendimiento e integrando la gestión del riesgo en el sistema de recompensas. Las acciones a seguir son divulgadas desde el principio por medio de políticas, procedimientos y el correcto nivel de ejecución. • La cultura del riesgo se promueve de manera activa, comenzando por las capas más altas. Esto ayuda a asegurar que aquellos implicados en la gestión de riesgos operacional funcionan sobre suposiciones de riesgo constantes. • Las decisiones de riesgos se toman por personas autorizadas, con un enfoque en la gestión organizacional, que desempeña un papel clave en la gestión de los riesgos, por ejemplo, para las decisiones de inversión, la financiación de proyectos, los principales cambios de entorno de TI, evaluaciones de riesgo, y el seguimiento de los controles y pruebas.
La gestión eficaz de los riesgos promueve la mejora continua y es una parte de las actividades diarias	• Debido a la naturaleza dinámica del riesgo, gestión de riesgos es un iterativo y perpetuo proceso en curso. Cada cambio conlleva riesgos y/o oportunidades, y la organización se prepara para ello, dando cuenta previamente a los cambios en la propia organización (fusiones y adquisiciones), en la regulación, en tecnologías de información, en el negocio, etc. • Se presta atención a la evaluación del riesgo mediante métodos, funciones y responsabilidades, herramientas, técnicas y criterios en toda la organización. o Identificación de los procesos clave y los riesgos asociados (la asignación de prioridad, que posee el perfil de riesgo) o Conocimiento de los impactos en el logro de objetivos o Identificación de los factores desencadenantes que indican cuando una actualización del marco o de los componentes es necesaria. • Las prácticas de gestión de riesgos están adecuadamente integradas en orden de prioridad y los procesos de toma de decisiones organizacionales. • Las prácticas de gestión de riesgos son simples y fáciles de usar, y contienen las prácticas para detectar las amenazas y los riesgos potenciales, así como para prevenir y mitigar las mismas.

Basado en los principios de los riesgos de TI, se ha desarrollado un modelo que agrupa los procesos gobierno del riesgo, evaluación del riesgo y respuesta ante los riesgos (Figura 22).

[18] Creada con base en la información recopilada del documento referenciado.

Figura 22. Marco RiskIT **[16]**



- Gobierno del riesgo (GR)
  - RG1 Establecer y mantener una vista de riesgo común.
  - RG2 Integrar con ERM.
  - RG3 Tomar decisiones conscientes de los riesgos del negocio.
- Evaluación de riesgos (RE)
  - RE1 Recoger datos.
  - RE2 Analizar los riesgos.
  - RE3 Mantener perfil de riesgo.
- Respuesta de riesgos
  - RR1 Riesgo articulado
  - RR2 Manejar riesgos
  - RR3 Reaccionar a acontecimientos

En la presente sección nos centraremos en la propuesta de Evaluación de riesgos (RE)

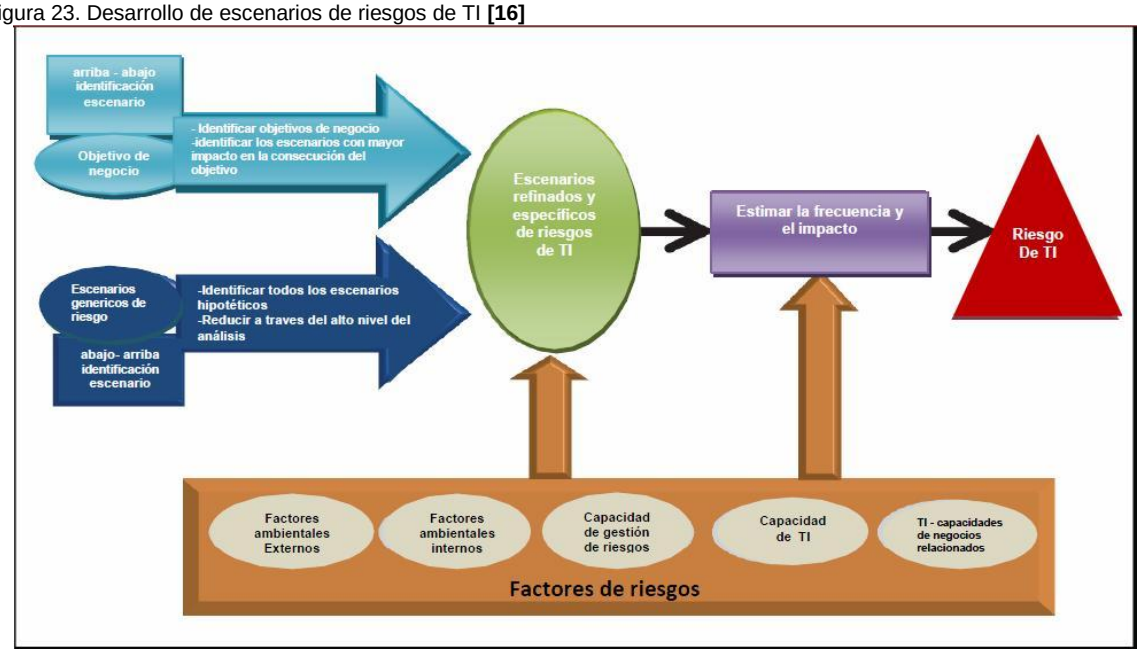
2.3.6.1 Identificación de riesgos

RiskIT encuentra que “uno de los desafíos para la gestión de riesgos de TI es identificar los riesgos importantes y relevantes entre todo lo que posiblemente puede relacionarse con TI, considerando la presencia y dependencia de TI en el negocio. Una de las técnicas para vencer este desafío es el desarrollo y el empleo de escenarios de riesgo. Este es un enfoque básico para lograr el realismo, visión, compromiso organizacional, mejorar el análisis y la estructura de la compleja cuestión de los riesgos de TI”.

La Figura 23 muestra que los escenarios de riesgo se pueden derivar a través de dos mecanismos diferentes:

1. Un enfoque de arriba abajo, en el que se parte de los objetivos generales y se realiza un análisis de los escenarios de riesgos de TI más relevantes y probables que impacten en los objetivos de negocio. Si los criterios de impacto están bien alineados con los controladores de valor real de la organización, los escenarios de riesgo relevantes se desarrollarán.
2. Un enfoque de abajo arriba, en el que se utiliza una lista de escenarios genérico para definir un conjunto de escenarios más concretos y personalizados, aplicados a la situación de la organización individual.

Figura 23. Desarrollo de escenarios de riesgos de TI **[16]**



2.3.6.2 Valoración de riesgos

Según RiskIT [16] “Una vez que el conjunto de escenarios de riesgo se define, puede ser utilizado para el análisis de riesgos, donde se evalúa la **frecuencia** y el **impacto** del escenario. Un componente importante de esta evaluación son los factores de riesgo, como se muestra en la Figura 23. Los factores de riesgo son aquellos factores que influyen en la frecuencia y / o impacto en el negocio de los escenarios de riesgo, ya que pueden ser de diferente naturaleza, y se pueden clasificar en dos categorías principales:

- **Factores ambientales**: estos se pueden dividir en factores internos y externos, diferenciándose en el grado de control que una organización tiene sobre ellos:
    - Factores internos del medio ambiente están, en gran medida, bajo el control de la organización, aunque no siempre sea fácil de cambiar.
    - Factores externos del medio ambiente están, en gran medida, fuera del control de la organización.
- **Capacidades**: lo buena que es una organización en las actividades relacionadas con TI. Pueden distinguirse según los tres marcos principales de ISACA:
    - Capacidades de gestión de riesgos de TI: ¿en qué medida es la organización madura en el desempeño de la gestión del riesgo de los procesos definidos en el marco de RISK IT?
    - Capacidades de TI: ¿cuán buena es la organización realizando los procesos de TI definidos en COBIT?
    - Capacidades de negocio relacionadas con TI (o gestión de valor): ¿cómo se alinean las actividades de gestión de valor de la organización con las expresadas en los procesos de Val IT?

Los factores de riesgo también se pueden interpretar como factores causales de la situación que se ha materializado, como vulnerabilidades o debilidades. Estos son términos que a menudo se utilizan en otros marcos de gestión de riesgos”.

Lo escenarios de análisis de riesgos deben contener los componentes, que se muestran en la Figura 24.

2.3.7 Propuesta MoR

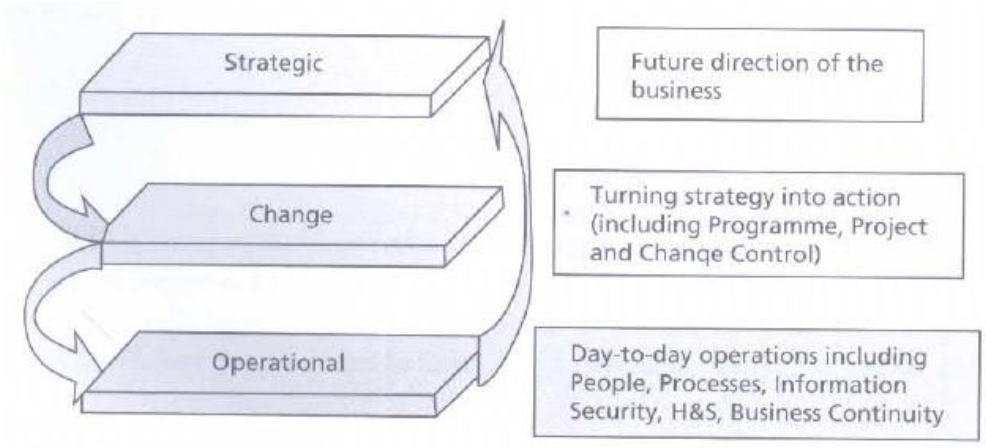
MoR afirma que la administración de los riesgos se puede aplicar a los tres núcleos de la empresa [17] estratégico, cambio, operativo (Figura 25); así:

- Estratégico: la dirección del negocio. Las decisiones tomadas son a largo plazo. El riesgo asociado con las decisiones estratégicas no se ven en el corto plazo y por eso se recomienda que se revisen periódicamente.

Figura 24. Componentes de escenarios de riesgos **[16]**

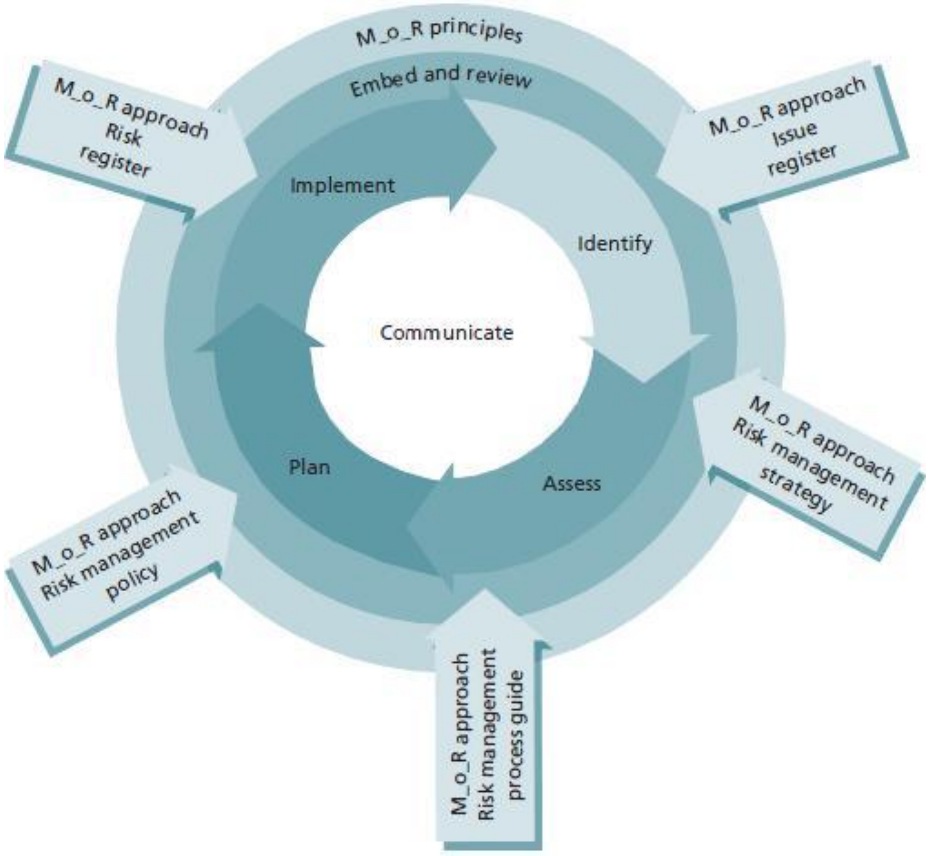
- Cambio (táctico): donde la estrategia o el direccionamiento estratégico se convierte en acciones; esto incluye programa, proyectos y administración del cambio.
- Operativo: operación diaria del negocio. Las decisiones tomadas en este nivel son de corto plazo y con el objetivo de mantener la continuidad del negocio; sin embargo, deben soportarse en los direccionamientos táctico y estratégico.

Figura 25.Tres núcleos donde puede aplicarse administración del riesgo **[17]**



El marco de trabajo de MoR [18] se basa en cuatro conceptos (Figura 26):

Figura 26. Marco de trabajo de MoR **[19]**



- **Principios** (Tabla 32): son esenciales para el desarrollo y mantenimiento de las buenas prácticas de gestión de riesgos. Son declaraciones de alto nivel y de aplicación universal que proporcionan orientación a las organizaciones, para que diseñen un enfoque adecuado para la gestión de riesgos como parte de sus controles internos.
- **Enfoque** (Tabla 33): los principios deben ser adaptados y adoptados a las necesidades de cada organización individual. En consecuencia, el enfoque de una organización a los principios debe ser acordado y definido dentro de políticas de gestión de riesgos, guías de procesos y estrategias.
- **Proceso**: se divide en cuatro pasos principales: identificar, evaluar, planificar y ejecutar. Cada paso describe las entradas, salidas, tareas y técnicas involucradas para asegurar que el proceso en general sea eficaz.
- **Incorporación y revisión**: después de haber puesto en marcha los principios, planteamientos y procesos, se necesita garantizar su aplicación coherente en toda la organización y que se someta a mejora continua a fin que éstos sean eficaces.

Tabla 32. Principios **[18]**

Principios	**Descripción**
Contexto organizacional	El punto de partida para la gestión del riesgo es entender el contexto de la organización o actividad objeto de examen y evitar así los puntos ciegos. El contexto incluye los aspectos político, económico, social, tecnológico, legal y ambiental.
Participación de los *stakeholders*	La gestión de riesgos debe comprometerse con todos los principales interesados para asegurar que los objetivos de la organización o actividad objeto de examen se han establecido y acordado.
Objetivos organizacionales	Como el propósito de la gestión del riesgo consiste en tratar de entender y manejar las amenazas y oportunidades derivadas de los objetivos de la organización o actividad, la gestión del riesgo sólo puede comenzar cuando están claros cuáles son estos objetivos.
Enfoque	Las organizaciones deben desarrollar un enfoque para la gestión del riesgo que reflejen sus objetivos particulares. Es común para las organizaciones describir su enfoque a través de sus políticas, procesos, estrategias y planes.
Informes	El órgano de gobierno de la organización debe recibir, revisar y actuar sobre los informes de gestión de riesgos. Como resultado de ello, un aspecto fundamental de la gestión del riesgo es la comunicación oportuna de información sobre los riesgos al equipo de administración que le permita tomar decisiones informadas.
Roles y responsabilidades	Las organizaciones deben establecer roles y responsabilidades claras para la gestión del riesgo en términos de liderazgo, dirección, control, gestión de riesgos en curso, informe y revisión.
Estructura de soporte	Un equipo de gestión de riesgos es necesario para garantizar que las políticas se cumplen, el proceso es seguido, las técnicas adecuadas se adoptan, los informes se emiten para satisfacer las necesidades de la alta gerencia y el tablero de mando, las directrices de los entes reguladores se respetas y las mejores prácticas son aplicadas (en el momento apropiado).
Indicadores de alerta temprana	Las organizaciones deben establecer indicadores de alerta temprana para las actividades críticas de negocio que proporcione información sobre las fuentes potenciales de riesgo. Esto permitirá gestión del riesgo proactivo y la anticipación a posibles problemas.
Superar barreras	Es necesario tener en cuenta que aunque una organización posea políticas de gestión de riesgos, procesos y estrategias, esto no conducirá automáticamente a prácticas de gestión de riesgo robustas, eficaces y eficientes. Hay una serie de barreras para la implementación de la gestión de riesgos que deben ser abordadas.
Mejora continua	Las organizaciones que estén interesadas en la mejora continua deben desarrollar estrategias para mejorar su grado de madurez de riesgo que les permitan planificar e implementar cambios radicales en sus prácticas de gestión de riesgos.

Tabla 33. Enfoque **[18]**

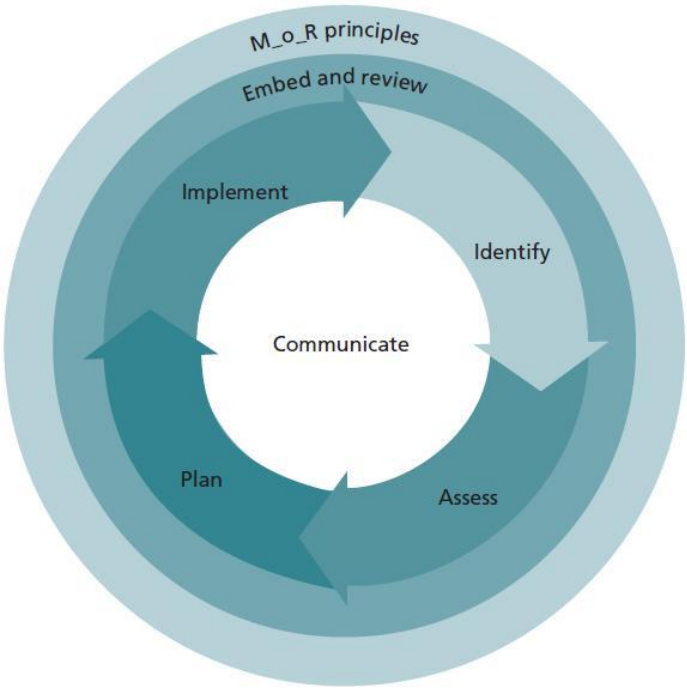
Documento	Descripción
Política de administración del riesgo	Su propósito es comunicar cómo la gestión del riesgo se llevará a cabo en toda la organización para apoyar la realización de sus objetivos estratégicos. La política comunica por qué la gestión del riesgo debe llevarse a cabo y cómo se relaciona con los objetivos corporativos, y proporciona un lenguaje común. Se esfuerza para lograr uniformidad en los procesos de gestión de riesgo, ayuda a eliminar la ambigüedad sobre el apetito de riesgo[19] de la organización y cuándo escalarlo.
Guía de procesos de administración del riesgo	Su propósito es describir los pasos y las actividades necesarias para implementar la gestión de riesgos. El proceso debe adaptarse a la organización y ser adecuado para los tipos de actividad en toda la organización. Debe ser aplicable a todos los niveles de gestión y de la actividad. Este documento debe describir un enfoque de mejores prácticas que apoyará un método coherente y ofrecer una gestión eficaz del riesgo. Esta guía se podría incorporar en la Política de Gestión de Riesgos.
Estrategias de administración del riesgo	Su propósito es el de describir, para una actividad particular de la organización, las actividades de riesgo específicos de gestión que se llevarán a cabo. Las estrategias suelen ser preparadas para una iniciativa estratégica en particular, un programa, un proyecto o un área operativa dentro de la organización. Cada estrategia debe adaptarse a cada actividad específica, mientras que al mismo tiempo que refleja la política de gestión de riesgos y la Guía del Proceso.
Registro del riesgo	Su propósito consiste en capturar y mantener información sobre todas las amenazas y oportunidades identificadas en relación con una actividad específica de la organización. El contenido exacto del registro de riesgos puede variar, pero el diseño del registro deberá reflejar la secuencia en la que se captura la información.
Log	Su propósito es capturar y mantener un registro coherente y estructurado de todos los sucesos identificados que ya han ocurrido y que requieren acción. Estos sucesos pueden incluir los riesgos que se han materializado y han cambiado de eventos posibles a eventos reales. Al igual que con el Registro de Riesgos, el contenido preciso del log puede variar, pero el diseño del registro deberá reflejar la secuencia en la que se captura la información.

2.3.7.1 Identificación de riesgos

La identificación de los riesgos, en MoR, es uno de los cuatro (4) procesos[18] del marco de trabajo (Figura 27): identificación, evaluación, planificación e implantación.

[19] Término utilizado para expresar la cantidad de riesgo que una organización está dispuesta a aceptar para alcanzar sus objetivos.

Figura 27. Procesos de MoR **[19]**



El proceso de identificación de riesgos se divide en dos: identificación del contexto e identificación del riesgo.

2.3.7.1.1 Identificación del contexto.

La identificación del contexto pretende obtener información acerca de la actividad planeada. Esto incluye la comprensión de:

- Cuáles son los objetivos de la actividad.
- Cuál es el alcance de la actividad.
- Qué suposiciones se han hecho.
- Qué tan completa es la información.
- Quiénes son y cuáles son los objetivos de los *stakeholders*.
- Dónde la actividad se ajusta a la organización con relación a la estructura organizativa, el medio ambiente propio de la organización y el enfoque de la organización para la gestión de riesgos.

Las entradas de este proceso son la política de gestión de riesgos y la guía del proceso y entre las salidas está la estrategia de gestión de riesgos.

2.3.7.1.2 Identificación del riesgo.

El objetivo principal es identificar los riesgos que pudieran reducir o eliminar la probabilidad de que la organización alcance sus objetivos; mientras se maximizan las oportunidades de obtener mejores rendimientos. Esto incluye:

- La identificación de las amenazas y oportunidades para la actividad.
- La preparación de un registro de riesgos.
- La preparación de indicadores clave de desempeño.
- La comprensión de vista de los interesados de los riesgos.

2.3.7.2 Valoración de riesgos

La valoración de los riesgos, en MoR, es otro de los cuatro (4) procesos [18] del marco de trabajo (Figura 27) y se divide en: estimación y evaluación.

2.3.7.2.1 Estimación.

La estimación consiste en evaluar cada una de las amenazas y las oportunidades de la organización en términos de su probabilidad de ocurrencia e impacto. La proximidad del riesgo también será de interés para medir la rapidez con que el riesgo se puede presentar si no se realizan acciones de control. El registro de riesgos se actualiza con los resultados de estas estimaciones.

2.3.7.2.2 Evaluación.

El objetivo de la evaluación es entender el efecto neto de las amenazas y oportunidades identificadas en una actividad cuando se suman entre sí. Esto incluye:

- Cálculo del valor monetario estimado que registre la media ponderada de los impactos previstos.
- Un modelo que agregue los riesgos mediante una técnica de simulación o el cálculo de un valor presente neto con una tasa de descuento aceptada.

2.3.8 Propuesta MagerIT

El objetivo general de esta norma es garantizar la seguridad los sistemas de información, identificando problemas y definiendo protocolos que los eviten. MagerIT se desarrolla en los siguientes productos:

Modelo de valor: Caracterización del valor que representen los activos para la organización así como de las dependencias entre los diferentes activos.

Mapa de riesgos: Relación de las amenazas a que están expuestos los activos.

Evaluación de salvaguardas: Evaluación de la eficiencia de las salvaguardas existentes en relación al riesgo que afrontan.

Estado del riesgo: Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.

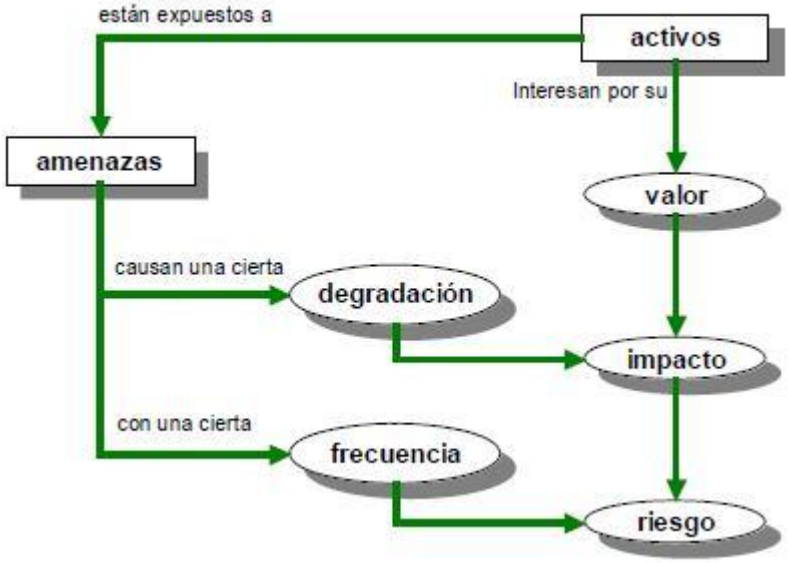
Informe de insuficiencias: Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema.

Plan de seguridad: Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos.

2.3.8.1 Identificación de riesgos

Para MagerIT la identificación de los riesgos es un proceso[20] que inicia con el análisis de los activos (Figura 28).

Figura 28. Proceso de identificación de riesgos **[20]**



2.3.8.1.1 Amenazas

Las amenazas son “cosas que ocurren”[20] y que pueden causarle daño a los activos; aunque debe tenerse claridad en que no todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

Hay accidentes naturales (terremotos, inundaciones, derrumbes, etc.) y desastres industriales (contaminación, fallos eléctricos, riego de líquidos, etc.) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos. Hay amenazas causadas por las personas, ya sean por errores o ataques intencionados.

Un activo no se ve afectado en todas sus dimensiones [20] [20] cuando es amenazado y en cada una de ellas se debe estimar su vulnerabilidad que puede calificarse como:

- **Degradación**: cuán perjudicado resultaría el activo, es decir, mide el daño causado por un incidente en el supuesto de que ocurriera. La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto “totalmente degradado”, o “degradado en una pequeña fracción”.

- **Frecuencia**: cada cuánto se presenta la amenaza. La frecuencia se relaciona con la degradación, pues una amenaza puede ser de terribles consecuencias pero de muy improbable ocurrencia; mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulando un daño considerable. La Tabla 34 muestra algunos valores de ocurrencia.

Tabla 34. Frecuencia **[20]**

Valor	Frecuencia	Ocurrencia
100	Muy frecuente	Diario
10	Frecuente	Mensualmente
1	Normal	Una vez al año
1/10	Poco frecuente	Cada X años

Para facilitar la identificación de las amenazas, MagerIT, propone la Tabla 35.

[20] Autenticidad, confidencialidad, integridad, disponibilidad.

Tabla 35. Identificación de amenazas **[21]**

[código] descripción sucinta de lo que puede pasar	
Tipos de activos[21]: Que se pueden ver afectados por este tipo de amenazas	**Dimensiones[22]:** 1. De seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante
Descripción: Complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas.	

2.3.8.1.2 Impacto

MagerIT define impacto como[20]: medida del daño sobre el activo derivado de la ocurrencia de una amenaza.

Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es fácil conocer el impacto que éstas tendrían sobre el sistema. Debido a que existe relación entre los diferentes activos se pueden identificar los siguientes tipos de impacto:

- Acumulado. Está dado en función de: el valor del activo (incluyendo el valor de los activos que se relacionan con él) y las amenazas a la que se encuentra expuesto.
- Repercutido. Está dado en función de: el valor del activo y las amenazas a la que están expuestos los activos relacionados con él.

[21] Los **tipos de activos** de MargeIT son:
- Servicios.
- Datos / Información.
- Aplicaciones (software).
- Equipos informáticos (hardware).
- Redes de comunicaciones.
- Soportes de información.
- Equipamiento auxiliar.
- Instalaciones.
- Personal.

[22] Las **dimensiones** de MagerIT son:
- Disponibilidad.
- Integridad de los datos.
- Confidencialidad de los datos.
- Autenticidad de los usuarios del servicio.
- Autenticidad del origen de los datos.
- Trazabilidad del servicio.
- Trazabilidad de los datos.

2.3.8.1.3 Riesgo

Conociendo el impacto de las amenazas sobre los activos, se puede determinar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia (Figura 28). El riesgo crece con el impacto y con la frecuencia.

2.3.8.2 Valoración de riesgos

Para valorar los riesgos, se deben tener en cuenta aspectos como la frecuencia, la degradación, la dimensión; entre otros, lo cual permite clasificarlos a en:

- Acumulado. Se calcula sobre un activo teniendo en cuenta el impacto acumulado debido a una amenaza y la frecuencia de ésta. El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la frecuencia de la amenaza.

- Repercutido. Se calcula sobre un activo teniendo en cuenta el impacto repercutido debido a una amenaza y la frecuencia de ésta. El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la frecuencia de la amenaza.

3. ANÁLISIS COMPARATIVO MARCOS EVALUADOS

3.1 Identificación de activos

Como punto de partida y conforme a lo presentado de los marcos revisados, se tomarán ISO27000, COBIT, ITIL e O-ISM3 para seleccionar las prácticas para identificación y valoración de activos.

Otra consideración es que, como se indica en [22], respecto a la utilización conjunta de estos cuatro marcos de referencia al momento de construir un sistema de gestión de seguridad de la información "Las implementaciones de O-ISM3 son compatibles con ISO27001 (*information Security Management Systems* – Requisitos), que establece los objetivos de control para cada proceso. Estas implementaciones usan un marco de responsabilidades de gestión similar al modelo del *IT Governance Institute* marco CobIT, que describe una mejor práctica en el campo de la administración de servicios de TI. Los usuarios ITIL pueden emplear orientación del proceso de O-ISM3 para fortalecer el proceso de seguridad ITIL sin problemas, utilizando mediciones de objetivos y metas estilo O-ISM3, es posible crear acuerdos de nivel de servicio medibles para los procesos de seguridad tercerizados".

El primer punto de comparación, para la selección se encuentra en lo que cada marco de referencia identifica como activo y que se muestra en la Tabla 36.

De este comparativo se toman para el modelo propuesto aquellos activos que sean sugeridos por el 50% o más de los marcos evaluados, obteniendo los valores de mostrados en la Tabla 37.

Si bien Servicios y Capital financiero no alcanzan el porcentaje de referenciación indicado, se considerarán dentro del modelo por la importancia que estos dos tipos de activos representan en la operación actual de las organizaciones.

Tabla 36. Comparativo activos en marcos de referencia **[5]**

MARCO DE REFERENCIA	ISO27000	COBIT	ITIL	ISM3
ACTIVOS CONSIDERADOS DENTRO DEL MARCO DE REFERENCIA	Información	Información	Información	
	Activos de software	Aplicaciones	Aplicaciones	° Repositorios ° Interfaces ° Fronteras ° Servicios [2] ° Sesiones ° Mensajes
	Activos físicos	Infraestructura	Infraestructura	° Dispositivos físicos ° Canales
	Servicios [1]			
	Personas	Personas	Personas	
	Intangibles			
			Gestión	
			Organización	
			Procesos	
			Conocimiento	
			Capital financiero	

1 - Se refiere a servicios tipo agua, energía eléctrica y aire acondicionado

2 - Se refiere a servicios provistos por los sistemas p.e. por la BIOS

CONVENCIONES	
	Activo sugerido en el 100% de los marcos de referencia
	Activo sugerido en el 75% de los marcos de referencia
	Activo sugerido en el 50% de los marcos de referencia
	Activo sugerido en el 25% de los marcos de referencia

Tabla 37: Tipos de activos modelo propuesto **[5]**

TIPO DE ACTIVO	DEFINICIÓN
INFORMACIÓN	Toda fuente o repositorio de información física o electrónica (bases de datos, documentos, manuales, diagramas)
APLICACIONES	Todos los componentes de software de los sistemas de información
INFRAESTRUCTURA	Todos las instalaciones y dispositivos físicos requeridos para la ejecución de un proceso (instalaciones, servidores, equipos de telecomunicaciones, dispositivos especiales)
PERSONAS	Personas naturales con el conocimiento, habilidades o destrezas
SERVICIOS	Todo servicio propio o suministrado por terceros (Agua, Energía Eléctrica, Telecomunicaciones, Aire Acondicionado, Sistemas de extinción de incendio, monitoreo, mantenimiento, etc.)
CAPITAL FINANCIERO	Recursos económicos requeridos para la realización de un proceso

3.2 Valoración de activos

Igualmente cada marco de referencia identifica las características o elementos de valor intrínseco que poseen estos activos y que definen la importancia del tratamiento que se le debe dar cada uno de ellos dentro del sistema de gestión de seguridad de la información (Tabla 38).

Tabla 38. Comparativo atributos en marcos de referencia **[5]**

MARCO DE REFERENCIA	ISO27000	COBIT	ITIL	ISM3[1]
ATRIBUTOS CONSIDERADOS DENTRO DEL MARCO DE REFERENCIA		EFECTIVIDAD		OBJETIVOS DE SEGURIDAD
		EFICIENCIA		
	CONFIDENCIALIDAD	CONFIDENCIALIDAD		
	INTEGRIDAD	INTEGRIDAD		
	DISPONIBILIDAD	DISPONIBILIDAD	GARANTÍA[2] - Disponilidad	
		CUMPLIMIENTO		
		CONFIABILIDAD	GARANTÍA[2] - Confiabilidad	
			GARANTÍA[2] - Continuidad	
			GARANTÍA[2] - Seguridad	
			UTILIDAD	

1 - ISM3 acoge la definición que se realice como objetivo de seguridad con cualquier otro marco de

2 - Garantía se integra por Disponibilidad, Confiabilidad, Continuidad y Seguridad.

CONVENCIONES	
	Atributo sugerido en el 100% de los marcos de referencia
	Atributo sugerido en el 75% de los marcos de referencia
	Atributo sugerido en el 50% de los marcos de referencia
	Atributo sugerido en el 25% de los marcos de referencia

De estos elementos se toman los que sean sugeridos en 50% o más de los marcos evaluados, definiendo para el modelo los atributos que se muestran en la Tabla 39.

Como referencia a las prácticas que proponen los marcos evaluados para la identificación y valoración de activos, se incluye el comparativo de las propuestas de los marcos evaluados (ANEXO A).

Tabla 39: Atributos activos en modelo propuesto **[5]**

ATRIBUTO	DEFINICIÓN
CONFIDENCIALIDAD	Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
INTEGRIDAD	Propiedad de salvaguardar la exactitud y estado completo de los activos.
DISPONIBILIDAD	Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
CONFIABILIDAD	Capacidad de un activo para ejecutar sin interrupción una función requerida, bajo las condiciones establecidas.

Nota: Las definiciones se toma de los términos y definiciones de la norma ISO 27001 e ITIL.

3.3 Identificación de riesgos

Para la selección de las propuestas para identificación de riesgos se partirá de la Tabla 40 donde se observan que la propuesta de la ISO ISO27000 es la más detallada y da cobertura a lo presentado por los otros marcos, sin embargo tomaremos elementos de MagerIT y MoR para el modelo a proponer como se muestra en la Tabla 41.

Tabla 40. Comparativo propuestas identificación de riesgos **[5]**

ISO27000	COBIT	ITIL	O-ISM3	NTC 5254	RiskIT	MoR	MagerIT
1. **Identificar los riesgos**	**PO9. Evaluar y Administrar los Riesgos de TI.**	**Análisis de Riesgos**	**Gestión de Riesgo**	**Identificar Riesgos**	**Evaluación de Riesgos**	**Identificación de Riesgos**	**Identificación de Riesgos**
						Identificación del contexto	
1.1 Identificar los activos.	PO9.1 Marco de Trabajo de Administración de Riesgos	Identifica Riesgos				Identificación del riesgo	
1.2 Identificar las amenazas	PO9.2 Establecimiento del Contexto del Riesgo			¿Qué puede suceder?			Identificación de Amenazas
1.3 Identificar las vulnerabilidades	PO9.3 Identificación de Eventos			¿Cómo puede suceder?			
1.4 Identificar los impactos que la pérdida la confidencialidad, integridad y disponibilidad puede tener sobre estos activos.					RE 1 Recoger datos (escenarios de riesgos)		

Tabla 41. Identificación de riesgos en modelo propuesto **[5]**

1. Identificar los riesgos
1.1 Identificar los activos
1.2 Identificar las amenazas
1.3 Identificar vulnerabilidades

3.4 Valoración de riesgos

Para la selección de las propuestas para la valoración de riesgos se partirá de la Tabla 42 donde se observan que las propuestas más completas son ISO27000, NTC5254 y MoR; de las cuales se tomarán los elementos a proponer como muestra la Tabla 43.

Tabla 42. Comparativo propuestas valoración de riesgos **[5]**

ISO27000	COBIT	ITIL	O-ISM3	NTC 5254	RiskIT	MoR	MagerIT
2. **Analizar y evaluar los riesgos**		**Gestión de Riesgos**		**Analizar los Riesgos**	**RE2 analizar los riesgos**	**Valoración de Riesgos**	**Valoración de Riesgos**
				Determinar controles existentes		Estimación del riesgo	
2.1 Valorar el impacto de negocios.	PO9.4 Evaluación de Riesgos de TI	Evalua Riesgos		Consecuencia y posibilidad		Evaluación del riesgo	Impacto (degradación y frecuencia)
2.2 Valorar la posibilidad realista de que ocurra una falla en la seguridad,							
2.3 Estimar los niveles de los riesgos.		Define Nivel Aceptable de Riesgos		Evaluación del riesgo			
2.4 Determinar la aceptación de riesgo o la necesidad de su tratamiento	PO9.5 Respuesta a los Riesgos	Identifica respuesta adecuada al riesgo					Riesgo

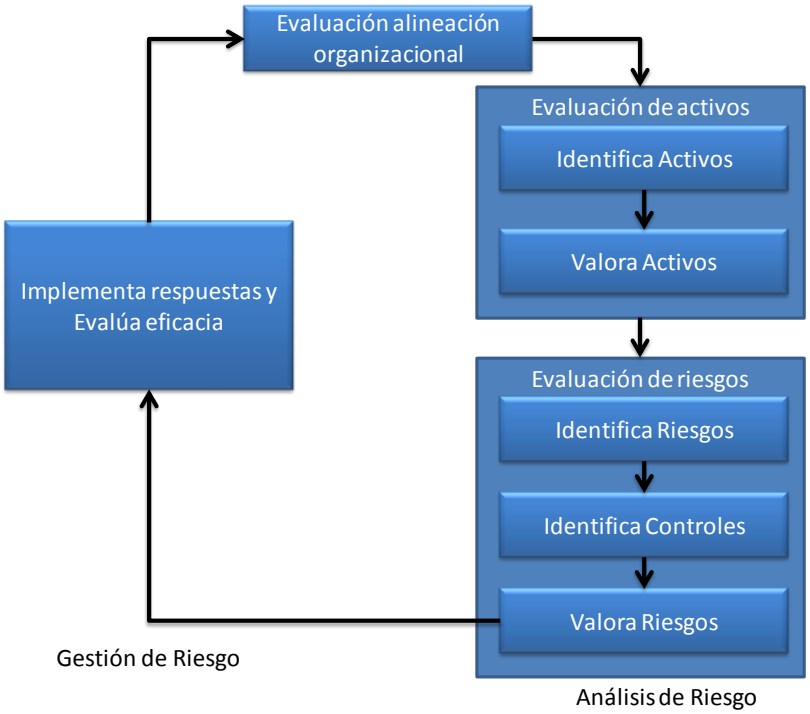
Tabla 43. Valoración de riesgos en modelo propuesto **[5]**

2. Valorar Riesgos
2.1 Identificar controles
2.2 Valorar impacto (degradación)
2.3 Valorar probabilidad (frecuencia)
2.4 Valorar riesgo

4. MODELO PROPUESTO

El modelo propuesto supone una organización basada en procesos con una definición en su política de gestión que permita integrar en su sistema un ciclo de alineación, análisis y gestión de riesgos como se muestra en la Figura 29.

Figura 29. Ciclo modelo propuesto **[5]**



A grosso modo, las fases del ciclo propuesto comprenden:

Evaluación alineación organizacional: corresponde a la revisión y priorización de los procesos productivos que van a ser objeto de aseguramiento y requieren que sus activos y riesgos asociados sean identificados y valorados.

Evaluación de activos: presenta las actividades y mecanismos que permitan a la organización identificar los activos que intervienen en sus procesos productivos y priorizarlos conforme a los criterios que dan valor a la información que intrínsecamente representan.

Evaluación de riesgos: una vez obtenida la relación de activos y definido su valor dentro del proceso productivo, se presentan las herramientas que permiten

identificar el grado de exposición y el impacto que puede generar en la organización la violación a la seguridad de estos activos críticos.

La fase de gestión de riesgo, donde se implementa y evalúa la eficiencia de la respuesta a los riesgos identificados, no se incluye en el modelo propuesto y puede ser objeto de otro estudio futuro.

4.1 Evaluación alineación organizacional

Partiendo de la premisa que los riesgos siempre existen y que aquellos que deben ser gestionados son los que, de llegar a hacerse reales, afectarían los resultados estimados por la organización, se debe identificar dentro de la cadena de valor de la empresa los procesos que tienen mayor influencia o participación en el logro de los objetivos.

La estimación de la importancia de cada proceso dentro de la cadena de valor puede hacerse de varias maneras:

- Por el conocimiento del negocio
- Por sentido común
- Por participación sobre los ingresos de la empresa
- Por el número de activos involucrados
- Por la criticidad dentro de la cadena productiva

El resultado ha de ser un vector que contiene los procesos que se incluirán dentro del alcance del análisis de riesgo, indicando el porcentaje de participación estimado sobre el resultado del negocio. Este vector ayudará posteriormente a definir la prioridad con que se deben analizar los riesgos de los activos de información que se identifiquen. En el ANEXO B se muestra un ejemplo de vector de procesos priorizado.

4.2 Evaluación de activos

En esta fase se realiza el inventario de los activos de información que participan dentro de los procesos incluidos en el alcance del análisis de riesgo y se estima el valor que cada uno de ellos representa para la organización

4.2.1 Identificación de activos

Para cada proceso dentro del alcance del análisis de riesgo se debe identificar claramente los activos involucrados a través de entrevistas con los responsables de los procesos objeto de evaluación.

Para cada activo se deberá diligenciar la información de la Tabla 44.

Tabla 44. Atributos de activo de información **[5]**

Atributo	**Descripción**
ID Activo	Número de identificación único con que se identificará el activo dentro del inventario.
Nombre de activo	Nombre con que se reconoce el activo dentro de la organización.
Propietario	Es la persona o proceso que tiene la responsabilidad de definir quiénes tienen acceso y qué pueden hacer con la información y dé determinar que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada y definir que se hace con la información una vez ya no sea requerida y los tiempos de retención asociados a la misma.

Administrador	Es la persona o área encargada de administrar y hacer efectivos los controles de seguridad que el propietario de la información ha definido, con base en los controles de seguridad disponibles.
	
	Entre los controles de seguridad se tiene:
	• Toma de copias de seguridad.
	• Asignar privilegios de:
	  ○ Acceso.
	  ○ Modificación.
	  ○ Borrado

Tipo activo	Para cada activo se identifica el grupo al que pertenece (Tabla 45).

Tabla 45. Grupo de activo de información **[5]**

Grupo	**Descripción**
Información	Toda fuente de información física o electrónica (Bases de datos y archivos de datos, contratos y acuerdos, documentación del sistema, información sobre investigación, manuales de usuario, material de formación, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos de recuperación, registros de auditoría e información archivada.
Aplicaciones	Todos los componentes de software de los sistemas de información, software del sistema, herramientas de desarrollo y utilidades.
Infraestructura	Todas las instalaciones y dispositivos físicos requeridos para la ejecución de un proceso (instalaciones, equipos de computación, equipos de comunicaciones, medios removibles y otros equipos).
Personas	Personas naturales con sus calificaciones, habilidades y experiencia.
Servicios	Todo servicio propio o suministrado por terceros (agua, energía eléctrica, telecomunicaciones, aire acondicionado, sistemas de extinción de incendios, monitoreo, mantenimiento de hardware, software o infraestructura).
Capital financiero	Recursos económicos directos requeridos para la realización de un proceso.

En el ANEXO C se presenta un ejemplo de matriz con la que se puede realizar el inventario de activos.

4.2.2 Valoración de activos

Para cada uno de los de los procesos dentro del alcance del análisis de riesgo se debe identificar que tan significativo es el aporte de cada activo a los atributos de la información que intrínsecamente representan según las siguientes definiciones (Tabla 46):

Tabla 46. Atributos de la información **[5]**

ATRIBUTO	DEFINICIÓN
CONFIDENCIALIDAD	Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
INTEGRIDAD	Propiedad de salvaguardar la exactitud y estado completo de los activos.
DISPONIBILIDAD	Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
CONFIABILIDAD	Capacidad de un activo para ejecutar sin interrupción una función requerida, bajo las condiciones establecidas.

Confidencialidad: Se debe evaluar el impacto que se tendría si el activo de información fuera accedido por personas no autorizadas (Tabla 47).

Tabla 47. Evaluación confidencialidad **[5]**

	VALORACIÓN				
ATRIBUTO	**1**	**2**	**3**	**4**	**5**
CONFIDENCIALIDAD	La información es de carácter PUBLICO y no se tiene ningún impacto sobre el resultado del proceso en caso de ser accedido por personas no autorizadas	La información a pesar de ser de carácter PUBLICO ya ha sido clasificada y nutrida por la organización y de ser accedida por personas no autorizadas podría afectar el resultado o poner en riesgo la empresa	La información es de carácter RESTRINGIDO pero de ser accedida por personas no autorizadas no afectaría en mayor grado el resultado o pondría en riesgo la empresa	La información es de carácter RESTRINGIDO y de ser accedida por personas no autorizadas podría afectar el resultado del proceso o poner en riesgo la empresa	La información es de carácter SECRETO y en caso de ser accedida por personas no autorizadas el impacto final sobre el proceso o resultado de la empresa sería muy grave

Integridad: Se debe evaluar el impacto que se tendría si la exactitud y estado completo de la información fuera alterado (Tabla 48).

Tabla 48. Evaluación integridad **[5]**

	VALORACIÓN				
ATRIBUTO	**1**	**2**	**3**	**4**	**5**
INTEGRIDAD	La información no es crítica, y no tiene repercusión en el proceso. Si presentara errores la pérdida que origina es muy pequeña y su reconstrucción consiste en la repetición de un proceso sencillo.	La información no es crítica pero es básica para algunas decisiones menores del proceso. La ocurrencia de un fraude o errores sobre la misma podría ocasionar pérdidas.	La información es crítica y sobre ella se basan algunas decisiones del proceso. La ocurrencia de un fraude o errores sobre la misma ocasionará pérdidas.	La información es crítica y es aquella en la cual se basan decisiones importantes del proceso. La ocurrencia de un fraude o errores sobre la misma ocasionará pérdidas importantes o severas, por lo cual, la información necesita un nivel razonable de protección contra error y fraude.	La información es base para la toma de decisiones estratégicas o es fundamental para la protección de los individuos de la organización. La ocurrencia de un fraude o errores sobre la misma ocasionará pérdidas graves o catastróficas, por lo cual, la información deberá estar libre de error

Disponibilidad: Se debe evaluar el impacto que se tendría si los usuarios autorizados no tuvieran acceso a los activos de información en el momento que lo requieran (Tabla 49).

Tabla 49. Evaluación disponibilidad **[5]**

	VALORACIÓN				
ATRIBUTO	**1**	**2**	**3**	**4**	**5**
DISPONIBILIDAD	El tiempo para recuperar la información no es crítico, puede esperar una semana o más sin tener consecuencia sobre el resultado del proceso.	El tiempo máximo para recuperar la información y volver a iniciar el procesamiento debe ser menor a una semana.	El tiempo máximo para recuperar la información y volver a iniciar el procesamiento debe ser menor a dos días.	El tiempo máximo para recuperar la información y volver a iniciar el procesamiento es menor a un día.	El tiempo máximo para recuperar la información y volver a iniciar el procesamiento es menor a 4 horas.

Confiabilidad: Se debe evaluar el impacto que se tendría si el activo interrumpe su servicio en el momento que lo requieran (Tabla 50).

Tabla 50. Evaluación Confiabilidad **[5]**

ATRIBUTO	VALORACIÓN 1	2	3	4	5
CONFIABILIDAD	Si el servicio del activo se interrumpe no se afecta la operación ni el resultado del proceso.	Si el servicio del activo se interrumpe, se puede continuar operando utilizando el servicio de otro activo ya existente.	Si el servicio del activo se interrumpe se afecta la operación pero el resultado se obtiene, aunque se requiere mayor duración del proceso.	Si el servicio del activo se interrumpe, no se puede continuar operando y se requiere reemplazar el activo para reiniciar la operación, generando pérdidas al negocio.	El servicio ofrecido por el activo no puede interrumpirse, de hacerlo tendría consecuencias catastrófica para el negocio, debe garantizarse su operación ininterrumpida.

En el ANEXO C se presenta un ejemplo de matriz que incluye los atributos de valoración de los activos.

4.2.2.1 Estimación del valor de activos.

Una vez concluido el diligenciamiento de la matriz de los activos involucrados en los procesos dentro del alcance del análisis de riesgo se estima el valor global de cada activo. El valor global de cada activo se calcula mediante la Fórmula 1.

Fórmula 1. Valor activo

$$ValorActivo = \sum_{i=1}^{n} (C_i + I_i + D_i + R_i) * PP_i$$

C : Confidencialidad
I : Integridad
D : Disponibilidad
R : Confiabilidad (*reliability*)
PP : Peso Proceso

En la Fórmula 1 se ha introducido el término peso proceso, que no es más que la asignación de un valor a la importancia que el activo posee dentro de cada uno de los procesos de la organización donde participa o está involucrado y esta dado por el peso que se estimó para el proceso en la primera fase del ciclo o fase de alineación estratégica; es decir, el valor de un activo es un resultado numérico ponderado que incluye la calificación de los atributos de éste.

Dado que el número de activos involucrados en la organización o procesos evaluados puede ser muy alto, se sugiere continuar la fase de evaluación de

riesgos con los activos de mayor valor. Teniendo en cuenta la naturaleza ponderada del valor de los activos de información, en el presente trabajo se continúa el análisis de riesgo con el 80% de los activos con mayor valoración bajo la premisa que son los más críticos y ponen en riesgo el logro de los objetivos del negocio; por lo tanto el análisis de riesgo debe centrarse sobre ellos.

En el ANEXO C se presenta un ejemplo de matriz que incluye el valor global del activo para los procesos dentro del alcance del análisis de riesgo.

4.3 Evaluación de riesgos

En esta fase se identifican amenazas, vulnerabilidades y salvaguardas (controles existentes) para posteriormente estimar el riesgo para cada uno de los activos críticos involucrados en los procesos dentro del alcance del análisis.

4.3.1 Identificación de riesgos

Para facilitar la identificación de las amenazas a que se expone cada uno de los activos críticos identificados en la fase anterior, se propone el atributo tipo de activo y se agrupan los de cada categoría. Luego se referencian con las tablas de amenazas (basada en MagerIT) para identificar cuáles de ellas afectan el grupo, centrándose principalmente en las que pueden impactar el o los atributos que presenten el mayor valor para cada uno de los activos seleccionados.

En el ANEXO D se presenta una tabla resumen, basada en MagerIT, de las amenazas posibles sobre los activos de un sistema de información y los atributos o dimensiones que son afectados por la amenaza con consecuencias para la seguridad del sistema de información y en el ANEXO E se presenta una muestran fragmentos de una matriz donde ya se han identificado los principales riesgos de los activos seleccionados como los más críticos de los procesos dentro del alcance del análisis.

4.3.2 Identificación de controles

Luego de tener identificadas las amenazas que pueden afectar los principales activos de los procesos considerados dentro del alcance del análisis, se identifican los controles o salvaguardas que ya estén implementados y se estima el nivel de mitigación que este representa frente a la amenaza.

En este modelo se asume la existencia de un proceso para la definición, diseño y seguimiento de controles o salvaguardas dentro el tratamiento de los riesgos identificados, pues como se plantea al inicio de este capítulo, la fase de gestión de riesgo, donde se implementa y evalúa la eficiencia de la respuesta a los riesgos identificados, no se incluye en el modelo propuesto y puede ser objeto de otro estudio, pero para efectos de valorar el riesgo considerando los elementos que pueden reducir su probabilidad o impacto, a continuación se proponen los elementos a identificar en esta fase.

4.3.2.1 Estimación de eficiencia de salvaguardas.

Para estimar la eficiencia de las salvaguardas, para cada una de las amenazas se debe identificar, primero si existe un control o salvaguarda que pueda mitigar su probabilidad o impacto y segundo cual puede ser su eficiencia, para ello se aplica a cada control los valores definidos en la Tabla 51.

Tabla 51. Evaluación eficiencia salvaguarda **[5]**

Cualificación	Consideración
Muy Adecuado	El control o salvaguarda establecido tiene un diseño fuerte, es automático y se ha comprobado su efectividad
Adecuado	El control o salvaguarda establecido tiene un diseño fuerte, **no** es automático, pero se ha comprobado su efectividad
Moderado	El control o salvaguarda establecido tiene un diseño fuerte, no es automático o no se ha comprobado su efectividad
Débil	El control o salvaguarda establecido **no** tiene un diseño fuerte, no es automático, pero se ha comprobado su efectividad
Muy débil	El control o salvaguarda establecido no tiene un diseño fuerte, no es automático y no se ha comprobado su efectividad

Una vez estimada la eficiencia del control o salvaguarda se aplicará el factor de mitigación al momento de valorar el riesgo (Tabla 52).

En el ANEXO F se muestra como ejemplo un fragmento de una matriz donde ya se han identificado los controles o salvaguardas de las amenazas de los activos seleccionados como los más críticos de los procesos dentro del alcance del análisis.

Tabla 52. Evaluación factor de mitigación salvaguarda **[5]**

Cualificación	Consideración	Eficiencia	Marginalidad
Muy Adecuado	El control o salvaguarda establecido tiene un diseño fuerte, es automático y se ha comprobado su efectividad	90%	0.1
Adecuado	El control o salvaguarda establecido tiene un diseño fuerte, **no** es automático, pero se ha comprobado su efectividad	70%	0.3
Moderado	El control o salvaguarda establecido tiene un diseño fuerte, no es automático o no se ha comprobado su efectividad	50%	0.5
Débil	El control o salvaguarda establecido **no** tiene un diseño fuerte, no es automático, pero se ha comprobado su efectividad	30%	0.7
Muy débil	El control o salvaguarda establecido no tiene un diseño fuerte, no es automático y no se ha comprobado su efectividad	10%	0.9

4.3.3 Valoración de riesgos

En esta etapa, para cada una de las amenazas identificadas se debe estimar la probabilidad de que esta se haga realidad y el impacto que causaría sobre el activo amenazado, sin considerar la existencia de las salvaguardas o controles.

4.3.3.1 Estimación de frecuencia o probabilidad.

Para cada uno de los riesgos identificados se estima la probabilidad de ocurrencia según la Tabla 53. El atributo de valor se utilizará para calcular el valor final de riesgo.

Tabla 53. Valor probabilidad de ocurrencia **[5]**

Valor	Frecuencia	Ocurrencia
0.2	Nada frecuente	No ha sucedido
0.4	Poco frecuente	Ha sucedido una vez cada 10 años
0.6	Normal	Ha sucedido una vez al año
0.8	Frecuente	Ha sucedido mensualmente
1	Muy frecuente	Sucede diariamente

4.3.3.2 Estimación de impacto o degradación.

Una vez estimada la frecuencia se debe considerar el impacto que causaría la amenaza sobre el activo en el evento en que la amenaza se hiciera real, aplicando

los valores de la Tabla 54. El atributo de valor se utilizará para calcular el valor final de riesgo.

Tabla 54. Valor impacto amenaza **[5]**

Valor	Degradación	Ocurrencia
0,2	Insignificante	El activo no sufre daños que le impidan continuar operando
0,4	Menor	El activo sufre daños, pero puede continuar operando
0,6	Moderado	El activo sufre daños y su operación queda restringida
0,8	Mayor	El activo sufre daños que impiden su operación pero que pueden recuperarse dentro del tiempo tolerable para la operación
1	Catastrófico	El activo sufre daños irreparables y la operación se ve afectada más allá de lo tolerable

4.3.3.3 Estimación riesgo marginal.

En este punto ya se dispone de la información para calcular tanto el riesgo inherente (Fórmula 2), que es igual al producto de la probabilidad o frecuencia de ocurrencia de la amenaza por el impacto o degradación del activo y el riesgo marginal (Fórmula 3) que corresponde al producto del riesgo inherente por el valor de marginalidad calculado para las salvaguardas estimadas en el paso anterior.

Fórmula 2. Riesgo inherente

$$RiesgoInherente = Frecuencia * Degradación$$

Fórmula 3. Riesgo marginal

$$RiesgoMarginal = RiesgoInherente * Marginalidad$$

Una vez concluida la evaluación de los riesgos que representan las amenazas identificadas para los activos más críticos de los procesos dentro del alcance de evaluación de riesgos, se tendrá como resultado una tabla que servirá de guía para continuar con el proceso de Gestión de riesgos, donde se deberá establecer la respuesta a cada uno de los riesgos identificados y se deberá hacer

seguimiento a la eficiencia de estas respuestas y posteriormente volver a repetir el ciclo de alineamiento, evaluación de activos y evaluación de riesgos.

En el ANEXO G se muestra un fragmento de una matriz donde ya se han estimado la frecuencia y el impacto de las amenazas sobre los activos y se han calculado los riesgos inherentes y residuales que representan estas amenazas.

5. **VALIDACIÓN DE LA PROPUESTA**

Para la validación del modelo propuesto se recurrió a la Unidad de Tecnología Informática (UTI) del Grupo Empresarial Cooperativo Coomeva (GECC), que a través de su macro proceso de Gestión de Riesgo y Seguridad Informática brinda soporte y apoyo metodológico a las empresas del grupo en lo que tiene que ver con el tema objeto de este modelo.

Este macro proceso de Riesgo y Seguridad Informática está dirigido por un ingeniero con especializaciones en Telemática de la Universidad Autónoma de Occidente en convenio con la Universidad del Cauca y en Seguridad en Redes, Aplicaciones y Sistemas Operativos de la Universidad Oberta de Catalunya y maestría en seguridad Informática de la universidad Oberta de Catalunya, quien acompañó el ejercicio de validación y guió la aplicación del modelo propuesto.

Apoyados en la experiencia previa y en los ejercicios realizados para empresas del sector financiero y de seguros se comparó el modelo con métodos y herramientas utilizados hasta el momento y se realizó la aplicación para la evaluación de riesgos de tres servicios del macro proceso de Infraestructura y Telecomunicaciones de esta misma unidad, que brinda sus servicios a todas las dieciséis (16) empresas del grupo y realiza la gestión de la red de datos y telecomunicaciones que integra con los centros de procesamiento principal y alterno de la organización más de doce mil (12.000) estaciones de trabajo a lo largo y ancho del país.

Para la definición del alcance del análisis se buscó que los procesos a evaluar tuvieran un alto impacto, pero que a su vez tuvieran información disponible y fuera posible comparar los resultados que arrojara el modelo propuesto frente a las prácticas existentes.

La simulación se llevó a cabo utilizando la información recaba en el proceso real de identificación de activos y valoración de riesgos, mapeándolo con las herramientas elaboradas para el modelo propuesto y verificadas mediante entrevista con los ingenieros administradores de la plataforma de telecomunicaciones del Grupo Empresarial Cooperativo Coomeva (GECC).

6. **RESULTADOS OBTENIDOS**

El primer resultado de este trabajo lo constituyen el conjunto de definiciones y herramientas para la identificación de activos y riesgos propuestos por el modelo. Con esto se establece el marco de trabajo a nivel de la identificación de activos, sus atributos y amenazas según los grupos que se consideran dentro del proceso de identificación y valoración de activos y de identificación y valoración de riesgos, facilitando y estandarizando el trabajo de las personas que participan en esta gestión.

En concepto del jefe de Gestión de Riesgo Tecnológico y Seguridad Informática y del administrador de la plataforma de Telecomunicaciones de la Unidad de Tecnología Informática del Grupo Empresarial Cooperativo Coomeva (GECC), esta herramienta presenta una secuencia más lógica, coherente y sencilla de aplicar, al ser comparada con la actualmente utilizada y podría ser aplicada en adelante para los procesos de valoración de activos y de identificación y valoración de riesgos que se realiza para la unidades o empresas del grupo empresarial.

Desde el proceso de identificación y valoración de activos se obtiene un método más objetivo y completo al analizar la importancia del activo desde cuatro perspectivas (Confidencialidad, Integridad, Disponibilidad y Confiabilidad) frente a cada uno de los procesos en los que el activo pueda estar involucrado y no con un solo valor estimado de manera global, como se viene haciendo.

Si bien la identificación de riesgos del modelo actualmente utilizado se basa en MagerIT, este proceso se aplica sobre grupos de activos y no sobre cada activo, como se hace en el modelo propuesto, incrementando con esto el nivel granularidad del análisis y facilitando la identificación de controles al momento de estimar los riesgos inherentes y residuales para los que deben ser gestionados los respectivos controles. Adicionalmente el modelo enriquece las referencias de MagerIT al agregar el atributo de confiabilidad en el mapa de amenazas por grupo de activos y los grupos de activos al adicionar el tipo Capital Financiero a los que hasta ahora se vienen manejado en el GECC para este tipo de análisis.

Otro resultado positivo del modelo propuesto se obtiene de la aplicación de los escenarios planteados para calificar el impacto de las amenazas sobre los activos, nuevamente, por ser manejados de manera individual y presentar una escala de valoración cualitativa que fácilmente puede ser entendida y aplicada sobre los procesos bajo análisis, que posteriormente es convertida por el modelo a escalas cuantitativas para lograr la priorización de los riesgos.

Si bien el ejercicio de simulación para la validación del modelo se realizó utilizando hojas electrónicas, la definición del modelo, de los parámetros de sus diferentes

componentes, de los mecanismos de valoración y de la interrelación entre todos estos elementos, permite que el modelo pueda ser llevado a una herramienta automatizada que facilite el manejo y reduzca la complejidad que significa la manipulación y evaluación de un alto número de activos y de amenazas para cada uno de ellos, apoyados en lenguajes de programación y manejadores de bases de datos de mayor capacidad y facilidad de uso.

A continuación se presentan los resultados de cada una de las etapas y fases de la aplicación del modelo con alcance a tres servicios del macro proceso de Infraestructura y Telecomunicaciones de la Unidad de Tecnología Informática del GECC.

6.1 Evaluación alineación organizacional.

Las empresas del GECC aplican un modelo de gestión estándar para toda la organización, modelado sobre la norma ISO9000 y todas sus empresas y unidades han sido certificadas y recertificadas bajo la norma ISO9001 versión 2000.

Dada la orientación al cliente de toda la organización, cuya promesa de valor es “Coomeva nos facilita la vida”, la satisfacción del cliente es uno de los principales indicadores y como tal se mide en todos los servicios que ofrece.

La Unidad de Tecnología Informática (UTI) es la proveedora de los servicios de tecnología para las cuatro (4) unidades y las dieciséis (16) empresas del grupo y dentro de su modelo de gestión, uno de sus principales indicadores es el de disponibilidad de su plataforma. Dentro de la UTI, el macro proceso de Infraestructura y Telecomunicaciones es el responsable de la gestión de toda la red de telecomunicaciones y servicios telemáticos que son utilizados por más de tres millones y medio (3´500.000) de clientes de todas las empresas a nivel nacional y doce mil (12.000) empleados directos que se conectan a la red de datos corporativa desde más de diez mil (10.000) estaciones de trabajo instaladas en alrededor de trescientos ochenta (380) sitios de la geografía Colombiana.

Para la aplicación del modelo propuesto se revisó con el macro proceso los diferentes servicios que desde allí se prestan a la organización y se seleccionaron los tres que mayor aporte hacen al indicador de disponibilidad de la red de datos corporativa, como factor determinante para la satisfacción de clientes tanto internos como externos y se priorizaron conforme a la importancia de cada uno de ellos frente a este indicador, arrojando los resultados mostrados en la Figura 30.

Figura 30. Vector de procesos de Telco priorizado **[5]**

Proceso	Adecuación de redes	Montaje de redes	Soporte y continuidad	TOTAL
Participación	50%	30%	20%	100%

6.2 Evaluación de activos.

Para la identificación de los activos que intervienen en la prestación de los tres servicios definidos dentro del alcance del análisis se recurrió a un ejercicio anterior realizado bajo las prácticas actuales y se verificó su consistencia con el ingeniero administrador de la plataforma de telecomunicaciones del GECC.

6.2.1 Identificación de activos.

El inventario de los activos identificados para los tres servicios dentro del alcance del análisis se complementó con la identificación del grupo de activos propuesto por el modelo (Información, Aplicaciones, Infraestructura, Personas, Servicios, Capital Financiero) arrojando los datos consignados en la Tabla 55.

Tabla 55. Inventario de activos Telco **[5]**

ID ACTIVO	IDENTIFICACIÓN			TIPO ACTIVO						COMENTARIO
	Nombre activo	Propietario	Administrador	Información	Aplicaciones	Infraestructura	Personas	Servicios	Capital financiero	
1	Ingenieros de Telemática	Infraestructura y telemática	Jefe infraestructura y telemática				X			Recurso humano del area de telecomunicaciones que desempeña el rol de administrador de infraestructura de telco
2	Analistas de telemática	Infraestructura y telemática	Jefe infraestructura y telemática				X			Recurso humano del area de telecomunicaciones que desempeña el rol de operador de infraestructura de telco
3	Documentación sistema de Calidad	Infraestructura y telemática	Ingeniero de Telemática	X						Documentación base para la prestación de los servicios - Procesos, Instructivos, etc
4	Carpeta Solicitud de Servicios	Infraestructura y telemática	Ingeniero de Telemática	X						Documentación red con servicios telemáticos implementados
5	Esquemas de red	Infraestructura y telemática	Ingeniero de Telemática	X						Planos físicos y lógicos del esquema de red de un sitio o nodo
6	Proveedores de telecomunicaciones	Proveedor equipos de telecomunicaciones	Jefe infraestructura y telemática					X		Terceros que prestan el servicio trasnporte de datos y de equipos de telecomunicaciones
7	Proveedores servicios de telefonia	Proveedor equipos de telefonía	Jefe infraestructura y telemática					X		Terceros que prestan el servicio y equipos de telefonia
8	Contratos	Coomeva	Director de Tecnología	X						Contratos firmados con los proveedores para la prestación de los servicios
9	Caja menor	Unidad de tecnología Informática	Asistente administrativa y financiera						X	Fondo de dinero controlado para gastos de emergencia
10	Servicio de Share Point	Centro de datos	Administrador Plataforma Windows			X				Repositorio de información donde residen copias del sistema operativo de los equipos de telecomunicaciones y servidor de gestión de telecomunicaciones
11	Equipos de telecomunicaciones	Proveedor servicio de telecomunicaciones	Ingeniero de Telemática			X				Hardware para la prestación de los servicios telemáticos
12	Equipos de telefonía	Proveedor servicios de telefonía	Ingeniero de Telemática			X				Hardware para la prestación de los servicios de telefonía
13	Redes WAN	Coomeva	Ingeniero de Telemática			X				Medios de comunicaciones que permiten la interconexión entre los nodos y el sitio central
14	Red LAN - Wireless	Coomeva	Ingeniero de Telemática			X				Medios de comunicaciones que permiten la interconexión de equipos.
15	Internet	Infraestructura y telemática	Jefe infraestructura y telemática			X				Medios de comunicaciones que permiten la interconexión a internet
16	Planes de mejoramiento	Infraestructura y telemática	Jefe infraestructura y telemática	X						Planes de trabajo sobre la mejora y eficacia en la prestación de los servicios telemáticos ofrecidos
17	Planes de continuidad	Infraestructura y telemática	Jefe infraestructura y telemática	X						Foma de operación ante una eventual falla para garantizar la continuidad en la prestación de los servicios
18	Registro de incidentes	Infraestructura y telemática	Jefe infraestructura y telemática	X						Herramienta en la cual se consigna la gestión de los incidentes relacionados con los servicios telemáticos
19	Servidor de Gestión	Infraestructura y telemática	Ingeniero de Telemática			X				Servidor en el cual se almacena la información relacionada con el servicio telemático
20	Software de registro de incidentes	Infraestructura y telemática	Ingeniero de Telemática		X					Herramienta para el registro, asignación y seguimiento de incidentes y solicitudes
21	Software de monitoreo	Infraestructura y telemática	Ingeniero de Telemática		X					Herramienta para el control y seguimiento de los servicios telemáticos

6.2.2 Valoración de activos.

Una vez levantado el inventario se realizó su valoración con los funcionarios del macro proceso de infraestructura y telecomunicaciones a cargo de la administración de estos activos, aplicando para cada activo las tablas de valoración de Confidencialidad, Integridad, Disponibilidad y Confiabilidad propuestas por el modelo, valorando de manera independiente cada atributo para cada uno de los tres procesos definidos dentro del alcance del análisis, dando como resultado la Tabla 56.

Tabla 56. Inventario de activos valorados **[5]**

ID ACTIVO	IDENTIFICACIÓN			ADECUACIÓN DE REDES				MONTAJE DE REDES				SOPORTE Y CONTINUIDAD			
				Peso proceso			50%	Peso proceso			30%	Peso proceso			20%
	Nombre activo	Propietario	Administrador	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	Confidencialidad	Integridad	Disponibilidad	Confiabilidad
1	Ingenieros de Telemática	Infraestructura y telemática	Jefe infraestructura y telemática	4	4	3	2	1	4	2	2	4	4	4	3
2	Analistas de telemática	Infraestructura y telemática	Jefe infraestructura y telemática	4	3	2	2	1	3	1	2	4	3	3	3
3	Documentación sistema de Calidad	Infraestructura y telemática	Ingeniero de Telemática	3	2	2	1	1	2	1	1	3	2	2	2
4	Carpeta Solicitud de Servicios	Infraestructura y telemática	Ingeniero de Telemática	2	4	3	2	3	4	1	1	2	4	3	3
5	Esquemas de red	Infraestructura y telemática	Ingeniero de Telemática	4	3	4	3	3	3	4	2	3	5	4	3
6	Proveedores de telecomunicaciones	Proveedor equipos de telecomunicaciones	Jefe infraestructura y telemática	1	4	3	4	1	4	4	4	1	2	5	5
7	Proveedores servicios de telefonia	Proveedor equipos de telefonía	Jefe infraestructura y telemática	1	4	3	3	2	4	3	3	1	2	4	4
8	Contratos	Coomeva	Director de Tecnología	3	3	1	1	3	4	3	2	3	4	3	1
9	Caja menor	Unidad de tecnología Informática	Asistente administrativa y financiera	1	1	2	1	1	1	3	2	1	2	3	3
10	Servicio de Share Point	Centro de datos	Administrador Plataforma Windows	3	4	3	3	3	3	2	3	3	4	4	3
11	Equipos de telecomunicaciones	Proveedor servicio de telecomunicaciones	Ingeniero de Telemática	4	4	3	4	1	3	3	3	4	4	5	5
12	Equipos de telefonía	Proveedor servicios de telefonía	Ingeniero de Telemática	3	3	3	3	1	2	2	2	3	3	4	4
13	Redes WAN	Coomeva	Ingeniero de Telemática	4	4	4	4	2	3	2	3	5	4	4	5
14	Red LAN - Wireless	Coomeva	Ingeniero de Telemática	4	3	4	3	3	2	2	2	4	4	3	4
15	Internet	Infraestructura y telemática	Jefe infraestructura y telemática	3	3	2	1	1	2	2	1	3	2	3	2
16	Planes de mejoramiento	Infraestructura y telemática	Jefe infraestructura y telemática	3	2	1	1	1	1	1	1	3	2	2	1
17	Planes de continuidad	Infraestructura y telemática	Jefe infraestructura y telemática	3	4	2	2	2	3	2	1	3	4	4	4
18	Registro de incidentes	Infraestructura y telemática	Jefe infraestructura y telemática	2	4	3	1	1	2	2	1	2	4	4	3
19	Servidor de Gestión	Infraestructura y telemática	Ingeniero de Telemática	3	4	3	3	2	3	3	3	3	4	4	4
20	Software de registro de incidentes	Infraestructura y telemática	Ingeniero de Telemática	2	3	3	2	1	1	2	1	2	4	3	3
21	Software de monitoreo	Infraestructura y telemática	Ingeniero de Telemática	2	3	3	3	1	2	2	2	2	4	4	3

6.2.2.1 Estimación del valor de activos.

Ya con la valoración de cada activo, en cada uno de los cuatro atributos propuestos por el modelo, para cada uno de los tres procesos dentro del alcance del análisis, se aplica la formula de valoración definida en el modelo, utilizando adicionalmente el atributo de colorimetría que dispone la hoja electrónica de uso común en Coomeva, con el resultado que se presenta en la Tabla 57, ordenado según el valor del activo resultante del cálculo numérico propuesto, desde el rojo, los más críticos o de mayor valor, hasta el verde, los menos críticos o de menor valor.

Tabla 57. Inventario activos de Telco valorado y priorizado **[5]**

ID ACTIVO	IDENTIFICACIÓN			TIPO ACTIVO						ADECUACIÓN DE REDES Peso proceso 50%				MONTAJE DE REDES Peso proceso 30%				SOPORTE Y CONTINUIDAD Peso proceso 20%				VALOR ACTIVO
	Nombre activo	Propietario	Administrador	Información	Aplicaciones	Infraestructura	Personas	Servicios	Capital financiero	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	
13	Redes WAN	Coomeva	Ingeniero de Telemática			X				4	4	4	4	2	3	2	3	5	4	4	5	14.6
11	Equipos de telecomunicaciones	Proveedor servicio de telecomunicaciones	Ingeniero de Telemática			X				4	4	3	4	1	3	3	3	4	4	5	5	14.1
5	Esquemas de red	Infraestructura y telemática	Ingeniero de Telemática	X						4	3	4	3	3	3	4	2	3	5	4	3	13.6
19	Servidor de Gestión	Infraestructura y telemática	Ingeniero de Telemática			X				3	4	3	3	2	3	3	3	3	4	4	4	12.8
14	Red LAN - Wireless	Coomeva	Ingeniero de Telemática			X				4	3	4	3	3	2	2	2	4	4	3	4	12.7
10	Servicio de Share Point	Centro de datos	Administrador Plataforma Windows			X				3	4	3	3	3	3	2	3	3	4	4	3	12.6
6	Proveedores de telecomunicaciones	Proveedor equipos de telecomunicaciones	Jefe infraestructura y telemática					X		1	4	3	4	1	4	4	4	1	2	5	5	12.5
1	Ingenieros de Telemática	Infraestructura y telemática	Jefe infraestructura y telemática				X			4	4	3	2	1	4	2	2	4	4	4	3	12.2
7	Proveedores servicios de telefonia	Proveedor equipos de telefonía	Jefe infraestructura y telemática					X		1	4	3	3	2	4	3	3	1	2	4	4	11.3
12	Equipos de telefonía	Proveedor servicios de telefonía	Ingeniero de Telemática			X				3	3	3	3	1	2	2	2	3	3	4	4	10.9
17	Planes de continuidad	Infraestructura y telemática	Jefe infraestructura y telemática	X						3	4	2	2	2	3	2	1	3	4	4	4	10.9
4	Carpeta Solicitud de Servicios	Infraestructura y telemática	Ingeniero de Telemática	X						2	4	3	2	3	4	1	1	2	4	3	3	10.6
2	Analistas de telemática	Infraestructura y telemática	Jefe infraestructura y telemática				X			4	3	2	2	1	3	1	2	4	3	3	3	10.2
21	Software de monitoreo	Infraestructura y telemática	Ingeniero de Telemática		X					2	3	3	3	1	2	2	2	2	4	4	3	10.2
8	Contratos	Coomeva	Director de Tecnología	X						3	3	1	1	3	4	3	2	3	4	3	1	9.8
18	Registro de incidentes	Infraestructura y telemática	Jefe infraestructura y telemática	X						2	4	3	1	1	2	2	1	2	4	4	3	9.4
20	Software de registro de incidentes	Infraestructura y telemática	Ingeniero de Telemática		X					2	3	3	2	1	1	2	1	2	4	3	3	8.9
15	Internet	Infraestructura y telemática	Jefe infraestructura y telemática			X				3	3	2	1	1	2	2	1	3	2	3	2	8.3
3	Documentación sistema de Calidad	Infraestructura y telemática	Ingeniero de Telemática	X						3	2	2	1	1	2	1	1	3	2	2	2	7.3
9	Caja menor	Unidad de tecnología Informática	Asistente administrativa y financiera						X	1	1	2	1	1	1	3	2	1	2	3	3	6.4
16	Planes de mejoramiento	Infraestructura y telemática	Jefe infraestructura y telemática	X						3	2	1	1	1	1	1	1	3	2	2	1	6.3

6.3 Evaluación de riesgos.

Esta fase fue la que representó mayor cambio frente al modelo que se viene aplicando para este proceso en Coomeva, dado que en este paso se agrupaban los activos según su tipo y la identificación y valoración de los riesgos se hacía sobre el grupo de activos y no sobre los activos individuales, tal como se plantea en el modelo propuesto.

6.3.1 Identificación de riesgos.

Para la identificación de las amenazas de cada uno de los activos se recurrió a las tablas propuestas en el ANEXO D, según el grupo a que corresponde cada activo identificado en la fase anterior. Cuando la cantidad de amenazas era muy alta (más de veinte), se evalúo cuál era el atributo con mayor valoración global para el activo evaluado y si al tomar las amenazas bajo este atributo, también se cubrían las del segundo, hasta lograr un número manejable de amenazas para el activo (máximo veinte), obteniendo la Tabla 58.

Tabla 58. Inventario de Activos de Telco con sus amenazas **[5]**

ID ACTIVO	IDENTIFICACIÓN			VALOR CONSOLIDADO ACTIVO					AMENAZAS	
	Nombre activo	Propietario	Administrador	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	TOTAL	ID	DESCRIPCIÓN
1	Ingenieros de Telemática	Infraestructura y telemática	Jefe infraestructura y telemática	3.1	4	2.9	2.2	12.2	E7	Deficiencias en la organización
									E28	Indisponibilidad accidental del personal
									A28	Indisponibilidad deliberada del personal
									A29	Extorsión
									A30	Ingeniería social
2	Analistas de telemática	Infraestructura y telemática	Jefe infraestructura y telemática	3.1	3	1.9	2.2	10.2	E7	Deficiencias en la organización
									E28	Indisponibilidad accidental del personal
									A28	Indisponibilidad deliberada del personal
									A29	Extorsión
									A30	Ingeniería social
3	Documentación sistema de Calidad	Infraestructura y telemática	Ingeniero de Telemática	2.4	2	1.7	1.2	7.3	E2	Errores del administrador
									E4	Errores de configuración
									E14	Escapes de información
									E19	Divulgación de información por indiscreción
									A4	Manipulación de la configuración
									A11	Acceso no autorizado
									A14	Interceptación de información (escucha)
									A19	Divulgación de información (intencional)
									A25	Robo
4	Carpeta Solicitud de Servicios	Infraestructura y telemática	Ingeniero de Telemática	2.3	4	2.4	1.9	10.6	N1	Fuego (sin intervención humana)
									N2	Daños por agua (sin intervención humana)
									N*	Desastres naturales
									I1	Fuego (con intervención humana)
									I2	Daños por agua (con intervención humana)
									I*	Desastres industriales
									I3	Contaminación mecánica
									I4	Contaminación electromagnética
									I5	Avería de origen físico o lógico
									I6	Corte del suministro eléctrico
									I7	Condiciones inadecuadas de temperatura y/o humedad
									I10	Degradación de los soportes de almacenamiento de la información
									E1	Errores de los usuarios
									E2	Errores del administrador
									E4	Errores de configuración
									E18	Destrucción de información
									A4	Manipulación de la configuración
									A18	Destrucción la información (intencional)
									A25	Robo
									A26	Ataque destructivo
5	Esquemas de red	Infraestructura y telemática	Ingeniero de Telemática	3.5	3.4	4	2.7	13.6	N1	Fuego (sin intervención humana)
									N2	Daños por agua (sin intervención humana)
									N*	Desastres naturales
									I1	Fuego (con intervención humana)
									I2	Daños por agua (con intervención humana)
									I*	Desastres industriales
									I3	Contaminación mecánica
									I4	Contaminación electromagnética
									I5	Avería de origen físico o lógico
									I6	Corte del suministro eléctrico
									I7	Condiciones inadecuadas de temperatura y/o humedad
									I10	Degradación de los soportes de almacenamiento de la información
									E1	Errores de los usuarios
									E2	Errores del administrador
									E4	Errores de configuración
									E18	Destrucción de información
									A4	Manipulación de la configuración
									A18	Destrucción la información (intencional)
									A25	Robo
									A26	Ataque destructivo

Tabla 58. Inventario de Activos de Telco con sus amenazas [5] (Continuación)

ID ACTIVO	IDENTIFICACIÓN			VALOR CONSOLIDADO ACTIVO					AMENAZAS	
	Nombre activo	Propietario	Administrador	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	TOTAL	ID	DESCRIPCIÓN
6	Proveedores de telecomunicaciones	Proveedor equipos de telecomunicaciones	Jefe infraestructura y telemática	1	3.6	3.7	4.2	12.5	N1	Fuego (sin intervención humana)
									N2	Daños por agua (sin intervención humana)
									N*	Desastres naturales
									I1	Fuego (con intervención humana)
									I2	Daños por agua (con intervención humana)
									I*	Desastres industriales
									I3	Contaminación mecánica
									I4	Contaminación electromagnética
									I6	Corte del suministro eléctrico
									I7	Condiciones inadecuadas de temperatura y/o humedad
									I8	Fallo de servicios de comunicaciones
									I9	Interrupción de otros servicios y suministros esenciales
									E1	Errores de los usuarios
									E2	Errores del administrador
									E4	Errores de configuración
									E24	Caída del sistema por agotamiento de recursos
									A4	Manipulación de la configuración
									A7	Uso no previsto
									A24	Denegación de servicio
									A26	Ataque destructivo
7	Proveedores servicios de telefonia	Proveedor equipos de telefonía	Jefe infraestructura y telemática	1.3	3.6	3.2	3.2	11.3	N1	Fuego (sin intervención humana)
									N2	Daños por agua (sin intervención humana)
									N*	Desastres naturales
									I1	Fuego (con intervención humana)
									I2	Daños por agua (con intervención humana)
									I*	Desastres industriales
									I3	Contaminación mecánica
									I4	Contaminación electromagnética
									I6	Corte del suministro eléctrico
									I7	Condiciones inadecuadas de temperatura y/o humedad
									I8	Fallo de servicios de comunicaciones
									I9	Interrupción de otros servicios y suministros esenciales
									E1	Errores de los usuarios
									E2	Errores del administrador
									E4	Errores de configuración
									E24	Caída del sistema por agotamiento de recursos
									A4	Manipulación de la configuración
									A7	Uso no previsto
									A24	Denegación de servicio
									A26	Ataque destructivo
8	Contratos	Coomeva	Director de Tecnología	3	3.5	2	1.3	9.8	E2	Errores del administrador
									E4	Errores de configuración
									E14	Escapes de información
									E19	Divulgación de información por indiscreción
									A4	Manipulación de la configuración
									A11	Acceso no autorizado
									A14	Interceptación de información (escucha)
									A19	Divulgación de información (intencional)
									A25	Robo
9	Caja menor	Unidad de tecnología Informática	Asistente administrativa y financiera	1	1.2	2.5	1.7	6.4	A7	Uso no previsto
									A11	Acceso no autorizado
									A25	Robo
10	Servicio de Share Point	Centro de datos	Administrador Plataforma Windows	3	3.7	2.9	3	12.6	I11	Emanaciones electromagnéticas
									E2	Errores del administrador
									E4	Errores de configuración
									E9	Errores de re-encaminamiento
									E14	Escapes de información
									A4	Manipulación de la configuración
									A5	Suplantación de la identidad del usuario
									A6	Abuso de privilegios de acceso
									A9	Re-encaminamiento intencional de mensajes
									A11	Acceso no autorizado
									A12	Análisis de tráfico
									A14	Interceptación de información (escucha)
									A25	Robo
									A27	Ocupación no autorizada
11	Equipos de telecomunicaciones	Proveedor servicio de telecomunicaciones	Ingeniero de Telemática	3.1	3.7	3.4	3.9	14.1	N1	Fuego (sin intervención humana)
									N2	Daños por agua (sin intervención humana)
									N*	Desastres naturales
									I1	Fuego (con intervención humana)
									I2	Daños por agua (con intervención humana)
									I*	Desastres industriales
									I3	Contaminación mecánica
									I4	Contaminación electromagnética
									I5	Avería de origen físico o lógico
									I6	Corte del suministro eléctrico
									I7	Condiciones inadecuadas de temperatura y/o humedad
									E2	Errores del administrador
									E4	Errores de configuración
									E23	Errores de mantenimiento / actualización de equipos (hardware)
									E24	Caída del sistema por agotamiento de recursos
									A4	Manipulación de la configuración
									A7	Uso no previsto
									A24	Denegación de servicio
									A25	Robo
									A26	Ataque destructivo
									A27	Ocupación no autorizada

Tabla 58. Inventario de Activos de Telco con sus amenazas [5] (Continuación)

ID ACTIVO	IDENTIFICACIÓN			VALOR CONSOLIDADO ACTIVO					AMENAZAS	
	Nombre activo	Propietario	Administrador	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	TOTAL	ID	DESCRIPCIÓN
12	Equipos de telefonía	Proveedor servicios de telefonía	Ingeniero de Telemática	2.4	2.7	2.9	2.9	10.9	N1	Fuego (sin intervención humana)
									N2	Daños por agua (sin intervención humana)
									N*	Desastres naturales
									I1	Fuego (con intervención humana)
									I2	Daños por agua (con intervención humana)
									I*	Desastres industriales
									I3	Contaminación mecánica
									I4	Contaminación electromagnética
									I5	Avería de origen físico o lógico
									I6	Corte del suministro eléctrico
									I7	Condiciones inadecuadas de temperatura y/o humedad
									E2	Errores del administrador
									E4	Errores de configuración
									E23	Errores de mantenimiento / actualización de equipos (hardware)
									E24	Caída del sistema por agotamiento de recursos
									A4	Manipulación de la configuración
									A7	Uso no previsto
									A24	Denegación de servicio
									A25	Robo
									A26	Ataque destructivo
									A27	Ocupación no autorizada
13	Redes WAN	Coomeva	Ingeniero de Telemática	3.6	3.7	3.4	3.9	14.6	I11	Emanaciones electromagnéticas
									E2	Errores del administrador
									E4	Errores de configuración
									E9	Errores de re-encaminamiento
									E14	Escapes de información
									A4	Manipulación de la configuración
									A5	Suplantación de la identidad del usuario
									A6	Abuso de privilegios de acceso
									A9	Re-encaminamiento intencional de mensajes
									A11	Acceso no autorizado
									A12	Análisis de tráfico
									A14	Interceptación de información (escucha)
									A25	Robo
									A27	Ocupación no autorizada
14	Red LAN - Wireless	Coomeva	Ingeniero de Telemática	3.7	2.9	3.2	2.9	12.7	I11	Emanaciones electromagnéticas
									E2	Errores del administrador
									E4	Errores de configuración
									E9	Errores de re-encaminamiento
									E14	Escapes de información
									A4	Manipulación de la configuración
									A5	Suplantación de la identidad del usuario
									A6	Abuso de privilegios de acceso
									A9	Re-encaminamiento intencional de mensajes
									A11	Acceso no autorizado
									A12	Análisis de tráfico
									A14	Interceptación de información (escucha)
									A25	Robo
									A27	Ocupación no autorizada
15	Internet	Infraestructura y telemática	Jefe infraestructura y telemática	2.4	2.5	2.2	1.2	8.3	I11	Emanaciones electromagnéticas
									E2	Errores del administrador
									E4	Errores de configuración
									E9	Errores de re-encaminamiento
									E14	Escapes de información
									A4	Manipulación de la configuración
									A5	Suplantación de la identidad del usuario
									A6	Abuso de privilegios de acceso
									A9	Re-encaminamiento intencional de mensajes
									A11	Acceso no autorizado
									A12	Análisis de tráfico
									A14	Interceptación de información (escucha)
									A25	Robo
									A27	Ocupación no autorizada
16	Planes de mejoramiento	Infraestructura y telemática	Jefe infraestructura y telemática	2.4	1.7	1.2	1	6.3	E2	Errores del administrador
									E4	Errores de configuración
									E14	Escapes de información
									E19	Divulgación de información por indiscreción
									A4	Manipulación de la configuración
									A11	Acceso no autorizado
									A14	Interceptación de información (escucha)
									A19	Divulgación de información (intencional)
									A25	Robo
17	Planes de continuidad	Infraestructura y telemática	Jefe infraestructura y telemática	2.7	3.7	2.4	2.1	10.9	E1	Errores de los usuarios
									E2	Errores del administrador
									E3	Errores de monitorización (log)
									E4	Errores de configuración
									E15	Alteración de la información
									E16	Introducción de información incorrecta
									E17	Degradación de la información
									A4	Manipulación de la configuración
									A11	Acceso no autorizado
									A15	Modificación de la información (intencional)
									A16	Introducción de falsa información
									A17	Corrupción de la información (intencional)

Tabla 58. Inventario de Activos de Telco con sus amenazas [5] (Continuación)

ID ACTIVO	IDENTIFICACIÓN			VALOR CONSOLIDADO ACTIVO					AMENAZAS	
	Nombre activo	Propietario	Administrador	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	TOTAL	ID	DESCRIPCIÓN
18	Registro de incidentes	Infraestructura y telemática	Jefe infraestructura y telemática	1.7	3.4	2.9	1.4	9.4	E1	Errores de los usuarios
									E2	Errores del administrador
									E3	Errores de monitorización (log)
									E4	Errores de configuración
									E15	Alteración de la información
									E16	Introducción de información incorrecta
									E17	Degradación de la información
									A4	Manipulación de la configuración
									A11	Acceso no autorizado
									A15	Modificación de la información (intencional)
									A16	Introducción de falsa información
									A17	Corrupción de la información (intencional)
19	Servidor de Gestión	Infraestructura y telemática	Ingeniero de Telemática	2.7	3.7	3.2	3.2	12.8	E2	Errores del administrador
									E4	Errores de configuración
									E9	Errores de re-encaminamiento
									E10	Errores de secuencia
									A4	Manipulación de la configuración
									A5	Suplantación de la identidad del usuario
									A6	Abuso de privilegios de acceso
									A9	Re-encaminamiento intencional de mensajes
									A10	Alteración de secuencia
									A11	Acceso no autorizado
20	Software de registro de incidentes	Infraestructura y telemática	Ingeniero de Telemática	1.7	2.6	2.7	1.9	8.9	E1	Errores de los usuarios
									E2	Errores del administrador
									E3	Errores de monitorización (log)
									E4	Errores de configuración
									E8	Difusión de software dañino
									E9	Errores de re-encaminamiento
									E10	Errores de secuencia
									E20	Vulnerabilidades de los programas (software)
									E21	Errores de mantenimiento / actualización de programas (software)
									A4	Manipulación de la configuración
									A5	Suplantación de la identidad del usuario
									A6	Abuso de privilegios de acceso
									A8	Difusión deliberada de software dañino
									A9	Re-encaminamiento intencional de mensajes
									A10	Alteración de secuencia
									A11	Acceso no autorizado
									A22	Manipulación de programas
21	Software de monitoreo	Infraestructura y telemática	Ingeniero de Telemática	1.7	2.9	2.9	2.7	10.2	E1	Errores de los usuarios
									E2	Errores del administrador
									E3	Errores de monitorización (log)
									E4	Errores de configuración
									E8	Difusión de software dañino
									E9	Errores de re-encaminamiento
									E10	Errores de secuencia
									E20	Vulnerabilidades de los programas (software)
									E21	Errores de mantenimiento / actualización de programas (software)
									A4	Manipulación de la configuración
									A5	Suplantación de la identidad del usuario
									A6	Abuso de privilegios de acceso
									A8	Difusión deliberada de software dañino
									A9	Re-encaminamiento intencional de mensajes
									A10	Alteración de secuencia
									A11	Acceso no autorizado
									A22	Manipulación de programas

6.3.2 Identificación de controles.

Para este paso se verificó con los administradores de la plataforma la existencia de controles que pudieran mitigar cada una de las amenazas identificadas para cada activo y el grado de confiabilidad que cada uno de estos controles ofrece, a la luz de lo propuesto en el modelo.

6.3.2.1 Estimación de eficiencia de salvaguardas.

Una vez evaluada la existencia, robustez, automatización y efectividad de controles para cada una de las amenazas de cada activo, se obtuvo la Tabla 59 valorada en su nivel de mitigación según la escala cualitativa que propone el modelo para los distintos niveles de solidez del control (para efectos de descongestionar la tabla se omiten las columnas Propietario y Administrador).

Tabla 59. Activos, Amenazas y Salvaguardas de Telco **[5]**

ID ACTIVO	IDENTIFICACIÓN	VALOR CONSOLIDADO ACTIVO					AMENAZAS		SALVAGUARDAS		
	Nombre activo	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	TOTAL	ID	DESCRIPCIÓN	Posee un control	Solidez del control	Nivel de mitigación
1	Ingenieros de Telemática	3.1	4	2.9	2.2	12.2	E7	Deficiencias en la organización	Si	Adecuado	0.7
							E28	Indisponibilidad accidental del personal	Si	Adecuado	0.7
							A28	Indisponibilidad deliberada del personal	Si	Adecuado	0.7
							A29	Extorsión	No	No existente	0.0
							A30	Ingeniería social	No	No existente	0.0
2	Analistas de telemática	3.1	3	1.9	2.2	10.2	E7	Deficiencias en la organización	Si	Adecuado	0.7
							E28	Indisponibilidad accidental del personal	Si	Adecuado	0.7
							A28	Indisponibilidad deliberada del personal	Si	Adecuado	0.7
							A29	Extorsión	No	No existente	0.0
							A30	Ingeniería social	No	No existente	0.0
3	Documentación sistema de Calidad	2.4	2	1.7	1.2	7.3	E2	Errores del administrador	Si	Moderado	0.5
							E4	Errores de configuración	Si	Adecuado	0.7
							E14	Escapes de información	Si	Adecuado	0.7
							E19	Divulgación de información por indiscreción	Si	Moderado	0.5
							A4	Manipulación de la configuración	Si	Adecuado	0.7
							A11	Acceso no autorizado	Si	Adecuado	0.7
							A14	Interceptación de información (escucha)	Si	Adecuado	0.7
							A19	Divulgación de información (intencional)	Si	Débil	0.3
							A25	Robo	Si	Moderado	0.5
4	Carpeta Solicitud de Servicios	2.3	4	2.4	1.9	10.6	N1	Fuego (sin intervención humana)	Si	Adecuado	0.7
							N2	Daños por agua (sin intervención humana)	No	No existente	0.0
							N*	Desastres naturales	Si	Moderado	0.5
							I1	Fuego (con intervención humana)	Si	Adecuado	0.7
							I2	Daños por agua (con intervención humana)	No	No existente	0.0
							I*	Desastres industriales	No	No existente	0.0
							I3	Contaminación mecánica	No	No existente	0.0
							I4	Contaminación electromagnética	No	No existente	0.0
							I5	Avería de origen físico o lógico	Si	Adecuado	0.7
							I6	Corte del suministro eléctrico	Si	Adecuado	0.7
							I7	Condiciones inadecuadas de temperatura y/o humedad	Si	Muy Adecuado	0.9
							I10	Degradación de los soportes de almacenamiento de la información	Si	Muy Adecuado	0.9
							E1	Errores de los usuarios	Si	Moderado	0.5
							E2	Errores del administrador	Si	Adecuado	0.7
							E4	Errores de configuración	Si	Adecuado	0.7
							E18	Destrucción de información	Si	Adecuado	0.7
							A4	Manipulación de la configuración	Si	Muy Adecuado	0.9
							A18	Destrucción la información (intencional)	Si	Adecuado	0.7
							A25	Robo	Si	Muy Adecuado	0.9
							A26	Ataque destructivo	Si	Adecuado	0.7

Tabla 59. Activos, Amenazas y Salvaguardas de Telco **[5]** (Continuación)

ID ACTIVO	IDENTIFICACIÓN	VALOR CONSOLIDADO ACTIVO					AMENAZAS		SALVAGURADAS		
	Nombre activo	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	TOTAL	ID	DESCRIPCIÓN	Posee un control	Solidez del control	Nivel de mitigación
5	Esquemas de red	3.5	3.4	4	2.7	13.6	N1	Fuego (sin intervención humana)	Si	Adecuado	0.7
							N2	Daños por agua (sin intervención humana)	No	No existente	0.0
							N*	Desastres naturales	Si	Moderado	0.5
							I1	Fuego (con intervención humana)	Si	Adecuado	0.7
							I2	Daños por agua (con intervención humana)	No	No existente	0.0
							I*	Desastres industriales	No	No existente	0.0
							I3	Contaminación mecánica	No	No existente	0.0
							I4	Contaminación electromagnética	No	No existente	0.0
							I5	Avería de origen físico o lógico	Si	Adecuado	0.7
							I6	Corte del suministro eléctrico	Si	Adecuado	0.7
							I7	Condiciones inadecuadas de temperatura y/o humedad	Si	Adecuado	0.7
							I10	Degradación de los soportes de almacenamiento de la información	Si	Muy Adecuado	0.9
							E1	Errores de los usuarios	Si	Moderado	0.5
							E2	Errores del administrador	Si	Adecuado	0.7
							E4	Errores de configuración	Si	Adecuado	0.7
							E18	Destrucción de información	Si	Adecuado	0.7
							A4	Manipulación de la configuración	Si	Muy Adecuado	0.9
							A18	Destrucción la información (intencional)	Si	Adecuado	0.7
							A25	Robo	Si	Muy Adecuado	0.9
							A26	Ataque destructivo	Si	Adecuado	0.7
6	Proveedores de telecomunicaciones	1	3.6	3.7	4.2	12.5	N1	Fuego (sin intervención humana)	Si	Adecuado	0.7
							N2	Daños por agua (sin intervención humana)	No	Muy débil	0.0
							N*	Desastres naturales	Si	Muy débil	0.1
							I1	Fuego (con intervención humana)	Si	Adecuado	0.7
							I2	Daños por agua (con intervención humana)	No	No existente	0.0
							I*	Desastres industriales	No	No existente	0.0
							I3	Contaminación mecánica	No	No existente	0.0
							I4	Contaminación electromagnética	No	No existente	0.0
							I6	Corte del suministro eléctrico	Si	Adecuado	0.7
							I7	Condiciones inadecuadas de temperatura y/o humedad	Si	Adecuado	0.7
							I8	Fallo de servicios de comunicaciones	Si	Adecuado	0.7
							I9	Interrupción de otros servicios y suministros esenciales	Si	Adecuado	0.7
							E1	Errores de los usuarios	Si	Adecuado	0.7
							E2	Errores del administrador	Si	Moderado	0.5
							E4	Errores de configuración	Si	Moderado	0.5
							E24	Caída del sistema por agotamiento de recursos	Si	Moderado	0.5
							A4	Manipulación de la configuración	Si	Moderado	0.5
							A7	Uso no previsto	Si	Adecuado	0.7
							A24	Denegación de servicio	Si	Adecuado	0.7
							A26	Ataque destructivo	Si	Adecuado	0.7
7	Proveedores servicios de telefonia	1.3	3.6	3.2	3.2	11.3	N1	Fuego (sin intervención humana)	Si	Adecuado	0.7
							N2	Daños por agua (sin intervención humana)	No	Adecuado	0.0
							N*	Desastres naturales	Si	Moderado	0.5
							I1	Fuego (con intervención humana)	Si	Adecuado	0.7
							I2	Daños por agua (con intervención humana)	No	No existente	0.0
							I*	Desastres industriales	No	No existente	0.0
							I3	Contaminación mecánica	No	No existente	0.0
							I4	Contaminación electromagnética	No	No existente	0.0
							I6	Corte del suministro eléctrico	Si	Adecuado	0.7
							I7	Condiciones inadecuadas de temperatura y/o humedad	Si	Adecuado	0.7
							I8	Fallo de servicios de comunicaciones	Si	Adecuado	0.7
							I9	Interrupción de otros servicios y suministros esenciales	Si	Adecuado	0.7
							E1	Errores de los usuarios	Si	Adecuado	0.7
							E2	Errores del administrador	Si	Moderado	0.5
							E4	Errores de configuración	Si	Moderado	0.5
							E24	Caída del sistema por agotamiento de recursos	Si	Moderado	0.5
							A4	Manipulación de la configuración	Si	Moderado	0.5
							A7	Uso no previsto	Si	Adecuado	0.7
							A24	Denegación de servicio	Si	Adecuado	0.7
							A26	Ataque destructivo	Si	Adecuado	0.7
8	Contratos	3	3.5	2	1.3	9.8	E2	Errores del administrador	Si	Muy Adecuado	0.9
							E4	Errores de configuración	Si	Muy Adecuado	0.9
							E14	Escapes de información	Si	Adecuado	0.7
							E19	Divulgación de información por indiscreción	Si	Adecuado	0.7
							A4	Manipulación de la configuración	Si	Muy Adecuado	0.9
							A11	Acceso no autorizado	Si	Moderado	0.5
							A14	Interceptación de información (escucha)	Si	Moderado	0.5
							A19	Divulgación de información (intencional)	Si	Adecuado	0.7
							A25	Robo	Si	Muy Adecuado	0.9

Tabla 59. Activos, Amenazas y Salvaguardas de Telco **[5]** (Continuación)

ID ACTIVO	IDENTIFICACIÓN	VALOR CONSOLIDADO ACTIVO					AMENAZAS		SALVAGUARDAS		
	Nombre activo	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	TOTAL	ID	DESCRIPCIÓN	Posee un control	Solidez del control	Nivel de mitigación
9	Caja menor	1	1.2	2.5	1.7	6.4	A7	Uso no previsto	Si	Adecuado	0.7
							A11	Acceso no autorizado	Si	Muy Adecuado	0.9
							A25	Robo	Si	Adecuado	0.7
10	Servicio de Share Point	3	3.7	2.9	3	12.6	I11	Emanaciones electromagnéticas	No	No existente	0.0
							E2	Errores del administrador	No	No existente	0.0
							E4	Errores de configuración	Si	Moderado	0.5
							E9	Errores de re-encaminamiento	No	No existente	0.0
							E14	Escapes de información	Si	Débil	0.3
							A4	Manipulación de la configuración	Si	Adecuado	0.7
							A5	Suplantación de la identidad del usuario	Si	Moderado	0.5
							A6	Abuso de privilegios de acceso	Si	Adecuado	0.7
							A9	Re-encaminamiento intencional de mensajes	No	No existente	0.0
							A11	Acceso no autorizado	Si	Adecuado	0.7
							A12	Análisis de tráfico	Si	Moderado	0.5
							A14	Interceptación de información (escucha)	Si	Moderado	0.5
							A25	Robo	Si	Muy Adecuado	0.9
							A27	Ocupación no autorizada	Si	Adecuado	0.7
11	Equipos de telecomunicaciones	3.1	3.7	3.4	3.9	14.1	N1	Fuego (sin intervención humana)	Si	Adecuado	0.7
							N2	Daños por agua (sin intervención humana)	No	No existente	0.0
							N*	Desastres naturales	Si	Moderado	0.5
							I1	Fuego (con intervención humana)	Si	Adecuado	0.7
							I2	Daños por agua (con intervención humana)	No	No existente	0.0
							I*	Desastres industriales	No	No existente	0.0
							I3	Contaminación mecánica	No	No existente	0.0
							I4	Contaminación electromagnética	No	No existente	0.0
							I5	Avería de origen físico o lógico	Si	Adecuado	0.7
							I6	Corte del suministro eléctrico	Si	Adecuado	0.7
							I7	Condiciones inadecuadas de temperatura y/o humedad	Si	Adecuado	0.7
							E2	Errores del administrador	Si	Adecuado	0.7
							E4	Errores de configuración	Si	Muy Adecuado	0.9
							E23	Errores de mantenimiento / actualización de equipos (hardware)	Si	Adecuado	0.7
							E24	Caída del sistema por agotamiento de recursos	Si	Adecuado	0.7
							A4	Manipulación de la configuración	Si	Muy Adecuado	0.9
							A7	Uso no previsto	Si	Adecuado	0.7
							A24	Denegación de servicio	Si	Adecuado	0.7
							A25	Robo	Si	Adecuado	0.7
							A26	Ataque destructivo	Si	Adecuado	0.7
							A27	Ocupación no autorizada	Si	Adecuado	0.7
12	Equipos de telefonía	2.4	2.7	2.9	2.9	10.9	N1	Fuego (sin intervención humana)	Si	Adecuado	0.7
							N2	Daños por agua (sin intervención humana)	No	No existente	0.0
							N*	Desastres naturales	Si	Moderado	0.5
							I1	Fuego (con intervención humana)	Si	Adecuado	0.7
							I2	Daños por agua (con intervención humana)	No	No existente	0.0
							I*	Desastres industriales	No	No existente	0.0
							I3	Contaminación mecánica	No	No existente	0.0
							I4	Contaminación electromagnética	No	No existente	0.0
							I5	Avería de origen físico o lógico	Si	Adecuado	0.7
							I6	Corte del suministro eléctrico	Si	Adecuado	0.7
							I7	Condiciones inadecuadas de temperatura y/o humedad	Si	Adecuado	0.7
							E2	Errores del administrador	Si	Adecuado	0.7
							E4	Errores de configuración	Si	Muy Adecuado	0.9
							E23	Errores de mantenimiento / actualización de equipos (hardware)	Si	Adecuado	0.7
							E24	Caída del sistema por agotamiento de recursos	Si	Adecuado	0.7
							A4	Manipulación de la configuración	Si	Muy Adecuado	0.9
							A7	Uso no previsto	Si	Adecuado	0.7
							A24	Denegación de servicio	Si	Adecuado	0.7
							A25	Robo	Si	Adecuado	0.7
							A26	Ataque destructivo	Si	Adecuado	0.7
							A27	Ocupación no autorizada	Si	Adecuado	0.7

Tabla 59. Activos, Amenazas y Salvaguardas de Telco **[5]** (Continuación)

ID ACTIVO	IDENTIFICACIÓN	VALOR CONSOLIDADO ACTIVO					AMENAZAS		SALVAGUARDAS		
	Nombre activo	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	TOTAL	ID	DESCRIPCIÓN	Posee un control	Solidez del control	Nivel de mitigación
13	Redes WAN	3.6	3.7	3.4	3.9	14.6	I11	Emanaciones electromagnéticas	No	No existente	0.0
							E2	Errores del administrador	Si	Muy Adecuado	0.9
							E4	Errores de configuración	Si	Muy Adecuado	0.9
							E9	Errores de re-encaminamiento	Si	Muy Adecuado	0.9
							E14	Escapes de información	Si	Adecuado	0.7
							A4	Manipulación de la configuración	Si	Muy Adecuado	0.9
							A5	Suplantación de la identidad del usuario	Si	Muy Adecuado	0.9
							A6	Abuso de privilegios de acceso	Si	Muy Adecuado	0.9
							A9	Re-encaminamiento intencional de mensajes	Si	Muy Adecuado	0.9
							A11	Acceso no autorizado	Si	Muy Adecuado	0.9
							A12	Análisis de tráfico	Si	Moderado	0.5
							A14	Interceptación de información (escucha)	Si	Moderado	0.5
							A25	Robo	Si	Adecuado	0.7
							A27	Ocupación no autorizada	Si	Adecuado	0.7
14	Red LAN - Wireless	3.7	2.9	3.2	2.9	12.7	I11	Emanaciones electromagnéticas	No	No existente	0.0
							E2	Errores del administrador	Si	Muy Adecuado	0.9
							E4	Errores de configuración	Si	Muy Adecuado	0.9
							E9	Errores de re-encaminamiento	Si	Muy Adecuado	0.9
							E14	Escapes de información	Si	Adecuado	0.7
							A4	Manipulación de la configuración	Si	Muy Adecuado	0.9
							A5	Suplantación de la identidad del usuario	Si	Muy Adecuado	0.9
							A6	Abuso de privilegios de acceso	Si	Muy Adecuado	0.9
							A9	Re-encaminamiento intencional de mensajes	Si	Muy Adecuado	0.9
							A11	Acceso no autorizado	Si	Muy Adecuado	0.9
							A12	Análisis de tráfico	Si	Moderado	0.5
							A14	Interceptación de información (escucha)	Si	Moderado	0.5
							A25	Robo	Si	Adecuado	0.7
							A27	Ocupación no autorizada	Si	Adecuado	0.7
15	Internet	2.4	2.5	2.2	1.2	8.3	I11	Emanaciones electromagnéticas	No	No existente	0.0
							E2	Errores del administrador	Si	Muy Adecuado	0.9
							E4	Errores de configuración	Si	Adecuado	0.7
							E9	Errores de re-encaminamiento	Si	Muy Adecuado	0.9
							E14	Escapes de información	Si	Adecuado	0.7
							A4	Manipulación de la configuración	Si	Adecuado	0.7
							A5	Suplantación de la identidad del usuario	Si	Muy Adecuado	0.9
							A6	Abuso de privilegios de acceso	Si	Adecuado	0.7
							A9	Re-encaminamiento intencional de mensajes	Si	Muy Adecuado	0.9
							A11	Acceso no autorizado	Si	Adecuado	0.7
							A12	Análisis de tráfico	Si	Moderado	0.5
							A14	Interceptación de información (escucha)	Si	Moderado	0.5
							A25	Robo	Si	Adecuado	0.7
							A27	Ocupación no autorizada	Si	Adecuado	0.7
16	Planes de mejoramiento	2.4	1.7	1.2	1	6.3	E2	Errores del administrador	No	No existente	0.0
							E4	Errores de configuración	Si	Moderado	0.5
							E14	Escapes de información	Si	Moderado	0.5
							E19	Divulgación de información por indiscreción	Si	Moderado	0.5
							A4	Manipulación de la configuración	Si	Moderado	0.5
							A11	Acceso no autorizado	Si	Adecuado	0.7
							A14	Interceptación de información (escucha)	Si	Moderado	0.5
							A19	Divulgación de información (intencional)	Si	Débil	0.3
							A25	Robo	Si	Adecuado	0.7
17	Planes de continuidad	2.7	3.7	2.4	2.1	10.9	E1	Errores de los usuarios	Si	Débil	0.3
							E2	Errores del administrador	No	No existente	0.0
							E3	Errores de monitorización (log)	Si	Muy débil	0.1
							E4	Errores de configuración	Si	Moderado	0.5
							E15	Alteración de la información	Si	Muy débil	0.1
							E16	Introducción de información incorrecta	Si	Moderado	0.5
							E17	Degradación de la información	Si	Moderado	0.5
							A4	Manipulación de la configuración	Si	Moderado	0.5
							A11	Acceso no autorizado	Si	Adecuado	0.7
							A15	Modificación de la información (intencional)	Si	Adecuado	0.7
							A16	Introducción de falsa información	Si	Adecuado	0.7
							A17	Corrupción de la información (intencional)	Si	Adecuado	0.7

Tabla 59. Activos, Amenazas y Salvaguardas de Telco **[5]** (Continuación)

ID ACTIVO	IDENTIFICACIÓN	VALOR CONSOLIDADO ACTIVO					AMENAZAS		SALVAGUARDAS		
	Nombre activo	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	TOTAL	ID	DESCRIPCIÓN	Posee un control	Solidez del control	Nivel de mitigación
18	Registro de incidentes	1.7	3.4	2.9	1.4	9.4	E1	Errores de los usuarios	No	No existente	0.0
							E2	Errores del administrador	No	No existente	0.0
							E3	Errores de monitorización (log)	No	No existente	0.0
							E4	Errores de configuración	No	No existente	0.0
							E15	Alteración de la información	Si	Adecuado	0.7
							E16	Introducción de información incorrecta	Si	Adecuado	0.7
							E17	Degradación de la información	Si	Adecuado	0.7
							A4	Manipulación de la configuración	Si	Adecuado	0.7
							A11	Acceso no autorizado	Si	Adecuado	0.7
							A15	Modificación de la información (intencional)	Si	Adecuado	0.7
							A16	Introducción de falsa información	Si	Adecuado	0.7
							A17	Corrupción de la información (intencional)	Si	Adecuado	0.7
19	Servidor de Gestión	2.7	3.7	3.2	3.2	12.8	E2	Errores del administrador	No	No existente	0.0
							E4	Errores de configuración	Si	Moderado	0.5
							E9	Errores de re-encaminamiento	No	No existente	0.0
							E10	Errores de secuencia	Si	Muy Adecuado	0.9
							A4	Manipulación de la configuración	Si	Adecuado	0.7
							A5	Suplantación de la identidad del usuario	Si	Adecuado	0.7
							A6	Abuso de privilegios de acceso	Si	Adecuado	0.7
							A9	Re-encaminamiento intencional de mensajes	No	No existente	0.0
							A10	Alteración de secuencia	Si	Muy Adecuado	0.9
							A11	Acceso no autorizado	Si	Adecuado	0.7
20	Software de registro de incidentes	1.7	2.6	2.7	1.9	8.9	E1	Errores de los usuarios	Si	Adecuado	0.7
							E2	Errores del administrador	No	No existente	0.0
							E3	Errores de monitorización (log)	Si	Muy débil	0.1
							E4	Errores de configuración	No	No existente	0.0
							E8	Difusión de software dañino	Si	Muy Adecuado	0.9
							E9	Errores de re-encaminamiento	No	No existente	0.0
							E10	Errores de secuencia	Si	Adecuado	0.7
							E20	Vulnerabilidades de los programas (software)	Si	Moderado	0.5
							E21	Errores de mantenimiento / actualización de programas (software)	Si	Adecuado	0.7
							A4	Manipulación de la configuración	Si	Adecuado	0.7
							A5	Suplantación de la identidad del usuario	Si	Adecuado	0.7
							A6	Abuso de privilegios de acceso	Si	Adecuado	0.7
							A8	Difusión deliberada de software dañino	Si	Muy Adecuado	0.9
							A9	Re-encaminamiento intencional de mensajes	No	No existente	0.0
							A10	Alteración de secuencia	Si	Adecuado	0.7
							A11	Acceso no autorizado	Si	Adecuado	0.7
							A22	Manipulación de programas	Si	Muy Adecuado	0.9
21	Software de monitoreo	1.7	2.9	2.9	2.7	10.2	E1	Errores de los usuarios	Si	Adecuado	0.7
							E2	Errores del administrador	No	Adecuado	0.0
							E3	Errores de monitorización (log)	Si	Moderado	0.5
							E4	Errores de configuración	Si	Moderado	0.5
							E8	Difusión de software dañino	Si	Muy Adecuado	0.9
							E9	Errores de re-encaminamiento	No	No existente	0.0
							E10	Errores de secuencia	Si	Moderado	0.5
							E20	Vulnerabilidades de los programas (software)	Si	Adecuado	0.7
							E21	Errores de mantenimiento / actualización de programas (software)	Si	Adecuado	0.7
							A4	Manipulación de la configuración	Si	Adecuado	0.7
							A5	Suplantación de la identidad del usuario	Si	Adecuado	0.7
							A6	Abuso de privilegios de acceso	Si	Adecuado	0.7
							A8	Difusión deliberada de software dañino	Si	Muy Adecuado	0.9
							A9	Re-encaminamiento intencional de mensajes	No	No existente	0.0
							A10	Alteración de secuencia	Si	Adecuado	0.7
							A11	Acceso no autorizado	Si	Adecuado	0.7
							A22	Manipulación de programas	Si	Muy Adecuado	0.9

6.3.3 Valoración de riesgos.

En este paso se guió a los administradores de la plataforma para que estimaran, para cada amenaza, según su experiencia previa la probabilidad de que esta llegara a suceder y el impacto que causaría sobre el activo amenazado, sin

considerar la existencia de las salvaguardas o controles, según los escenarios propuestos por el modelo.

6.3.3.1 Estimación de frecuencia o probabilidad.

Este paso guarda similitud con el del modelo actualmente aplicado en Coomeva y difiere muy poco en las escalas de tiempo aplicadas para los niveles cualitativos propuestos por el modelo (Nada frecuente, Poco frecuente, Normal, Frecuente, Muy frecuente), pero difiere en la conversión cuantitativa del modelo propuesto.

La presentación de los resultados se integrará con la del impacto o degradación realizada en la siguiente sección.

6.3.3.2 Estimación de Impacto o degradación

En este paso el modelo de estimación propuesto fue considerado más coherente con la realidad al aplicarse a cada activo y no un grupo de activos, y si bien es un poco más largo el ejercicio, es más fácil de estimar, más real y con un resultado más confiable (Tabla 60).

Tabla 60. Activos, Amenazas, Salvaguardas y Riesgos de Telco **[5]**

ID ACTIVO	IDENTIFICACIÓN	VALOR CONSOLIDADO ACTIVO					AMENAZAS		SALVAGUARDAS			RIESGOS	
	Nombre activo	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	TOTAL	ID	DESCRIPCIÓN	Posee un control	Solidez del control	Nivel de mitigación	Probabilidad (Frecuencia)	Impacto (Degradación)
1	Ingenieros de Telemática	3.1	4	2.9	2.2	12.2	E7	Deficiencias en la organización	Si	Adecuado	0.7	Normal	Menor
							E28	Indisponibilidad accidental del personal	Si	Adecuado	0.7	Normal	Menor
							A28	Indisponibilidad deliberada del personal	Si	Adecuado	0.7	Nada frecuente	Menor
							A29	Extorsión	No	No existente	0.0	Nada frecuente	Menor
							A30	Ingeniería social	No	No existente	0.0	Nada frecuente	Menor
2	Analistas de telemática	3.1	3	1.9	2.2	10.2	E7	Deficiencias en la organización	Si	Adecuado	0.7	Normal	Menor
							E28	Indisponibilidad accidental del personal	Si	Adecuado	0.7	Normal	Menor
							A28	Indisponibilidad deliberada del personal	Si	Adecuado	0.7	Nada frecuente	Menor
							A29	Extorsión	No	No existente	0.0	Nada frecuente	Menor
							A30	Ingeniería social	No	No existente	0.0	Nada frecuente	Menor
3	Documentación sistema de Calidad	2.4	2	1.7	1.2	7.3	E2	Errores del administrador	Si	Moderado	0.5	Normal	Mayor
							E4	Errores de configuración	Si	Adecuado	0.7	Normal	Mayor
							E14	Escapes de información	Si	Adecuado	0.7	Nada frecuente	Insignificante
							E19	Divulgación de información por indiscreción	Si	Moderado	0.5	Nada frecuente	Menor
							A4	Manipulación de la configuración	Si	Adecuado	0.7	Normal	Mayor
							A11	Acceso no autorizado	Si	Adecuado	0.7	Poco frecuente	Menor
							A14	Interceptación de información (escucha)	Si	Adecuado	0.7	Nada frecuente	Menor
							A19	Divulgación de información (intencional)	Si	Débil	0.3	Nada frecuente	Menor
							A25	Robo	Si	Moderado	0.5	Nada frecuente	Menor

Tabla 60. Activos, Amenazas, Salvaguardas y Riesgos de Telco **[5]** (Continuación)

ID ACTIVO	IDENTIFICACIÓN	VALOR CONSOLIDADO ACTIVO					AMENAZAS		SALVAGUARDAS			RIESGOS	
	Nombre activo	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	TOTAL	ID	DESCRIPCIÓN	Posee un control	Solidez del control	Nivel de mitigación	Probabilidad (Frecuencia)	Impacto (Degradación)
4	Carpeta Solicitud de Servicios	2.3	4	2.4	1.9	10.6	N1	Fuego (sin intervención humana)	Si	Adecuado	0.7	Nada frecuente	Mayor
							N2	Daños por agua (sin intervención humana)	No	No existente	0.0	Poco frecuente	Mayor
							N*	Desastres naturales	Si	Moderado	0.5	Poco frecuente	Mayor
							I1	Fuego (con intervención humana)	Si	Adecuado	0.7	Nada frecuente	Mayor
							I2	Daños por agua (con intervención humana)	No	No existente	0.0	Nada frecuente	Mayor
							I*	Desastres industriales	No	No existente	0.0	Nada frecuente	Moderado
							I3	Contaminación mecánica	No	No existente	0.0	Nada frecuente	Moderado
							I4	Contaminación electromagnética	No	No existente	0.0	Nada frecuente	Moderado
							I5	Avería de origen físico o lógico	Si	Adecuado	0.7	Normal	Moderado
							I6	Corte del suministro eléctrico	Si	Adecuado	0.7	Muy frecuente	Mayor
							I7	Condiciones inadecuadas de temperatura y/o humedad	Si	Muy Adecuado	0.9	Frecuente	Moderado
							I10	Degradación de los soportes de almacenamiento de la información	Si	Muy Adecuado	0.9	Normal	Mayor
							E1	Errores de los usuarios	Si	Moderado	0.5	Muy frecuente	Menor
							E2	Errores del administrador	Si	Adecuado	0.7	Frecuente	Moderado
							E4	Errores de configuración	Si	Adecuado	0.7	Frecuente	Mayor
							E18	Destrucción de información	Si	Adecuado	0.7	Normal	Moderado
							A4	Manipulación de la configuración	Si	Muy Adecuado	0.9	Poco frecuente	Mayor
							A18	Destrucción la información (intencional)	Si	Adecuado	0.7	Nada frecuente	Mayor
							A25	Robo	Si	Muy Adecuado	0.9	Nada frecuente	Menor
							A26	Ataque destructivo	Si	Adecuado	0.7	Nada frecuente	Catastrófico
5	Esquemas de red	3.5	3.4	4	2.7	13.6	N1	Fuego (sin intervención humana)	Si	Adecuado	0.7	Nada frecuente	Mayor
							N2	Daños por agua (sin intervención humana)	No	No existente	0.0	Poco frecuente	Moderado
							N*	Desastres naturales	Si	Moderado	0.5	Poco frecuente	Moderado
							I1	Fuego (con intervención humana)	Si	Adecuado	0.7	Nada frecuente	Mayor
							I2	Daños por agua (con intervención humana)	No	No existente	0.0	Nada frecuente	Moderado
							I*	Desastres industriales	No	No existente	0.0	Nada frecuente	Insignificante
							I3	Contaminación mecánica	No	No existente	0.0	Nada frecuente	Insignificante
							I4	Contaminación electromagnética	No	No existente	0.0	Nada frecuente	Insignificante
							I5	Avería de origen físico o lógico	Si	Adecuado	0.7	Normal	Moderado
							I6	Corte del suministro eléctrico	Si	Adecuado	0.7	Frecuente	Menor
							I7	Condiciones inadecuadas de temperatura y/o humedad	Si	Adecuado	0.7	Poco frecuente	Insignificante
							I10	Degradación de los soportes de almacenamiento de la información	Si	Muy Adecuado	0.9	Normal	Mayor
							E1	Errores de los usuarios	Si	Moderado	0.5	Normal	Moderado
							E2	Errores del administrador	Si	Adecuado	0.7	Normal	Moderado
							E4	Errores de configuración	Si	Adecuado	0.7	Poco frecuente	Moderado
							E18	Destrucción de información	Si	Adecuado	0.7	Poco frecuente	Catastrófico
							A4	Manipulación de la configuración	Si	Muy Adecuado	0.9	Nada frecuente	Mayor
							A18	Destrucción la información (intencional)	Si	Adecuado	0.7	Nada frecuente	Catastrófico
							A25	Robo	Si	Muy Adecuado	0.9	Nada frecuente	Mayor
							A26	Ataque destructivo	Si	Adecuado	0.7	Nada frecuente	Catastrófico
6	Proveedores de telecomunicaciones	1	3.6	3.7	4.2	12.5	N1	Fuego (sin intervención humana)	Si	Adecuado	0.7	Poco frecuente	Catastrófico
							N2	Daños por agua (sin intervención humana)	No	Muy débil	0.0	Poco frecuente	Catastrófico
							N*	Desastres naturales	Si	Muy débil	0.1	Poco frecuente	Catastrófico
							I1	Fuego (con intervención humana)	Si	Adecuado	0.7	Nada frecuente	Catastrófico
							I2	Daños por agua (con intervención humana)	No	No existente	0.0	Nada frecuente	Mayor
							I*	Desastres industriales	No	No existente	0.0	Nada frecuente	Mayor
							I3	Contaminación mecánica	No	No existente	0.0	Poco frecuente	Moderado
							I4	Contaminación electromagnética	No	No existente	0.0	Nada frecuente	Mayor
							I6	Corte del suministro eléctrico	Si	Adecuado	0.7	Frecuente	Mayor
							I7	Condiciones inadecuadas de temperatura y/o humedad	Si	Adecuado	0.7	Normal	Moderado
							I8	Fallo de servicios de comunicaciones	Si	Adecuado	0.7	Normal	Mayor
							I9	Interrupción de otros servicios y suministros esenciales	Si	Adecuado	0.7	Normal	Mayor
							E1	Errores de los usuarios	Si	Adecuado	0.7	Poco frecuente	Moderado
							E2	Errores del administrador	Si	Moderado	0.5	Normal	Moderado
							E4	Errores de configuración	Si	Moderado	0.5	Normal	Moderado
							E24	Caída del sistema por agotamiento de recursos	Si	Moderado	0.5	Poco frecuente	Moderado
							A4	Manipulación de la configuración	Si	Moderado	0.5	Normal	Moderado
							A7	Uso no previsto	Si	Adecuado	0.7	Nada frecuente	Moderado
							A24	Denegación de servicio	Si	Adecuado	0.7	Poco frecuente	Moderado
							A26	Ataque destructivo	Si	Adecuado	0.7	Normal	Moderado
7	Proveedores servicios de telefonia	1.3	3.6	3.2	3.2	11.3	N1	Fuego (sin intervención humana)	Si	Adecuado	0.7	Nada frecuente	Catastrófico
							N2	Daños por agua (sin intervención humana)	No	Adecuado	0.0	Poco frecuente	Mayor
							N*	Desastres naturales	Si	Moderado	0.5	Poco frecuente	Moderado
							I1	Fuego (con intervención humana)	Si	Adecuado	0.7	Nada frecuente	Catastrófico
							I2	Daños por agua (con intervención humana)	No	No existente	0.0	Nada frecuente	Mayor
							I*	Desastres industriales	No	No existente	0.0	Nada frecuente	Mayor
							I3	Contaminación mecánica	No	No existente	0.0	Poco frecuente	Moderado
							I4	Contaminación electromagnética	No	No existente	0.0	Nada frecuente	Mayor
							I6	Corte del suministro eléctrico	Si	Adecuado	0.7	Frecuente	Mayor
							I7	Condiciones inadecuadas de temperatura y/o humedad	Si	Adecuado	0.7	Normal	Menor
							I8	Fallo de servicios de comunicaciones	Si	Adecuado	0.7	Frecuente	Moderado
							I9	Interrupción de otros servicios y suministros esenciales	Si	Adecuado	0.7	Frecuente	Moderado
							E1	Errores de los usuarios	Si	Adecuado	0.7	Normal	Menor
							E2	Errores del administrador	Si	Moderado	0.5	Poco frecuente	Moderado
							E4	Errores de configuración	Si	Moderado	0.5	Normal	Moderado
							E24	Caída del sistema por agotamiento de recursos	Si	Moderado	0.5	Poco frecuente	Mayor
							A4	Manipulación de la configuración	Si	Moderado	0.5	Normal	Moderado
							A7	Uso no previsto	Si	Adecuado	0.7	Nada frecuente	Moderado
							A24	Denegación de servicio	Si	Adecuado	0.7	Nada frecuente	Moderado
							A26	Ataque destructivo	Si	Adecuado	0.7	Nada frecuente	Catastrófico

Tabla 60. Activos, Amenazas, Salvaguardas y Riesgos de Telco **[5]** (Continuación)

ID ACTIVO	IDENTIFICACIÓN	VALOR CONSOLIDADO ACTIVO					AMENAZAS		SALVAGUARDAS			RIESGOS	
	Nombre activo	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	TOTAL	ID	DESCRIPCIÓN	Posee un control	Solidez del control	Nivel de mitigación	Probabilidad (Frecuencia)	Impacto (Degradación)
8	Contratos	3	3.5	2	1.3	9.8	E2	Errores del administrador	Si	Muy Adecuado	0.9	Poco frecuente	Moderado
							E4	Errores de configuración	Si	Muy Adecuado	0.9	Poco frecuente	Moderado
							E14	Escapes de información	Si	Adecuado	0.7	Poco frecuente	Menor
							E19	Divulgación de información por indiscreción	Si	Adecuado	0.7	Poco frecuente	Insignificante
							A4	Manipulación de la configuración	Si	Muy Adecuado	0.9	Poco frecuente	Moderado
							A11	Acceso no autorizado	Si	Moderado	0.5	Poco frecuente	Menor
							A14	Interceptación de información (escucha)	Si	Moderado	0.5	Poco frecuente	Menor
							A19	Divulgación de información (intencional)	Si	Adecuado	0.7	Poco frecuente	Menor
							A25	Robo	Si	Muy Adecuado	0.9	Nada frecuente	Menor
9	Caja menor	1	1.2	2.5	1.7	6.4	A7	Uso no previsto	Si	Adecuado	0.7	Poco frecuente	Moderado
							A11	Acceso no autorizado	Si	Muy Adecuado	0.9	Poco frecuente	Mayor
							A25	Robo	Si	Adecuado	0.7	Nada frecuente	Mayor
10	Servicio de Share Point	3	3.7	2.9	3	12.6	I11	Emanaciones electromagnéticas	No	No existente	0.0	Nada frecuente	Mayor
							E2	Errores del administrador	No	No existente	0.0	Normal	Moderado
							E4	Errores de configuración	Si	Moderado	0.5	Normal	Moderado
							E9	Errores de re-encaminamiento	No	No existente	0.0	Normal	Menor
							E14	Escapes de información	Si	Débil	0.3	Poco frecuente	Moderado
							A4	Manipulación de la configuración	Si	Adecuado	0.7	Normal	Moderado
							A5	Suplantación de la identidad del usuario	Si	Moderado	0.5	Poco frecuente	Menor
							A6	Abuso de privilegios de acceso	Si	Adecuado	0.7	Poco frecuente	Moderado
							A9	Re-encaminamiento intencional de mensajes	No	No existente	0.0	Nada frecuente	Menor
							A11	Acceso no autorizado	Si	Adecuado	0.7	Nada frecuente	Moderado
							A12	Análisis de tráfico	Si	Moderado	0.5	Poco frecuente	Menor
							A14	Interceptación de información (escucha)	Si	Moderado	0.5	Poco frecuente	Menor
							A25	Robo	Si	Muy Adecuado	0.9	Nada frecuente	Mayor
							A27	Ocupación no autorizada	Si	Adecuado	0.7	Nada frecuente	Mayor
11	Equipos de telecomunicaciones	3.1	3.7	3.4	3.9	14.1	N1	Fuego (sin intervención humana)	Si	Adecuado	0.7	Nada frecuente	Catastrófico
							N2	Daños por agua (sin intervención humana)	No	No existente	0.0	Poco frecuente	Mayor
							N*	Desastres naturales	Si	Moderado	0.5	Poco frecuente	Moderado
							I1	Fuego (con intervención humana)	Si	Adecuado	0.7	Nada frecuente	Catastrófico
							I2	Daños por agua (con intervención humana)	No	No existente	0.0	Nada frecuente	Mayor
							I*	Desastres industriales	No	No existente	0.0	Nada frecuente	Mayor
							I3	Contaminación mecánica	No	No existente	0.0	Poco frecuente	Moderado
							I4	Contaminación electromagnética	No	No existente	0.0	Nada frecuente	Mayor
							I5	Avería de origen físico o lógico	Si	Adecuado	0.7	Poco frecuente	Mayor
							I6	Corte del suministro eléctrico	Si	Adecuado	0.7	Frecuente	Mayor
							I7	Condiciones inadecuadas de temperatura y/o humedad	Si	Adecuado	0.7	Normal	Menor
							E2	Errores del administrador	Si	Adecuado	0.7	Normal	Moderado
							E4	Errores de configuración	Si	Muy Adecuado	0.9	Poco frecuente	Moderado
							E23	Errores de mantenimiento / actualización de equipos (hardware)	Si	Adecuado	0.7	Poco frecuente	Moderado
							E24	Caída del sistema por agotamiento de recursos	Si	Adecuado	0.7	Poco frecuente	Mayor
							A4	Manipulación de la configuración	Si	Muy Adecuado	0.9	Normal	Moderado
							A7	Uso no previsto	Si	Adecuado	0.7	Nada frecuente	Mayor
							A24	Denegación de servicio	Si	Adecuado	0.7	Poco frecuente	Mayor
							A25	Robo	Si	Adecuado	0.7	Nada frecuente	Mayor
							A26	Ataque destructivo	Si	Adecuado	0.7	Nada frecuente	Catastrófico
							A27	Ocupación no autorizada	Si	Adecuado	0.7	Nada frecuente	Mayor
12	Equipos de telefonía	2.4	2.7	2.9	2.9	10.9	N1	Fuego (sin intervención humana)	Si	Adecuado	0.7	Nada frecuente	Catastrófico
							N2	Daños por agua (sin intervención humana)	No	No existente	0.0	Poco frecuente	Mayor
							N*	Desastres naturales	Si	Moderado	0.5	Poco frecuente	Moderado
							I1	Fuego (con intervención humana)	Si	Adecuado	0.7	Nada frecuente	Catastrófico
							I2	Daños por agua (con intervención humana)	No	No existente	0.0	Nada frecuente	Mayor
							I*	Desastres industriales	No	No existente	0.0	Nada frecuente	Mayor
							I3	Contaminación mecánica	No	No existente	0.0	Poco frecuente	Moderado
							I4	Contaminación electromagnética	No	No existente	0.0	Nada frecuente	Mayor
							I5	Avería de origen físico o lógico	Si	Adecuado	0.7	Poco frecuente	Mayor
							I6	Corte del suministro eléctrico	Si	Adecuado	0.7	Frecuente	Mayor
							I7	Condiciones inadecuadas de temperatura y/o humedad	Si	Adecuado	0.7	Normal	Menor
							E2	Errores del administrador	Si	Adecuado	0.7	Normal	Moderado
							E4	Errores de configuración	Si	Muy Adecuado	0.9	Poco frecuente	Moderado
							E23	Errores de mantenimiento / actualización de equipos (hardware)	Si	Adecuado	0.7	Poco frecuente	Moderado
							E24	Caída del sistema por agotamiento de recursos	Si	Adecuado	0.7	Poco frecuente	Mayor
							A4	Manipulación de la configuración	Si	Muy Adecuado	0.9	Normal	Moderado
							A7	Uso no previsto	Si	Adecuado	0.7	Nada frecuente	Menor
							A24	Denegación de servicio	Si	Adecuado	0.7	Normal	Mayor
							A25	Robo	Si	Adecuado	0.7	Nada frecuente	Mayor
							A26	Ataque destructivo	Si	Adecuado	0.7	Nada frecuente	Catastrófico
							A27	Ocupación no autorizada	Si	Adecuado	0.7	Nada frecuente	Mayor
13	Redes WAN	3.6	3.7	3.4	3.9	14.6	I11	Emanaciones electromagnéticas	No	No existente	0.0	Nada frecuente	Moderado
							E2	Errores del administrador	Si	Muy Adecuado	0.9	Normal	Mayor
							E4	Errores de configuración	Si	Muy Adecuado	0.9	Poco frecuente	Mayor
							E9	Errores de re-encaminamiento	Si	Muy Adecuado	0.9	Nada frecuente	Mayor
							E14	Escapes de información	Si	Adecuado	0.7	Nada frecuente	Moderado
							A4	Manipulación de la configuración	Si	Muy Adecuado	0.9	Normal	Mayor
							A5	Suplantación de la identidad del usuario	Si	Muy Adecuado	0.9	Nada frecuente	Mayor
							A6	Abuso de privilegios de acceso	Si	Muy Adecuado	0.9	Nada frecuente	Mayor
							A9	Re-encaminamiento intencional de mensajes	Si	Muy Adecuado	0.9	Nada frecuente	Mayor
							A11	Acceso no autorizado	Si	Muy Adecuado	0.9	Nada frecuente	Mayor
							A12	Análisis de tráfico	Si	Moderado	0.5	Muy frecuente	Mayor
							A14	Interceptación de información (escucha)	Si	Moderado	0.5	Muy frecuente	Mayor
							A25	Robo	Si	Adecuado	0.7	Nada frecuente	Mayor
							A27	Ocupación no autorizada	Si	Adecuado	0.7	Nada frecuente	Mayor

Tabla 60. Activos, Amenazas, Salvaguardas y Riesgos de Telco **[5]** (Continuación)

ID ACTIVO	IDENTIFICACIÓN	VALOR CONSOLIDADO ACTIVO					AMENAZAS		SALVAGUARDAS			RIESGOS	
	Nombre activo	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	TOTAL	ID	DESCRIPCIÓN	Posee un control	Solidez del control	Nivel de mitigación	Probabilidad (Frecuencia)	Impacto (Degradación)
14	Red LAN - Wireless	3.7	2.9	3.2	2.9	12.7	I11	Emanaciones electromagnéticas	No	No existente	0.0	Nada frecuente	Moderado
							E2	Errores del administrador	Si	Muy Adecuado	0.9	Normal	Moderado
							E4	Errores de configuración	Si	Muy Adecuado	0.9	Poco frecuente	Mayor
							E9	Errores de re-encaminamiento	Si	Muy Adecuado	0.9	Nada frecuente	Moderado
							E14	Escapes de información	Si	Adecuado	0.7	Nada frecuente	Mayor
							A4	Manipulación de la configuración	Si	Muy Adecuado	0.9	Normal	Moderado
							A5	Suplantación de la identidad del usuario	Si	Muy Adecuado	0.9	Nada frecuente	Moderado
							A6	Abuso de privilegios de acceso	Si	Muy Adecuado	0.9	Poco frecuente	Mayor
							A9	Re-encaminamiento intencional de mensajes	Si	Muy Adecuado	0.9	Nada frecuente	Mayor
							A11	Acceso no autorizado	Si	Muy Adecuado	0.9	Poco frecuente	Moderado
							A12	Análisis de tráfico	Si	Moderado	0.5	Frecuente	Moderado
							A14	Interceptación de información (escucha)	Si	Moderado	0.5	Frecuente	Moderado
							A25	Robo	Si	Adecuado	0.7	Nada frecuente	Moderado
							A27	Ocupación no autorizada	Si	Adecuado	0.7	Nada frecuente	Mayor
15	Internet	2.4	2.5	2.2	1.2	8.3	I11	Emanaciones electromagnéticas	No	No existente	0.0	Nada frecuente	Moderado
							E2	Errores del administrador	Si	Muy Adecuado	0.9	Normal	Mayor
							E4	Errores de configuración	Si	Adecuado	0.7	Poco frecuente	Mayor
							E9	Errores de re-encaminamiento	Si	Muy Adecuado	0.9	Nada frecuente	Mayor
							E14	Escapes de información	Si	Adecuado	0.7	Poco frecuente	Mayor
							A4	Manipulación de la configuración	Si	Adecuado	0.7	Frecuente	Moderado
							A5	Suplantación de la identidad del usuario	Si	Muy Adecuado	0.9	Poco frecuente	Mayor
							A6	Abuso de privilegios de acceso	Si	Adecuado	0.7	Poco frecuente	Mayor
							A9	Re-encaminamiento intencional de mensajes	Si	Muy Adecuado	0.9	Nada frecuente	Mayor
							A11	Acceso no autorizado	Si	Adecuado	0.7	Poco frecuente	Mayor
							A12	Análisis de tráfico	Si	Moderado	0.5	Muy frecuente	Mayor
							A14	Interceptación de información (escucha)	Si	Moderado	0.5	Muy frecuente	Mayor
							A25	Robo	Si	Adecuado	0.7	Nada frecuente	Mayor
							A27	Ocupación no autorizada	Si	Adecuado	0.7	Nada frecuente	Mayor
16	Planes de mejoramiento	2.4	1.7	1.2	1	6.3	E2	Errores del administrador	No	No existente	0.0	Poco frecuente	Menor
							E4	Errores de configuración	Si	Moderado	0.5	Poco frecuente	Menor
							E14	Escapes de información	Si	Moderado	0.5	Nada frecuente	Menor
							E19	Divulgación de información por indiscreción	Si	Moderado	0.5	Nada frecuente	Menor
							A4	Manipulación de la configuración	Si	Moderado	0.5	Frecuente	Menor
							A11	Acceso no autorizado	Si	Adecuado	0.7	Nada frecuente	Menor
							A14	Interceptación de información (escucha)	Si	Moderado	0.5	Poco frecuente	Menor
							A19	Divulgación de información (intencional)	Si	Débil	0.3	Nada frecuente	Menor
							A25	Robo	Si	Adecuado	0.7	Nada frecuente	Menor
17	Planes de continuidad	2.7	3.7	2.4	2.1	10.9	E1	Errores de los usuarios	Si	Débil	0.3	Normal	Moderado
							E2	Errores del administrador	No	No existente	0.0	Poco frecuente	Moderado
							E3	Errores de monitorización (log)	Si	Muy débil	0.1	Normal	Menor
							E4	Errores de configuración	Si	Moderado	0.5	Poco frecuente	Moderado
							E15	Alteración de la información	Si	Muy débil	0.1	Poco frecuente	Moderado
							E16	Introducción de información incorrecta	Si	Moderado	0.5	Poco frecuente	Moderado
							E17	Degradación de la información	Si	Moderado	0.5	Normal	Moderado
							A4	Manipulación de la configuración	Si	Moderado	0.5	Frecuente	Moderado
							A11	Acceso no autorizado	Si	Adecuado	0.7	Nada frecuente	Menor
							A15	Modificación de la información (intencional)	Si	Adecuado	0.7	Nada frecuente	Moderado
							A16	Introducción de falsa información	Si	Adecuado	0.7	Nada frecuente	Moderado
							A17	Corrupción de la información (intencional)	Si	Adecuado	0.7	Nada frecuente	Moderado
18	Registro de incidentes	1.7	3.4	2.9	1.4	9.4	E1	Errores de los usuarios	No	No existente	0.0	Normal	Moderado
							E2	Errores del administrador	No	No existente	0.0	Poco frecuente	Moderado
							E3	Errores de monitorización (log)	No	No existente	0.0	Poco frecuente	Insignificante
							E4	Errores de configuración	No	No existente	0.0	Poco frecuente	Menor
							E15	Alteración de la información	Si	Adecuado	0.7	Poco frecuente	Moderado
							E16	Introducción de información incorrecta	Si	Adecuado	0.7	Poco frecuente	Moderado
							E17	Degradación de la información	Si	Adecuado	0.7	Poco frecuente	Moderado
							A4	Manipulación de la configuración	Si	Adecuado	0.7	Normal	Menor
							A11	Acceso no autorizado	Si	Adecuado	0.7	Nada frecuente	Insignificante
							A15	Modificación de la información (intencional)	Si	Adecuado	0.7	Nada frecuente	Moderado
							A16	Introducción de falsa información	Si	Adecuado	0.7	Poco frecuente	Menor
							A17	Corrupción de la información (intencional)	Si	Adecuado	0.7	Nada frecuente	Moderado
19	Servidor de Gestión	2.7	3.7	3.2	3.2	12.8	E2	Errores del administrador	No	No existente	0.0	Normal	Moderado
							E4	Errores de configuración	Si	Moderado	0.5	Poco frecuente	Moderado
							E9	Errores de re-encaminamiento	No	No existente	0.0	Nada frecuente	Moderado
							E10	Errores de secuencia	Si	Muy Adecuado	0.9	Nada frecuente	Moderado
							A4	Manipulación de la configuración	Si	Adecuado	0.7	Frecuente	Moderado
							A5	Suplantación de la identidad del usuario	Si	Adecuado	0.7	Nada frecuente	Moderado
							A6	Abuso de privilegios de acceso	Si	Adecuado	0.7	Nada frecuente	Mayor
							A9	Re-encaminamiento intencional de mensajes	No	No existente	0.0	Nada frecuente	Moderado
							A10	Alteración de secuencia	Si	Muy Adecuado	0.9	Nada frecuente	Moderado
							A11	Acceso no autorizado	Si	Adecuado	0.7	Nada frecuente	Moderado

Tabla 60. Activos, Amenazas, Salvaguardas y Riesgos de Telco **[5]** (Continuación)

ID ACTIVO	IDENTIFICACIÓN	VALOR CONSOLIDADO ACTIVO					AMENAZAS		SALVAGUARDAS			RIESGOS	
	Nombre activo	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	TOTAL	ID	DESCRIPCIÓN	Posee un control	Solidez del control	Nivel de mitigación	Probabilidad (Frecuencia)	Impacto (Degradación)
20	Software de registro de incidentes	1.7	2.6	2.7	1.9	8.9	E1	Errores de los usuarios	Si	Adecuado	0.7	Normal	Moderado
							E2	Errores del administrador	No	No existente	0.0	Normal	Menor
							E3	Errores de monitorización (log)	Si	Muy débil	0.1	Normal	Menor
							E4	Errores de configuración	No	No existente	0.0	Poco frecuente	Menor
							E8	Difusión de software dañino	Si	Muy Adecuado	0.9	Frecuente	Moderado
							E9	Errores de re-encaminamiento	No	No existente	0.0	Nada frecuente	Menor
							E10	Errores de secuencia	Si	Adecuado	0.7	Nada frecuente	Menor
							E20	Vulnerabilidades de los programas (software)	Si	Moderado	0.5	Normal	Moderado
							E21	Errores de mantenimiento / actualización de programas (software)	Si	Adecuado	0.7	Poco frecuente	Moderado
							A4	Manipulación de la configuración	Si	Adecuado	0.7	Normal	Moderado
							A5	Suplantación de la identidad del usuario	Si	Adecuado	0.7	Nada frecuente	Menor
							A6	Abuso de privilegios de acceso	Si	Adecuado	0.7	Nada frecuente	Menor
							A8	Difusión deliberada de software dañino	Si	Muy Adecuado	0.9	Poco frecuente	Moderado
							A9	Re-encaminamiento intencional de mensajes	No	No existente	0.0	Nada frecuente	Menor
							A10	Alteración de secuencia	Si	Adecuado	0.7	Nada frecuente	Menor
							A11	Acceso no autorizado	Si	Adecuado	0.7	Nada frecuente	Menor
							A22	Manipulación de programas	Si	Muy Adecuado	0.9	Nada frecuente	Moderado
21	Software de monitoreo	1.7	2.9	2.9	2.7	10.2	E1	Errores de los usuarios	Si	Adecuado	0.7	Poco frecuente	Moderado
							E2	Errores del administrador	No	Adecuado	0.0	Normal	Moderado
							E3	Errores de monitorización (log)	Si	Moderado	0.5	Normal	Menor
							E4	Errores de configuración	Si	Moderado	0.5	Poco frecuente	Moderado
							E8	Difusión de software dañino	Si	Muy Adecuado	0.9	Frecuente	Moderado
							E9	Errores de re-encaminamiento	No	No existente	0.0	Nada frecuente	Menor
							E10	Errores de secuencia	Si	Moderado	0.5	Nada frecuente	Moderado
							E20	Vulnerabilidades de los programas (software)	Si	Adecuado	0.7	Normal	Moderado
							E21	Errores de mantenimiento / actualización de programas (software)	Si	Adecuado	0.7	Poco frecuente	Moderado
							A4	Manipulación de la configuración	Si	Adecuado	0.7	Frecuente	Moderado
							A5	Suplantación de la identidad del usuario	Si	Adecuado	0.7	Nada frecuente	Menor
							A6	Abuso de privilegios de acceso	Si	Adecuado	0.7	Nada frecuente	Menor
							A8	Difusión deliberada de software dañino	Si	Muy Adecuado	0.9	Poco frecuente	Moderado
							A9	Re-encaminamiento intencional de mensajes	No	No existente	0.0	Nada frecuente	Menor
							A10	Alteración de secuencia	Si	Adecuado	0.7	Nada frecuente	Menor
							A11	Acceso no autorizado	Si	Adecuado	0.7	Nada frecuente	Moderado
							A22	Manipulación de programas	Si	Muy Adecuado	0.9	Nada frecuente	Moderado

6.3.3.3 Estimación riesgo marginal.

En este paso se aplicaron las tablas de conversión de los estimados cualitativos para volverlos en cuantitativos y hacer los cálculos numéricos correspondientes para obtener los valores de riesgo inherente y riesgo residual, conforme lo propone el modelo. Adicionalmente se realizó la priorización y ordenamiento de estos dos valores resultantes utilizando la propiedad de colorimetría que posee la hoja electrónica utilizada, para obtener las tablas finales, ordenadas según la importancia de los activos en primera instancia, y en segunda instancia, para cada activo se ordenan las amenazas según la criticidad del riesgo marginal (una vez estimado el grado de mitigación de la salvaguarda descrito en la sección 6.3.2.1) y luego por su riesgo inherente, empezando por los más críticos en rojo y terminando con los menos críticos en verde.

En la Tabla 61 se muestra el resultado final del ejercicio, omitiendo las columnas Propietario, Administrador y atributos de los activos para descongestionar su lectura.

Tabla 61. Activos y Riesgos de Telco priorizados **[5]**

ID ACTIVO	IDENTIFICACIÓN	VALOR CONSOLIDADO	AMENAZAS		SALVAGUARDAS			RIESGOS					
	Nombre activo	TOTAL	ID	DESCRIPCIÓN	Posee un control	Solidez del control	Nivel de mitigación	Probabilidad (Frecuencia)	Impacto (Degradación)	Valor probabilidad	Valor impacto	Riesgo Inherente	Riesgo Marginal
13	Redes WAN	14.6	A12	Análisis de tráfico	Si	Moderado	0.5	Muy frecuente	Mayor	1.0	0.8	0.8	0.4
			A14	Interceptación de información (escucha)	Si	Moderado	0.5	Muy frecuente	Mayor	1.0	0.8	0.8	0.4
			I11	Emanaciones electromagnéticas	No	No existente	0.0	Nada frecuente	Moderado	0.2	0.6	0.12	0.12
			A25	Robo	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			A27	Ocupación no autorizada	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			E2	Errores del administrador	Si	Muy Adecuado	0.9	Normal	Mayor	0.6	0.8	0.48	0.048
			A4	Manipulación de la configuración	Si	Muy Adecuado	0.9	Normal	Mayor	0.6	0.8	0.48	0.048
			E14	Escapes de información	Si	Adecuado	0.7	Nada frecuente	Moderado	0.2	0.6	0.12	0.036
			E4	Errores de configuración	Si	Muy Adecuado	0.9	Poco frecuente	Mayor	0.4	0.8	0.32	0.032
			E9	Errores de re-encaminamiento	Si	Muy Adecuado	0.9	Nada frecuente	Mayor	0.2	0.8	0.16	0.016
			A5	Suplantación de la identidad del usuario	Si	Muy Adecuado	0.9	Nada frecuente	Mayor	0.2	0.8	0.16	0.016
			A6	Abuso de privilegios de acceso	Si	Muy Adecuado	0.9	Nada frecuente	Mayor	0.2	0.8	0.16	0.016
			A9	Re-encaminamiento intencional de mensajes	Si	Muy Adecuado	0.9	Nada frecuente	Mayor	0.2	0.8	0.16	0.016
			A11	Acceso no autorizado	Si	Muy Adecuado	0.9	Nada frecuente	Mayor	0.2	0.8	0.16	0.016
11	Equipos de telecomunicaciones	14.1	N2	Daños por agua (sin intervención humana)	No	No existente	0.0	Poco frecuente	Mayor	0.4	0.8	0.32	0.32
			I3	Contaminación mecánica	No	No existente	0.0	Poco frecuente	Moderado	0.4	0.6	0.24	0.24
			I6	Corte del suministro eléctrico	Si	Adecuado	0.7	Frecuente	Mayor	0.8	0.8	0.64	0.192
			I2	Daños por agua (con intervención humana)	No	No existente	0.0	Nada frecuente	Mayor	0.2	0.8	0.16	0.16
			I*	Desastres industriales	No	No existente	0.0	Nada frecuente	Mayor	0.2	0.8	0.16	0.16
			I4	Contaminación electromagnética	No	No existente	0.0	Nada frecuente	Mayor	0.2	0.8	0.16	0.16
			N*	Desastres naturales	Si	Moderado	0.5	Poco frecuente	Moderado	0.4	0.6	0.24	0.12
			E2	Errores del administrador	Si	Adecuado	0.7	Normal	Moderado	0.6	0.6	0.36	0.108
			I5	Avería de origen físico o lógico	Si	Adecuado	0.7	Poco frecuente	Mayor	0.4	0.8	0.32	0.096
			E24	Caída del sistema por agotamiento de recursos	Si	Adecuado	0.7	Poco frecuente	Mayor	0.4	0.8	0.32	0.096
			A24	Denegación de servicio	Si	Adecuado	0.7	Poco frecuente	Mayor	0.4	0.8	0.32	0.096
			I7	Condiciones inadecuadas de temperatura y/o humedad	Si	Adecuado	0.7	Normal	Menor	0.6	0.4	0.24	0.072
			E23	Errores de mantenimiento / actualización de equipos (hardware)	Si	Adecuado	0.7	Poco frecuente	Moderado	0.4	0.6	0.24	0.072
			N1	Fuego (sin intervención humana)	Si	Adecuado	0.7	Nada frecuente	Catastrófico	0.2	1.0	0.2	0.06
			I1	Fuego (con intervención humana)	Si	Adecuado	0.7	Nada frecuente	Catastrófico	0.2	1.0	0.2	0.06
			A26	Ataque destructivo	Si	Adecuado	0.7	Nada frecuente	Catastrófico	0.2	1.0	0.2	0.06
			A7	Uso no previsto	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			A25	Robo	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			A27	Ocupación no autorizada	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			A4	Manipulación de la configuración	Si	Muy Adecuado	0.9	Normal	Moderado	0.6	0.6	0.36	0.036
			E4	Errores de configuración	Si	Muy Adecuado	0.9	Poco frecuente	Moderado	0.4	0.6	0.24	0.024
5	Esquemas de red	13.6	N2	Daños por agua (sin intervención humana)	No	No existente	0.0	Poco frecuente	Moderado	0.4	0.6	0.24	0.24
			E1	Errores de los usuarios	Si	Moderado	0.5	Normal	Moderado	0.6	0.6	0.36	0.18
			E18	Destrucción de información	Si	Adecuado	0.7	Poco frecuente	Catastrófico	0.4	1.0	0.4	0.12
			N*	Desastres naturales	Si	Moderado	0.5	Poco frecuente	Moderado	0.4	0.6	0.24	0.12
			I2	Daños por agua (con intervención humana)	No	No existente	0.0	Nada frecuente	Moderado	0.2	0.6	0.12	0.12
			I5	Avería de origen físico o lógico	Si	Adecuado	0.7	Normal	Moderado	0.6	0.6	0.36	0.108
			E2	Errores del administrador	Si	Adecuado	0.7	Normal	Moderado	0.6	0.6	0.36	0.108
			I6	Corte del suministro eléctrico	Si	Adecuado	0.7	Frecuente	Menor	0.8	0.4	0.32	0.096
			E4	Errores de configuración	Si	Adecuado	0.7	Poco frecuente	Moderado	0.4	0.6	0.24	0.072
			A18	Destrucción la información (intencional)	Si	Adecuado	0.7	Nada frecuente	Catastrófico	0.2	1.0	0.2	0.06
			A26	Ataque destructivo	Si	Adecuado	0.7	Nada frecuente	Catastrófico	0.2	1.0	0.2	0.06
			N1	Fuego (sin intervención humana)	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			I1	Fuego (con intervención humana)	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			I10	Degradación de los soportes de almacenamiento de la información	Si	Muy Adecuado	0.9	Normal	Mayor	0.6	0.8	0.48	0.048
			I*	Desastres industriales	No	No existente	0.0	Nada frecuente	Insignificante	0.2	0.2	0.04	0.04
			I3	Contaminación mecánica	No	No existente	0.0	Nada frecuente	Insignificante	0.2	0.2	0.04	0.04
			I4	Contaminación electromagnética	No	No existente	0.0	Nada frecuente	Insignificante	0.2	0.2	0.04	0.04
			I7	Condiciones inadecuadas de temperatura y/o humedad	Si	Adecuado	0.7	Poco frecuente	Insignificante	0.4	0.2	0.08	0.024
			A4	Manipulación de la configuración	Si	Muy Adecuado	0.9	Nada frecuente	Mayor	0.2	0.8	0.16	0.016
			A25	Robo	Si	Muy Adecuado	0.9	Nada frecuente	Mayor	0.2	0.8	0.16	0.016
19	Servidor de Gestión	12.8	E2	Errores del administrador	No	No existente	0.0	Normal	Moderado	0.6	0.6	0.36	0.36
			A4	Manipulación de la configuración	Si	Adecuado	0.7	Frecuente	Moderado	0.8	0.6	0.48	0.144
			E4	Errores de configuración	Si	Moderado	0.5	Poco frecuente	Moderado	0.4	0.6	0.24	0.12
			E9	Errores de re-encaminamiento	No	No existente	0.0	Nada frecuente	Moderado	0.2	0.6	0.12	0.12
			A9	Re-encaminamiento intencional de mensajes	No	No existente	0.0	Nada frecuente	Moderado	0.2	0.6	0.12	0.12
			A6	Abuso de privilegios de acceso	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			A5	Suplantación de la identidad del usuario	Si	Adecuado	0.7	Nada frecuente	Moderado	0.2	0.6	0.12	0.036
			A11	Acceso no autorizado	Si	Adecuado	0.7	Nada frecuente	Moderado	0.2	0.6	0.12	0.036
			E10	Errores de secuencia	Si	Muy Adecuado	0.9	Nada frecuente	Moderado	0.2	0.6	0.12	0.012
			A10	Alteración de secuencia	Si	Muy Adecuado	0.9	Nada frecuente	Moderado	0.2	0.6	0.12	0.012
14	Red LAN - Wireless	12.7	A12	Análisis de tráfico	Si	Moderado	0.5	Frecuente	Moderado	0.8	0.6	0.48	0.24
			A14	Interceptación de información (escucha)	Si	Moderado	0.5	Frecuente	Moderado	0.8	0.6	0.48	0.24
			I11	Emanaciones electromagnéticas	No	No existente	0.0	Nada frecuente	Moderado	0.2	0.6	0.12	0.12
			E14	Escapes de información	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			A27	Ocupación no autorizada	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			A25	Robo	Si	Adecuado	0.7	Nada frecuente	Moderado	0.2	0.6	0.12	0.036
			E2	Errores del administrador	Si	Muy Adecuado	0.9	Normal	Moderado	0.6	0.6	0.36	0.036
			A4	Manipulación de la configuración	Si	Muy Adecuado	0.9	Normal	Moderado	0.6	0.6	0.36	0.036
			E4	Errores de configuración	Si	Muy Adecuado	0.9	Poco frecuente	Mayor	0.4	0.8	0.32	0.032
			A6	Abuso de privilegios de acceso	Si	Muy Adecuado	0.9	Poco frecuente	Mayor	0.4	0.8	0.32	0.032
			A11	Acceso no autorizado	Si	Muy Adecuado	0.9	Poco frecuente	Moderado	0.4	0.6	0.24	0.024
			A9	Re-encaminamiento intencional de mensajes	Si	Muy Adecuado	0.9	Nada frecuente	Mayor	0.2	0.8	0.16	0.016
			E9	Errores de re-encaminamiento	Si	Muy Adecuado	0.9	Nada frecuente	Moderado	0.2	0.6	0.12	0.012
			A5	Suplantación de la identidad del usuario	Si	Muy Adecuado	0.9	Nada frecuente	Moderado	0.2	0.6	0.12	0.012

Tabla 61. Activos y Riesgos de Telco priorizados **[5]** (Continuación)

ID ACTIVO	IDENTIFICACIÓN	VALOR CONSOLIDADO	AMENAZAS		SALVAGUARDAS			RIESGOS					
	Nombre activo	TOTAL	ID	DESCRIPCIÓN	Posee un control	Solidez del control	Nivel de mitigación	Probabilidad (Frecuencia)	Impacto (Degradación)	Valor probabilidad	Valor impacto	Riesgo Inherente	Riesgo Marginal
10	Servicio de Share Point	12.6	E2	Errores del administrador	No	No existente	0.0	Normal	Moderado	0.6	0.6	0.36	0.36
			E9	Errores de re-encaminamiento	No	No existente	0.0	Normal	Menor	0.6	0.4	0.24	0.24
			E4	Errores de configuración	Si	Moderado	0.5	Normal	Moderado	0.6	0.6	0.36	0.18
			E14	Escapes de información	Si	Débil	0.3	Poco frecuente	Moderado	0.4	0.6	0.24	0.168
			I11	Emanaciones electromagnéticas	No	No existente	0.0	Nada frecuente	Mayor	0.2	0.8	0.16	0.16
			A4	Manipulación de la configuración	Si	Adecuado	0.7	Normal	Moderado	0.6	0.6	0.36	0.108
			A5	Suplantación de la identidad del usuario	Si	Moderado	0.5	Poco frecuente	Menor	0.4	0.4	0.16	0.08
			A12	Análisis de tráfico	Si	Moderado	0.5	Poco frecuente	Menor	0.4	0.4	0.16	0.08
			A14	Interceptación de información (escucha)	Si	Moderado	0.5	Poco frecuente	Menor	0.4	0.4	0.16	0.08
			A9	Re-encaminamiento intencional de mensajes	No	No existente	0.0	Nada frecuente	Menor	0.2	0.4	0.08	0.08
			A6	Abuso de privilegios de acceso	Si	Adecuado	0.7	Poco frecuente	Moderado	0.4	0.6	0.24	0.072
			A27	Ocupación no autorizada	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			A11	Acceso no autorizado	Si	Adecuado	0.7	Nada frecuente	Moderado	0.2	0.6	0.12	0.036
			A25	Robo	Si	Muy Adecuado	0.9	Nada frecuente	Mayor	0.2	0.8	0.16	0.016
6	Proveedores de telecomunicaciones	12.5	N2	Daños por agua (sin intervención humana)	No	Muy débil	0.0	Poco frecuente	Catastrófico	0.4	1.0	0.4	0.4
			N*	Desastres naturales	Si	Muy débil	0.1	Poco frecuente	Catastrófico	0.4	1.0	0.4	0.36
			I3	Contaminación mecánica	No	No existente	0.0	Poco frecuente	Moderado	0.4	0.6	0.24	0.24
			I6	Corte del suministro eléctrico	Si	Adecuado	0.7	Frecuente	Mayor	0.8	0.8	0.64	0.192
			E2	Errores del administrador	Si	Moderado	0.5	Normal	Moderado	0.6	0.6	0.36	0.18
			E4	Errores de configuración	Si	Moderado	0.5	Normal	Moderado	0.6	0.6	0.36	0.18
			A4	Manipulación de la configuración	Si	Moderado	0.5	Normal	Moderado	0.6	0.6	0.36	0.18
			I2	Daños por agua (con intervención humana)	No	No existente	0.0	Nada frecuente	Mayor	0.2	0.8	0.16	0.16
			I*	Desastres industriales	No	No existente	0.0	Nada frecuente	Mayor	0.2	0.8	0.16	0.16
			I4	Contaminación electromagnética	No	No existente	0.0	Nada frecuente	Mayor	0.2	0.8	0.16	0.16
			I8	Fallo de servicios de comunicaciones	Si	Adecuado	0.7	Normal	Mayor	0.6	0.8	0.48	0.144
			I9	Interrupción de otros servicios y suministros esenciales	Si	Adecuado	0.7	Normal	Mayor	0.6	0.8	0.48	0.144
			N1	Fuego (sin intervención humana)	Si	Adecuado	0.7	Poco frecuente	Catastrófico	0.4	1.0	0.4	0.12
			E24	Caída del sistema por agotamiento de recursos	Si	Moderado	0.5	Poco frecuente	Moderado	0.4	0.6	0.24	0.12
			I7	Condiciones inadecuadas de temperatura y/o humedad	Si	Adecuado	0.7	Normal	Moderado	0.6	0.6	0.36	0.108
			A26	Ataque destructivo	Si	Adecuado	0.7	Normal	Moderado	0.6	0.6	0.36	0.108
			E1	Errores de los usuarios	Si	Adecuado	0.7	Poco frecuente	Moderado	0.4	0.6	0.24	0.072
			A24	Denegación de servicio	Si	Adecuado	0.7	Poco frecuente	Moderado	0.4	0.6	0.24	0.072
			I1	Fuego (con intervención humana)	Si	Adecuado	0.7	Nada frecuente	Catastrófico	0.2	1.0	0.2	0.06
			A7	Uso no previsto	Si	Adecuado	0.7	Nada frecuente	Moderado	0.2	0.6	0.12	0.036
1	Ingenieros de Telemática	12.2	A29	Extorsión	No	No existente	0.0	Nada frecuente	Menor	0.2	0.4	0.08	0.08
			A30	Ingeniería social	No	No existente	0.0	Nada frecuente	Menor	0.2	0.4	0.08	0.08
			E7	Deficiencias en la organización	Si	Adecuado	0.7	Normal	Menor	0.6	0.4	0.24	0.072
			E28	Indisponibilidad accidental del personal	Si	Adecuado	0.7	Normal	Menor	0.6	0.4	0.24	0.072
			A28	Indisponibilidad deliberada del personal	Si	Adecuado	0.7	Nada frecuente	Menor	0.2	0.4	0.08	0.024
7	Proveedores servicios de telefonia	11.3	N2	Daños por agua (sin intervención humana)	No	Adecuado	0.0	Poco frecuente	Mayor	0.4	0.8	0.32	0.32
			I3	Contaminación mecánica	No	No existente	0.0	Poco frecuente	Moderado	0.4	0.6	0.24	0.24
			I6	Corte del suministro eléctrico	Si	Adecuado	0.7	Frecuente	Mayor	0.8	0.8	0.64	0.192
			E4	Errores de configuración	Si	Moderado	0.5	Normal	Moderado	0.6	0.6	0.36	0.18
			A4	Manipulación de la configuración	Si	Moderado	0.5	Normal	Moderado	0.6	0.6	0.36	0.18
			E24	Caída del sistema por agotamiento de recursos	Si	Moderado	0.5	Poco frecuente	Mayor	0.4	0.8	0.32	0.16
			I2	Daños por agua (con intervención humana)	No	No existente	0.0	Nada frecuente	Mayor	0.2	0.8	0.16	0.16
			I*	Desastres industriales	No	No existente	0.0	Nada frecuente	Mayor	0.2	0.8	0.16	0.16
			I4	Contaminación electromagnética	No	No existente	0.0	Nada frecuente	Mayor	0.2	0.8	0.16	0.16
			I8	Fallo de servicios de comunicaciones	Si	Adecuado	0.7	Frecuente	Moderado	0.8	0.6	0.48	0.144
			I9	Interrupción de otros servicios y suministros esenciales	Si	Adecuado	0.7	Frecuente	Moderado	0.8	0.6	0.48	0.144
			N*	Desastres naturales	Si	Moderado	0.5	Poco frecuente	Moderado	0.4	0.6	0.24	0.12
			E2	Errores del administrador	Si	Moderado	0.5	Poco frecuente	Moderado	0.4	0.6	0.24	0.12
			I7	Condiciones inadecuadas de temperatura y/o humedad	Si	Adecuado	0.7	Normal	Menor	0.6	0.4	0.24	0.072
			E1	Errores de los usuarios	Si	Adecuado	0.7	Normal	Menor	0.6	0.4	0.24	0.072
			N1	Fuego (sin intervención humana)	Si	Adecuado	0.7	Nada frecuente	Catastrófico	0.2	1.0	0.2	0.06
			I1	Fuego (con intervención humana)	Si	Adecuado	0.7	Nada frecuente	Catastrófico	0.2	1.0	0.2	0.06
			A26	Ataque destructivo	Si	Adecuado	0.7	Nada frecuente	Catastrófico	0.2	1.0	0.2	0.06
			A7	Uso no previsto	Si	Adecuado	0.7	Nada frecuente	Moderado	0.2	0.6	0.12	0.036
			A24	Denegación de servicio	Si	Adecuado	0.7	Nada frecuente	Moderado	0.2	0.6	0.12	0.036
12	Equipos de telefonía	10.9	N2	Daños por agua (sin intervención humana)	No	No existente	0.0	Poco frecuente	Mayor	0.4	0.8	0.32	0.32
			I3	Contaminación mecánica	No	No existente	0.0	Poco frecuente	Moderado	0.4	0.6	0.24	0.24
			I6	Corte del suministro eléctrico	Si	Adecuado	0.7	Frecuente	Mayor	0.8	0.8	0.64	0.192
			I2	Daños por agua (con intervención humana)	No	No existente	0.0	Nada frecuente	Mayor	0.2	0.8	0.16	0.16
			I*	Desastres industriales	No	No existente	0.0	Nada frecuente	Mayor	0.2	0.8	0.16	0.16
			I4	Contaminación electromagnética	No	No existente	0.0	Nada frecuente	Mayor	0.2	0.8	0.16	0.16
			A24	Denegación de servicio	Si	Adecuado	0.7	Normal	Mayor	0.6	0.8	0.48	0.144
			N*	Desastres naturales	Si	Moderado	0.5	Poco frecuente	Moderado	0.4	0.6	0.24	0.12
			E2	Errores del administrador	Si	Adecuado	0.7	Normal	Moderado	0.6	0.6	0.36	0.108
			I5	Avería de origen físico o lógico	Si	Adecuado	0.7	Poco frecuente	Mayor	0.4	0.8	0.32	0.096
			E24	Caída del sistema por agotamiento de recursos	Si	Adecuado	0.7	Poco frecuente	Mayor	0.4	0.8	0.32	0.096
			I7	Condiciones inadecuadas de temperatura y/o humedad	Si	Adecuado	0.7	Normal	Menor	0.6	0.4	0.24	0.072
			E23	Errores de mantenimiento / actualización de equipos (hardware)	Si	Adecuado	0.7	Poco frecuente	Moderado	0.4	0.6	0.24	0.072
			N1	Fuego (sin intervención humana)	Si	Adecuado	0.7	Nada frecuente	Catastrófico	0.2	1.0	0.2	0.06
			I1	Fuego (con intervención humana)	Si	Adecuado	0.7	Nada frecuente	Catastrófico	0.2	1.0	0.2	0.06
			A26	Ataque destructivo	Si	Adecuado	0.7	Nada frecuente	Catastrófico	0.2	1.0	0.2	0.06
			A25	Robo	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			A27	Ocupación no autorizada	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			A4	Manipulación de la configuración	Si	Muy Adecuado	0.9	Normal	Moderado	0.6	0.6	0.36	0.036
			A7	Uso no previsto	Si	Adecuado	0.7	Nada frecuente	Menor	0.2	0.4	0.08	0.024
			E4	Errores de configuración	Si	Muy Adecuado	0.9	Poco frecuente	Moderado	0.4	0.6	0.24	0.024

Tabla 61. Activos y Riesgos de Telco priorizados **[5]** (Continuación)

ID ACTIVO	IDENTIFICACIÓN	VALOR CONSOLIDADO	AMENAZAS		SALVAGUARDAS			RIESGOS					
	Nombre activo	TOTAL	ID	DESCRIPCIÓN	Posee un control	Solidez del control	Nivel de mitigación	Probabilidad (Frecuencia)	Impacto (Degradación)	Valor probabilidad	Valor impacto	Riesgo Inherente	Riesgo Marginal
17	Planes de continuidad	10.9	E1	Errores de los usuarios	Si	Débil	0.3	Normal	Moderado	0.6	0.6	0.36	0.252
			E2	Errores del administrador	No	No existente	0.0	Poco frecuente	Moderado	0.4	0.6	0.24	0.24
			E3	Errores de monitorización (log)	Si	Muy débil	0.1	Normal	Menor	0.6	0.4	0.24	0.216
			E4	Errores de configuración	Si	Moderado	0.5	Poco frecuente	Moderado	0.4	0.6	0.24	0.12
			E15	Alteración de la información	Si	Muy débil	0.1	Poco frecuente	Moderado	0.4	0.6	0.24	0.216
			E16	Introducción de información incorrecta	Si	Moderado	0.5	Poco frecuente	Moderado	0.4	0.6	0.24	0.12
			E17	Degradación de la información	Si	Moderado	0.5	Normal	Moderado	0.6	0.6	0.36	0.18
			A4	Manipulación de la configuración	Si	Moderado	0.5	Frecuente	Moderado	0.8	0.6	0.48	0.24
			A11	Acceso no autorizado	Si	Adecuado	0.7	Nada frecuente	Menor	0.2	0.4	0.08	0.024
			A15	Modificación de la información (intencional)	Si	Adecuado	0.7	Nada frecuente	Moderado	0.2	0.6	0.12	0.036
			A16	Introducción de falsa información	Si	Adecuado	0.7	Nada frecuente	Moderado	0.2	0.6	0.12	0.036
			A17	Corrupción de la información (intencional)	Si	Adecuado	0.7	Nada frecuente	Moderado	0.2	0.6	0.12	0.036
4	Carpeta Solicitud de Servicios	10.6	N2	Daños por agua (sin intervención humana)	No	No existente	0.0	Poco frecuente	Mayor	0.4	0.8	0.32	0.32
			I6	Corte del suministro eléctrico	Si	Adecuado	0.7	Muy frecuente	Mayor	1.0	0.8	0.8	0.24
			E1	Errores de los usuarios	Si	Moderado	0.5	Muy frecuente	Menor	1.0	0.4	0.4	0.2
			E4	Errores de configuración	Si	Adecuado	0.7	Frecuente	Mayor	0.8	0.8	0.64	0.192
			N*	Desastres naturales	Si	Moderado	0.5	Poco frecuente	Mayor	0.4	0.8	0.32	0.16
			I2	Daños por agua (con intervención humana)	No	No existente	0.0	Nada frecuente	Mayor	0.2	0.8	0.16	0.16
			E2	Errores del administrador	Si	Adecuado	0.7	Frecuente	Moderado	0.8	0.6	0.48	0.144
			I*	Desastres industriales	No	No existente	0.0	Nada frecuente	Moderado	0.2	0.6	0.12	0.12
			I3	Contaminación mecánica	No	No existente	0.0	Nada frecuente	Moderado	0.2	0.6	0.12	0.12
			I4	Contaminación electromagnética	No	No existente	0.0	Nada frecuente	Moderado	0.2	0.6	0.12	0.12
			I5	Avería de origen físico o lógico	Si	Adecuado	0.7	Normal	Moderado	0.6	0.6	0.36	0.108
			E18	Destrucción de información	Si	Adecuado	0.7	Normal	Moderado	0.6	0.6	0.36	0.108
			A26	Ataque destructivo	Si	Adecuado	0.7	Nada frecuente	Catastrófico	0.2	1.0	0.2	0.06
			N1	Fuego (sin intervención humana)	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			I1	Fuego (con intervención humana)	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			A18	Destrucción la información (intencional)	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			I7	Condiciones inadecuadas de temperatura y/o humedad	Si	Muy Adecuado	0.9	Frecuente	Moderado	0.8	0.6	0.48	0.048
			I10	Degradación de los soportes de almacenamiento de la información	Si	Muy Adecuado	0.9	Normal	Mayor	0.6	0.8	0.48	0.048
			A4	Manipulación de la configuración	Si	Muy Adecuado	0.9	Poco frecuente	Mayor	0.4	0.8	0.32	0.032
			A25	Robo	Si	Muy Adecuado	0.9	Nada frecuente	Menor	0.2	0.4	0.08	0.008
2	Analistas de telemática	10.2	A29	Extorsión	No	No existente	0.0	Nada frecuente	Menor	0.2	0.4	0.08	0.08
			A30	Ingeniería social	No	No existente	0.0	Nada frecuente	Menor	0.2	0.4	0.08	0.08
			E7	Deficiencias en la organización	Si	Adecuado	0.7	Normal	Menor	0.6	0.4	0.24	0.072
			E28	Indisponibilidad accidental del personal	Si	Adecuado	0.7	Normal	Menor	0.6	0.4	0.24	0.072
			A28	Indisponibilidad deliberada del personal	Si	Adecuado	0.7	Nada frecuente	Menor	0.2	0.4	0.08	0.024
21	Software de monitoreo	10.2	E2	Errores del administrador	No	Adecuado	0.0	Normal	Moderado	0.6	0.6	0.36	0.36
			A4	Manipulación de la configuración	Si	Adecuado	0.7	Frecuente	Moderado	0.8	0.6	0.48	0.144
			E3	Errores de monitorización (log)	Si	Moderado	0.5	Normal	Menor	0.6	0.4	0.24	0.12
			E4	Errores de configuración	Si	Moderado	0.5	Poco frecuente	Moderado	0.4	0.6	0.24	0.12
			E20	Vulnerabilidades de los programas (software)	Si	Adecuado	0.7	Normal	Moderado	0.6	0.6	0.36	0.108
			E9	Errores de re-encaminamiento	No	No existente	0.0	Nada frecuente	Menor	0.2	0.4	0.08	0.08
			A9	Re-encaminamiento intencional de mensajes	No	No existente	0.0	Nada frecuente	Menor	0.2	0.4	0.08	0.08
			E1	Errores de los usuarios	Si	Adecuado	0.7	Poco frecuente	Moderado	0.4	0.6	0.24	0.072
			E21	Errores de mantenimiento / actualización de programas (software)	Si	Adecuado	0.7	Poco frecuente	Moderado	0.4	0.6	0.24	0.072
			E10	Errores de secuencia	Si	Moderado	0.5	Nada frecuente	Moderado	0.2	0.6	0.12	0.06
			E8	Difusión de software dañino	Si	Muy Adecuado	0.9	Frecuente	Moderado	0.8	0.6	0.48	0.048
			A11	Acceso no autorizado	Si	Adecuado	0.7	Nada frecuente	Moderado	0.2	0.6	0.12	0.036
			A5	Suplantación de la identidad del usuario	Si	Adecuado	0.7	Nada frecuente	Menor	0.2	0.4	0.08	0.024
			A6	Abuso de privilegios de acceso	Si	Adecuado	0.7	Nada frecuente	Menor	0.2	0.4	0.08	0.024
			A10	Alteración de secuencia	Si	Adecuado	0.7	Nada frecuente	Menor	0.2	0.4	0.08	0.024
			A8	Difusión deliberada de software dañino	Si	Muy Adecuado	0.9	Poco frecuente	Moderado	0.4	0.6	0.24	0.024
			A22	Manipulación de programas	Si	Muy Adecuado	0.9	Nada frecuente	Moderado	0.2	0.6	0.12	0.012
8	Contratos	9.8	A11	Acceso no autorizado	Si	Moderado	0.5	Poco frecuente	Menor	0.4	0.4	0.16	0.08
			A14	Interceptación de información (escucha)	Si	Moderado	0.5	Poco frecuente	Menor	0.4	0.4	0.16	0.08
			E14	Escapes de información	Si	Adecuado	0.7	Poco frecuente	Menor	0.4	0.4	0.16	0.048
			A19	Divulgación de información (intencional)	Si	Adecuado	0.7	Poco frecuente	Menor	0.4	0.4	0.16	0.048
			E19	Divulgación de información por indiscreción	Si	Adecuado	0.7	Poco frecuente	Insignificante	0.4	0.2	0.08	0.024
			E2	Errores del administrador	Si	Muy Adecuado	0.9	Poco frecuente	Moderado	0.4	0.6	0.24	0.024
			E4	Errores de configuración	Si	Muy Adecuado	0.9	Poco frecuente	Moderado	0.4	0.6	0.24	0.024
			A4	Manipulación de la configuración	Si	Muy Adecuado	0.9	Poco frecuente	Moderado	0.4	0.6	0.24	0.024
			A25	Robo	Si	Muy Adecuado	0.9	Nada frecuente	Menor	0.2	0.4	0.08	0.008
18	Registro de incidentes	9.4	E1	Errores de los usuarios	No	No existente	0.0	Normal	Moderado	0.6	0.6	0.36	0.36
			E2	Errores del administrador	No	No existente	0.0	Poco frecuente	Moderado	0.4	0.6	0.24	0.24
			E4	Errores de configuración	No	No existente	0.0	Poco frecuente	Menor	0.4	0.4	0.16	0.16
			E3	Errores de monitorización (log)	No	No existente	0.0	Poco frecuente	Insignificante	0.4	0.2	0.08	0.08
			E15	Alteración de la información	Si	Adecuado	0.7	Poco frecuente	Moderado	0.4	0.6	0.24	0.072
			E16	Introducción de información incorrecta	Si	Adecuado	0.7	Poco frecuente	Moderado	0.4	0.6	0.24	0.072
			E17	Degradación de la información	Si	Adecuado	0.7	Poco frecuente	Moderado	0.4	0.6	0.24	0.072
			A4	Manipulación de la configuración	Si	Adecuado	0.7	Normal	Menor	0.6	0.4	0.24	0.072
			A16	Introducción de falsa información	Si	Adecuado	0.7	Poco frecuente	Menor	0.4	0.4	0.16	0.048
			A15	Modificación de la información (intencional)	Si	Adecuado	0.7	Nada frecuente	Moderado	0.2	0.6	0.12	0.036
			A17	Corrupción de la información (intencional)	Si	Adecuado	0.7	Nada frecuente	Moderado	0.2	0.6	0.12	0.036
			A11	Acceso no autorizado	Si	Adecuado	0.7	Nada frecuente	Insignificante	0.2	0.2	0.04	0.012

Tabla 61. Activos y Riesgos de Telco priorizados **[5]** (Continuación)

ID ACTIVO	IDENTIFICACIÓN	VALOR CONSOLIDADO	AMENAZAS		SALVAGUARDAS			RIESGOS					
	Nombre activo	TOTAL	ID	DESCRIPCIÓN	Posee un control	Solidez del control	Nivel de mitigación	Probabilidad (Frecuencia)	Impacto (Degradación)	Valor probabilidad	Valor impacto	Riesgo Inherente	Riesgo Marginal
20	Software de registro de incidentes	8.9	E2	Errores del administrador	No	No existente	0.0	Normal	Menor	0.6	0.4	0.24	0.24
			E3	Errores de monitorización (log)	Si	Muy débil	0.1	Normal	Menor	0.6	0.4	0.24	0.216
			E20	Vulnerabilidades de los programas (software)	Si	Moderado	0.5	Normal	Moderado	0.6	0.6	0.36	0.18
			E4	Errores de configuración	No	No existente	0.0	Poco frecuente	Menor	0.4	0.4	0.16	0.16
			E1	Errores de los usuarios	Si	Adecuado	0.7	Normal	Moderado	0.6	0.6	0.36	0.108
			A4	Manipulación de la configuración	Si	Adecuado	0.7	Normal	Moderado	0.6	0.6	0.36	0.108
			E9	Errores de re-encaminamiento	No	No existente	0.0	Nada frecuente	Menor	0.2	0.4	0.08	0.08
			A9	Re-encaminamiento intencional de mensajes	No	No existente	0.0	Nada frecuente	Menor	0.2	0.4	0.08	0.08
			E21	Errores de mantenimiento / actualización de programas (software)	Si	Adecuado	0.7	Poco frecuente	Moderado	0.4	0.6	0.24	0.072
			E8	Difusión de software dañino	Si	Muy Adecuado	0.9	Frecuente	Moderado	0.8	0.6	0.48	0.048
			E10	Errores de secuencia	Si	Adecuado	0.7	Nada frecuente	Menor	0.2	0.4	0.08	0.024
			A5	Suplantación de la identidad del usuario	Si	Adecuado	0.7	Nada frecuente	Menor	0.2	0.4	0.08	0.024
			A6	Abuso de privilegios de acceso	Si	Adecuado	0.7	Nada frecuente	Menor	0.2	0.4	0.08	0.024
			A10	Alteración de secuencia	Si	Adecuado	0.7	Nada frecuente	Menor	0.2	0.4	0.08	0.024
			A11	Acceso no autorizado	Si	Adecuado	0.7	Nada frecuente	Menor	0.2	0.4	0.08	0.024
			A8	Difusión deliberada de software dañino	Si	Muy Adecuado	0.9	Poco frecuente	Moderado	0.4	0.6	0.24	0.024
			A22	Manipulación de programas	Si	Muy Adecuado	0.9	Nada frecuente	Moderado	0.2	0.6	0.12	0.012
15	Internet	8.3	A12	Análisis de tráfico	Si	Moderado	0.5	Muy frecuente	Mayor	1.0	0.8	0.8	0.4
			A14	Interceptación de información (escucha)	Si	Moderado	0.5	Muy frecuente	Mayor	1.0	0.8	0.8	0.4
			A4	Manipulación de la configuración	Si	Adecuado	0.7	Frecuente	Moderado	0.8	0.6	0.48	0.144
			I11	Emanaciones electromagnéticas	No	No existente	0.0	Nada frecuente	Moderado	0.2	0.6	0.12	0.12
			E4	Errores de configuración	Si	Adecuado	0.7	Poco frecuente	Mayor	0.4	0.8	0.32	0.096
			E14	Escapes de información	Si	Adecuado	0.7	Poco frecuente	Mayor	0.4	0.8	0.32	0.096
			A6	Abuso de privilegios de acceso	Si	Adecuado	0.7	Poco frecuente	Mayor	0.4	0.8	0.32	0.096
			A11	Acceso no autorizado	Si	Adecuado	0.7	Poco frecuente	Mayor	0.4	0.8	0.32	0.096
			A25	Robo	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			A27	Ocupación no autorizada	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			E2	Errores del administrador	Si	Muy Adecuado	0.9	Normal	Mayor	0.6	0.8	0.48	0.048
			A5	Suplantación de la identidad del usuario	Si	Muy Adecuado	0.9	Poco frecuente	Mayor	0.4	0.8	0.32	0.032
			E9	Errores de re-encaminamiento	Si	Muy Adecuado	0.9	Nada frecuente	Mayor	0.2	0.8	0.16	0.016
			A9	Re-encaminamiento intencional de mensajes	Si	Muy Adecuado	0.9	Nada frecuente	Mayor	0.2	0.8	0.16	0.016
3	Documentación sistema de Calidad	7.3	E2	Errores del administrador	Si	Moderado	0.5	Normal	Mayor	0.6	0.8	0.48	0.24
			E4	Errores de configuración	Si	Adecuado	0.7	Normal	Mayor	0.6	0.8	0.48	0.144
			A4	Manipulación de la configuración	Si	Adecuado	0.7	Normal	Mayor	0.6	0.8	0.48	0.144
			A19	Divulgación de información (intencional)	Si	Débil	0.3	Nada frecuente	Menor	0.2	0.4	0.08	0.056
			A11	Acceso no autorizado	Si	Adecuado	0.7	Poco frecuente	Menor	0.4	0.4	0.16	0.048
			E19	Divulgación de información por indiscreción	Si	Moderado	0.5	Nada frecuente	Menor	0.2	0.4	0.08	0.04
			A25	Robo	Si	Moderado	0.5	Nada frecuente	Menor	0.2	0.4	0.08	0.04
			A14	Interceptación de información (escucha)	Si	Adecuado	0.7	Nada frecuente	Menor	0.2	0.4	0.08	0.024
			E14	Escapes de información	Si	Adecuado	0.7	Nada frecuente	Insignificante	0.2	0.2	0.04	0.012
9	Caja menor	6.4	A7	Uso no previsto	Si	Adecuado	0.7	Poco frecuente	Moderado	0.4	0.6	0.24	0.072
			A25	Robo	Si	Adecuado	0.7	Nada frecuente	Mayor	0.2	0.8	0.16	0.048
			A11	Acceso no autorizado	Si	Muy Adecuado	0.9	Poco frecuente	Mayor	0.4	0.8	0.32	0.032
16	Planes de mejoramiento	6.3	A4	Manipulación de la configuración	Si	Moderado	0.5	Frecuente	Menor	0.8	0.4	0.32	0.16
			E2	Errores del administrador	No	No existente	0.0	Poco frecuente	Menor	0.4	0.4	0.16	0.16
			E4	Errores de configuración	Si	Moderado	0.5	Poco frecuente	Menor	0.4	0.4	0.16	0.08
			A14	Interceptación de información (escucha)	Si	Moderado	0.5	Poco frecuente	Menor	0.4	0.4	0.16	0.08
			A19	Divulgación de información (intencional)	Si	Débil	0.3	Nada frecuente	Menor	0.2	0.4	0.08	0.056
			E14	Escapes de información	Si	Moderado	0.5	Nada frecuente	Menor	0.2	0.4	0.08	0.04
			E19	Divulgación de información por indiscreción	Si	Moderado	0.5	Nada frecuente	Menor	0.2	0.4	0.08	0.04
			A11	Acceso no autorizado	Si	Adecuado	0.7	Nada frecuente	Menor	0.2	0.4	0.08	0.024
			A25	Robo	Si	Adecuado	0.7	Nada frecuente	Menor	0.2	0.4	0.08	0.024

Con estas tablas priorizadas ya se cuenta con el insumo necesario para iniciar el ciclo de Gestión de Riesgos, donde se deberá definir el curso de acción para cada uno de los riesgos identificados conforme a las políticas de Coomeva para el tratamiento de los mismos y posteriormente volver a aplicar el ciclo aquí descrito.

7. CONCLUSIONES Y FUTURO TRABAJO

El modelo planteado por este trabajo cumple con el objetivo de entregar una herramienta en donde confluyen las propuestas de los principales marcos de referencia en lo que tiene que ver con la identificación y valoración de activos y con la identificación y valoración de sus riesgos; permitiendo hacerlo de una manera práctica, sencilla, que es fácilmente entendida y que al ser aplicada por una entidad, estará acogiendo las prácticas recomendadas y comúnmente auditadas por lo entes de control y, lo que es aún más importante, tendrá certeza de estar protegiendo los activos más críticos de las amenazas que mayor impacto puedan causar sobre el logro de los objetivos de la misma.

La construcción del Modelo Unificado para Identificación y Valoración de los Riesgos de los Activos de Información en una Organización deja identificado espacios para el desarrollo de al menos dos futuros trabajos. El primero de ellos es la definición de un modelo de gestión de riesgos para la fase de implementación de respuestas y evaluación de la eficacia de los controles que se establezcan como resultado del proceso de análisis de los riesgos que se identifican con la aplicación del modelo; con este quedaría concluido el ciclo completo de la gestión de riesgos, complementando el presente trabajo.

El segundo trabajo propuesto consiste en la automatización del modelo, partiendo de las definiciones aquí establecidas y ejecutando todo el ciclo de desarrollo de aplicaciones. Crear una herramienta automatizada que pueda ser utilizada en cualquier tipo de organización, basadas en las definiciones, procesos y métodos planteados en este trabajo, dado que uno de los inconvenientes de la propuesta es lo dispendioso del manejo de un gran número de activos, multiplicado por la cantidad de amenazas que puede tener cada uno de ellos y su manipulación para la priorización y ordenamiento conforme los valores que se van generando a lo largo del proceso.

Finalmente podemos decir que la multiplicidad de marcos de referencia si bien difieren en sus propuestas metodológicas, en el fondo mantienen un marco común para este tipo de procesos y la misión de trabajos como el presente es llegar a la simplicidad de este trasfondo y plasmarlo en herramientas que permitan a las organizaciones aplicarlas sin necesidad de sumergirse en las complejidades de las normas y *frameworks* que las rigen, permitiéndoles lograr los objetivos que finalmente requiere la organización y con esto vencer uno de los principales obstáculos para la adopción de la seguridad de la información identificado a lo largo de los años en las empresas Colombianas y Latinoamericanas, como lo han mostrado los resultados de las encuestas de seguridad realizadas por la Asociación Colombiana de Ingenieros de Sistemas (ACIS).

BIBLIOGRAFÍA

ACEITUNO CANAL, Vicente. Seguridad de La información. Mexico: Limusa, 2006. 149p. ISBN 968-18-6856-0.

BARRERA R., Tania; BORJA B. Sergio y BARRERA N., Jorge. Metodologia de implementación del GTI. En: Revista Sistemas. Enero-Marzo 2011, No. 118. p. 72-81.

CALDER, Alan. Nueve claves para el éxito.Ely: IT Governance Publishing, 2005. 127p. ISBN 958-9383-62-9.

CALDER, Alan, WATKINS Steve. International IT governance: an executive guide to ISO 17799/ISSO 27001. London: Kagen, 2006. 366p. ISBN 0749447486.

CANO, Jeimy J. La seguridad informática y los procesos de negocio: ¿dos mundos distintos? En: Revista Sistemas. Enero-Marzo 2008, No. 104. p. 53-61.

FERRER, Rodrigo. Modelo ISO 27001 alineado con ITIL v3 y Cobit 4.1. En: (26 de agosto de 2010: Bogotá D.C.). Memorias. Bogotá D.C.: Asociación Colombiana de Sistemas de Información, 2010. Disponible en internet: http://www.acis.org.co/fileadmin/Conferencias/ISO27001alineadoconITILCOBIT.pdf.

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Gestión del Riesgo. NTC 5254. Bogotá: ICONTEC 2004. 38p.

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Trabajos escritos: presentación y referencias bibliográficas. NTC 1486, NTC 5613, NTC 4490. Bogotá: ICONTEC 2008.

INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Information technology – Security techniques – Code of practice for information security management. ISO/IEC 17799. Geneva: ISO, 2005.

INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Information technology – Security techniques – Information security management systems – Requirements. ISO/IEC 27001. Geneva: ISO, 2005.

ISACA. IT Governance Global Status Report 2008. Rolling Meadows. IT Governance Institute, 2008. Disponible en internet (29 noviembre, 2011): http://www.isaca.org/bookstore/extras/Pages/IT-Governance-Global-Status-Report-2008.aspx.

ISACA. Global Status Report on the Governance of Enterprise IT (GEIT) — 2011. Rolling Meadows. IT Governance Institute, 2011. Disponible en internet (29 noviembre, 2011): http://www.isaca.org/Knowledge-Center/Research/Documents/Global-Status-Report-GEIT-10Jan2011-Research.pdf.

IT Governance Institute. Aligning COBIT, ITIL and ISO 17799 for Business Benefit. 2005. Disponible en internet (25 enero, 2010): http://www.itgovernance.co.uk/files/ITIL-COBiT-SO17799JointFramework.pdf.

IT Governance Institute. Cobit Mapping: Mapping of ISO/IEC 17799:2000 with COBIT, 2end Edition. 2006. Disponible en internet (17 noviembre, 2011): http://www.isaca-oregon.org/docs/Mapping%20Cobit%20to%20ISO%2017799.pdf.

IT Governance Institute. Information Risks: Whose Business Are They? 2005. Disponible en internet (17 noviembre, 2011): http://www.isaca.org/Knowledge-Center/Research/Documents/info-risks-whose-business.pdf.

IT Governance Institute. Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, 2006. Disponible en internet (29 noviembre, 2011): http://www.isaca.org/Knowledge-Center/Research/Documents/InfoSecGuidanceDirectorsExecMgt.pdf.

ITSMF. Foundations of IT Service Management based on ITIL. 2 ed. Wilco: Van Haren Publishing, 2006. ISBN 90-77212-58-2. 232p.

ITSMF. Frameworks for IT Management. Wilco: Van Haren Publishing, 2006. ISBN 90-77212-90-6. 227p.

Revista Sistemas. Bogotá D.C. Julio-Septiembre 2007, No. 101. ISSN 0120-5919.

Revista Sistemas. Bogotá D.C. Abril-Junio 2008, No. 105. ISSN 0120-5919.

Revista Sistemas. Bogotá D.C. Abril-Junio 2009, No. 110. ISSN 0120-5919.

Revista Sistemas. Bogotá D.C. Mayo-Julio 2010, No. 115. ISSN 0120-5919.

Revista Sistemas. Bogotá D.C. Abril-Junio 2011, No. 119. ISSN 0120-5919.

TRUJILLO, Dalia. EUP: Una guia para gerenciar áreas de tecnologia. En: Revista Sistemas. Enero-Marzo 2011, No. 118. p. 62-71.

WULGAERT, Tim. Security Awareness—Best Practices to Secure Your Enterprise. Rolling Meadows, ISACA, 2005. 124 p. ISBN 1-933-284-06-4.

REFERENCIAS BIBLIOGRÁFICAS

[1] Axentian, «Consultora Axentian,» marzo 2011. [En línea]. Available: http://www.axentian.com/index.php?option=com_docman&task=doc_download&gid=55&Itemid=59&lang=es.. [Último acceso: 06 diciembre 2011].

[2] ACIS, “Memorias VII Jornada Nacional de Seguridad Informática,” 14 diciembre 2007. [Online]. Available: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VII_JornadaSeguridad/VIIENSI.pdf. [Acesso em 12 diciembre 2011].

[3] ACIS, “Memorias IX Jornada Nacional de Seguridad Informática,” 7 diciembre 2009. [Online]. Available: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/IX_JornadaSeguridad/I-ELSI09-JJCM-Uniandes.pdf. [Acesso em 12 diciembre 2011].

[4] Gartner, “The 2007 Gartner Scenario: An Annual Report on the Current State and Future Directions of the IT Industry,” 15 septiembre 2007. [Online]. Available: http://my.gartner.com/portal/server.pt?open=512&objID=249&&PageID=864059&mode=2&in_hi_userid=2&cached=true&resId=522806&ref=AnalystProfile. [Acesso em 17 mayo 2011].

[5] F. Caviedes Sanabria e B. A. Prado Urrego, *Modelo unificado para identificación y valoración de los riesgos de los activos de información en una organización,* 2012.

[6] ISO/IEC, Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001), Geneva: ISO/IEC, 2005.

[7] ISO27000.es, MARZO 2012. [Online]. Available: http://www.iso27000.es/iso27000.html#section3e.

[8] IT Governance Institute (ITGI) y la Oficina Gubernamental de Comercio (OGC), “Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa,” IT GOVERNANCE INSTITUTE, 2008.

[9] ISO/IEC, Information technology - Security techniques - Code of practice for information security management (ISO/IEC 17799:2005), segunda ed., Geneva: ISO, 2005.

[10] IT Governance Institute, COBIT 4.1, Rolling Meadows: ISACA, 2007.

[11] IT Governance Institue, Enterprise Value: Governance of IT Investments, The Val IT Framework, Rolling Meadows.

[12] ITSMF-NL, Foundations of IT Service Management Based on ITIL V3, Van Haren Publishing, 2007.

[13] The Open Group, Open Information Security Management Maturity Model, Berkshire: The Open group, 2011.

[14] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION., “Information Technology, Security Techniques. Information Security Risk Management. ISO/IEC FDIS 27005:2008 (E),” INTERNATIONAL ORGANIZATION FOR STANDARDIZATION., GENEVA, 2008.

[15] Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), “Norma Técnica Colombiana NTC 5254 Gestión de Riesgo,” ICONTEC, Bogotá, 2004.

[16] ISACA, The Risk IT Framework, Rolling Meadows, 2009.

[17] itSMF, Frameworks for IT management, Wilco: Van Haren Publishing, 2006.

[18] G. Williams. [Online]. Available: http://www.mor-officialsite.com/AboutM_o_R/WhatIsM_o_R.aspx. [Acesso em 1 Abril 2012].

[19] G. Williams, 2011. [Online]. Available: http://www.best-management-practice.com/gempdf/MoR_1000Words_White_Paper_Dec11.pdf. [Acesso em 1 Abril 2012].

[20] Ministerio de Administraciones públicas, 20 Junio 2006. [Online]. Available: http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=P80029225 1293651550991&langPae=es&detalleLista=PAE_1276529683497133. [Acesso em 06 Febrero 2012].

[21] Ministerio de Administraciones públicas, Junio 2006. [Online]. Available: http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=P80029225 1293651550991&langPae=es&detalleLista=PAE_1276529683497133. [Acesso em 06 Febrero 2012].

[22] Information Technology Industry Council (ITI), “RECOMMENDATION FOR CREATING A COMPREHENSIVE FRAMEWORK FOR RISK MANAGEMENT AND COMPLIANCE IN THE FINANCIAL SERVICES AND INSURANCE INDUSTRIES,” International comitee for Information Technology Standards, Gaithersburg, MD 20899-8930, 2008.

ANEXOS

ANEXO A: COMPARATIVO PRÁCTICAS PARA GESTIÓN Y VALORACIÓN DE ACTIVOS.

Para las prácticas identificadas debemos considerar que COBIT, O-ISM3 e ISO/IEC 27002 ayudan a definir lo que debería hacerse, e ITIL proporciona el cómo para los aspectos de la gestión y se resaltan algunos aspectos generales tal como se presentan en [8].

“COBIT está basado en marcos de referencia establecidos, tales como CMM de SEI (*Software Engineering Institute*), ISO 9000, ITIL e ISO/IEC 27002; sin embargo, COBIT no incluye tareas y pasos de procesos porque, aunque está orientado a procesos de TI, es un marco de referencia para gestión y control antes que un marco de referencia para procesos. COBIT se focaliza en lo que una empresa necesita hacer, no cómo lo tiene que hacer, y la audiencia objetivo es la alta gerencia, los gerentes funcionales, los gerentes de TI y los auditores”.

“ITIL está basado en la definición de procesos de mejores prácticas para la gestión y el soporte de servicios de TI, antes que en la definición de un marco de control de amplio alcance. Se focaliza en el método y define un grupo más compacto de procesos”.

O-ISM3 define en [13] que “Una característica distintiva de de O-ISM3 es que se basa en un enfoque totalmente basado en el proceso de administración y madurez de seguridad de la información, sobre la base de que cada control necesita un proceso de administración de TI. Rompe los administración de seguridad de la información en un amplio pero manejable número de procesos, con los controles de seguridad pertinentes, identificándolos dentro de cada proceso como un conjunto esencial de ese proceso.” Y más adelante anota “Mientras muchos enfoques de gestión de seguridad de información consideran evaluación del riesgo como una primera etapa necesaria y O-ISM3 puede utilizarse como cualquier otra norma en este campo, no exige un enfoque basado en la evaluación de riesgo. En algunos casos, una empresa puede decidir no es necesario hacer una evaluación del riesgo para decidir que necesita un control de seguridad.

Como punto de referencia de las prácticas para la gestión y valoración de activos seleccionados para el modelo unificado se toma el mapeo de los objetivos de control de COBIT 4.1 e ITIL V3 (Tabla 62) con ISO/IEC 27002 de [8], tomando como base lo propuesto por la ISO/IEC 27002 para la gestión y valoración de activos de información complementada con lo propuesto por O-ISM3.

Tabla 62. Mapeo de los objetivos de control de COBIT 4.1 e ITIL V3 con ISO/IEC 27002 **[5]**

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3	Referencia O-ISM3
7.1 Responsabilidad sobre los activos	**7.0 Gestión de los activos**				
7.1.1 Inventario de activos		• PO2.2 Diccionario de datos empresarial y reglas de sintaxis de los datos • DS9.2 Identificación y mantenimiento de elementos de la configuración • DS9.3 Revisión de integridad de la configuración	• PO2 Definir la arquitectura de la información • DS9 Gestionar la configuración	• SD 5.2 Gestión de los datos y la información • SD 7 Consideraciones tecnológicas • ST 4.1.5.2 Preparación para la transición del servicio • ST 4.3.5.3 Identificación de la configuración • ST 4.3.5.4 Control de la configuración • ST 4.3.5.5 Contabilización y registro de estados • ST 4.3.5.6 Auditoría y verificación • SO 5.4 Gestión de servidores y soporte • SO 7 Consideraciones de tecnología (especialmente para licenciamiento, indicado en SO).	• TSP-3 Define Objetivos de seguridad • OSP-3 Gestión de inventarios • OSP-4 Dominio de IT Gestionado Control de Cambios • OSP-5 Dominio de IT Gestionado Parcheo (Patching) • OSP-6 Dominio de IT Gestionado Limpieza • OSP-7 Dominio de IT Gestionado Fortalecimiento (Hardening)
7.1.2 Propiedad de los activos		• PO4.9 Propiedad de los datos y sistemas • DS9.2 Identificación y mantenimiento de elementos de la configuración	• PO4 Definir los procesos, organización y relaciones de TI • DS9 Gestionar la configuración	• SO 6.3 Gestión técnica • ST 4.1.5.2 Preparación para la transición del servicio • ST 4.3.5.3 Identificación de la configuración • ST 4.3.5.4 Control de la configuración • ST 4.3.5.5 Contabilización y registro de estados	• OSP-3 Gestión de inventarios
7.1.3 Uso aceptable de activos		• PO4.10 Supervisión • PO6.2 Riesgo corporativo y marco de referencia del control interno de TI	• PO4 Definir los procesos, organización y relaciones de TI • PO6 Comunicar las aspiraciones y la dirección de la gerencia		• TSP-3 Define Objetivos de seguridad • GP-2 Auditoria del Sistema
7.2 Clasificación de la información					
7.2.1 Lineamientos para la clasificación		• PO2.3 Esquema de clasificación de datos • AI2.4 Seguridad y disponibilidad de las aplicaciones	• PO2 Definir la arquitectura de la información • AI2 Adquirir y mantener el software aplicativo	• SD 3.6.1 Diseño de soluciones de servicios • SD 5.2 Gestión de los datos y la información • SO 4.4.5.11 Errores detectados en el ambiente de desarrollo	• TSP-3 Define Objetivos de seguridad • TSP-6 Arquitectura de seguridad

Tabla62. Mapeo de los objetivos de control de COBIT 4.1 e ITIL V3 con ISO/IEC 27002 **[5]** (continuación)

Clasificaciones ISO/IEC 27002 información de soporte	Áreas clave ISO/IEC 27002	Objetivos de control COBIT 4.1	Procesos TI de COBIT	Referencia ITIL v3	Referencia O-ISM3
7.2.2 Etiquetado y manejo de la información		• DS9.1 Repositorio y línea base de configuración	• DS9 Gestionar la Configuración	• SS 8.2 Interfaces del servicio • ST 4.1.5.2 Preparación para la transición del servicio • ST 4.3.5.2 Gestión y planificación • ST 4.3.5.3 Identificación de la configuración • ST 4.3.5.4 Control de la configuración • ST 4.3.5.5 Contabilización y registro de estados	• OSP-3 Gestión de inventarios

Y el cruce de elementos comunes desde las prácticas propuestas por COBIT (Tabla 37) cuyo foco de gobierno de TI es Primario o Secundario en Gestión de Recursos.

Tabla 63. Enfoque común de procesos ISO27000, COBIT, ITIL y O-ISM3 **[5]**

Enfoque Gestión de	Enfoque Gestión de	PROCESO	
S	**S**	PO1	Definir un Plan Estratégico de TI
P	**S**	PO2	Definir la Arquitectura de la Información
P	**S**	PO3	Determinar la Dirección Tecnológica
P	**P**	PO4	Definir los Procesos, Organización y Relaciones de TI
S		PO5	Administrar la Inversión en TI
P	**S**	PO7	Administrar Recursos Humanos de TI
S	**S**	PO10	Administrar Proyectos
S	**S**	AI1	Identificar soluciones automatizadas
P		AI3	Adquirir y mantener infraestructura tecnológica
S	**S**	AI4	Facilitar la operación y el uso
P		AI5	Adquirir recursos de TI
P		AI6	Administrar cambios
S	**S**	AI7	Instalar y acreditar soluciones y cambios
P		DS1	Definir y administrar los niveles de servicio
S	**P**	DS2	Administrar los servicios de terceros
P	**S**	DS3	Administrar el desempeño y la capacidad
S	**P**	DS4	Garantizar la continuidad del servicio
P		DS6	Identificar y asignar costos
S	**S**	DS7	Educar y entrenar a los usuarios
P	**S**	DS9	Administrar la configuración
P	**P**	DS11	Administrar los datos
S	**P**	DS12	Administrar el ambiente físico
P		DS13	Administrar las operaciones
S	**S**	ME1	Monitorear y Evaluar el Desempeño de TI
P	**P**	ME4	Proporcionar Gobierno de TI

Tabla63. Enfoque común de procesos ISO27000, COBIT, ITIL y O-ISM3 **[5]** (Continuación)

Enfoque	Común	**COBIT**	con **ITIL**
Enfoque	Común	**COBIT**	con **ISO27000 (17799:2005)**
Enfoque	Común	**COBIT**	con **O-ISM3**
Enfoque	Común	**COBIT**	con **ITIL + ISO27000**
Enfoque	Común	**COBIT**	con **ITIL + O-ISM3**
Enfoque	Común	**COBIT**	con **ISO27000 + O-ISM3**

ANEXO B. ALINEACIÓN ORGANIZACIONAL.

En una unidad corporativa de servicios de tecnología se cuenta con el macroproceso de servicios telemáticos que ofrece los siguientes:

- Transmisión de voz y datos sobre la red corporativa
- Servicio de correo electrónico
- Servicio de video conferencia

Estos servicios son prestados a las empresas del grupo empresarial y facturados según la demanda que de cada uno de ellos se haga desde cada empresa.

Para priorizar la orientación que debe aplicar su SGSI al momento de realizar la evaluación de riesgos del macroproceso se aplica la proporción de ingresos a partir de la facturación a las empresas, dando como resultado un vector de procesos con prioridades como el mostrado en la Tabla 64.

Tabla 64. Vector de procesos [5]

Proceso	Transmisión de Datos/Voz	Correo Electrónico	Video Conferencia	TOTAL
Participación	50%	30%	20%	100%

ANEXO C. INVENTARIO DE ACTIVOS.

La Tabla 65 presenta un ejemplo de matriz para levantamiento de inventario de activos de información en una organización.

Tabla 65. Levantamiento de inventario de activos de información **[5]**

ID ACTIVO	IDENTIFICACIÓN			TIPO ACTIVO					
	Nombre activo	Propietario	Administrador	Información	Aplicaciones	Infraestructura	Personas	Servicios	Capital financiero
1	Planta telefónica	Servicios generales	Administrador telefonía			X			
2	Licencias CU	Empresas	Unidad de tecnología	X					
3	Administrador LAN	Unidad de Tecnología	Unidad de tecnología				X		
4									
5									
6									

Una vez valorados los activos del primer proceso, la matriz puede tomar una forma como la mostrada en la Tabla 66.

Tabla 66. Levantamiento de inventario de activos de información (primer proceso) **[5]**

ID ACTIVO	IDENTIFICACIÓN			TIPO ACTIVO						VALOR PROCESO 1			
										Peso proceso 1			50%
	Nombre activo	Propietario	Administrador	Información	Aplicaciones	Infraestructura	Personas	Servicios	Capital financiero	Confidencilidad	Integridad	Disponibilidad	Confiabilidad
1	Planta telefónica	Servicios generales	Administrador telefonía			X				2	5	4	5
2	Licencias CU	Empresas	Unidad de tecnología	X						3	4	4	1
3	Administrador LAN	Unidad de Tecnología	Unidad de tecnología				X			3	4	4	2
4													
5													
6													

Al concluir el ejercicio de identificación y valoración de activos de los procesos dentro del alcance de análisis de riesgo, la matriz diligenciada debe tener una forma similar a la mostrada en la Tabla 67.

Tabla 67. Resultado de identificar y valorar activos **[5]**

ID ACTIVO	IDENTIFICACIÓN			TIPO ACTIVO						VALOR PROCESO 1				VALOR PROCESO 2				VALOR PROCESO N			
										Peso proceso 1			50%	Peso proceso 2			30%	Peso proceso n			20%
	Nombre activo	Propietario	Administrador	Información	Aplicaciones	Infraestructura	Personas	Servicios	Capital financiero	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	Confidencialidad	Integridad	Disponibilidad	Confiabilidad
1	Planta telefónica	Servicios generales	Administrador telefonía			X				2	5	4	5	2	2	2	3	1	1	1	2
2	Licencias CU	Empresas	Unidad de tecnología	X						3	4	4	1	4	2	3	1	3	2	4	1
3	Administrador LAN	Unidad de Tecnología	Unidad de tecnología				X			3	4	4	2	3	2	4	2	1	1	4	2
4																					
5																					
6																					

El valor global de cada activo se calcula mediante la Fórmula 4.

Fórmula 4. Valor activo (ANEXO C)

$$ValorActivo = \sum_{i=1}^{n} (C_i + I_i + D_i + R_i) * PP_i$$

C : Confidencialidad
I : Integridad
D : Disponibilidad
R : Confiabilidad (*reliability*)
PP : Peso proceso

Valor activo 1 = (2+5+4+5)*50%+(2+2+2+3)*30%+(1+1+1+2)*20% = 11.7
Valor activo 2 = (3+4+4+1)*50%+(4+2+3+1)*30%+(3+2+4+1)*20% = 11
Valor activo 3 = (3+4+4+2)*50%+(3+2+4+2)*30%+(1+1+4+2)*20% = 11.4

Aplicando los datos anteriores, la matriz de valoración de activos final se convierte en la mostrada en la Tabla 68.

Tabla 68. Levantamiento de inventario de activos de información (final) **[5]**

ID ACTIVO	IDENTIFICACIÓN			TIPO ACTIVO						VALOR PROCESO 1				VALOR PROCESO 2				VALOR PROCESO N				VALOR ACTIVO
										Peso proceso 1			50%	Peso proceso 2			30%	Peso proceso n			20%	
	Nombre activo	Propietario	Administrador	Información	Aplicaciones	Infraestructura	Personas	Servicios	Capital financiero	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	
1	Planta telefónica	Servicios generales	Administrador telefonía			X				2	5	4	5	2	2	2	3	1	1	1	2	11.7
2	Licencias CU	Empresas	Unidad de tecnología	X						3	4	4	1	4	2	3	1	3	2	4	1	11
3	Administrador LAN	Unidad de Tecnología	Unidad de tecnología				X			3	4	4	2	3	2	4	2	1	1	4	2	11.4
4																						
5																						
6																						

ANEXO D. IDENTIFICACIÓN DE AMENAZAS.

Basado en MagerIT se presenta en la Tabla 69 un catálogo de amenazas posibles sobre los activos de un sistema de información y los atributos o dimensiones que son afectados por la amenaza.

Tabla 69. Catálogo de amenazas **[5]**[23]

AMENAZA			TIPO ACTIVO AMENAZADO						DIMENSIÓN AFECTADA			
ID	Nombre amenaza	Descripción	Información	Aplicaciones	Infraestructura	Personas	Servicios	Capital financiero	Confidencialidad	Integridad	Disponibilidad	Confiabilidad
	Desastres naturales (sin intervención humana)											
N1	Fuego (sin intervención humana)	incendios: posibilidad de que el fuego causado por un desastre natural acabe con recursos del sistema.	X		X		X				X	X
N2	Daños por agua (sin intervención humana)	inundaciones: posibilidad de que el agua acabe con recursos del sistema.	X		X		X				X	X
N*	Desastres naturales	otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc	X		X		X				X	X
	De origen industrial (con intervención humana)											
I1	Fuego (con intervención humana)	incendios: posibilidad de que el fuego generado por fallas industriales acabe con recursos del sistema.	X		X		X				X	X
I2	Daños por agua (con intervención humana)	escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	X		X		X				X	X
I*	Desastres industriales	otros desastres debidos a la actividad humana: explosiones, derrumbes, ... contaminación química, ... sobrecarga eléctrica, fluctuaciones eléctricas, ... accidentes de tráfico, ...	X		X		X				X	X
I3	Contaminación mecánica	vibraciones, polvo, suciedad, ...	X		X		X				X	X
I4	Contaminación electromagnética	interferencias de radio, campos magnéticos, luz ultravioleta, ...	X		X		X				X	X
I5	Avería de origen físico o lógico	fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.	X		X						X	X
I6	Corte del suministro eléctrico	cese de la alimentación de potencia	X		X		X				X	X
I7	Condiciones inadecuadas de temperatura y/o humedad	deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ...	X		X		X				X	X
I8	Fallo de servicios de comunicaciones	cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente					X				X	X
I9	Interrupción de otros servicios y suministros esenciales	otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante, ...					X				X	X
I10	Degradación de los soportes de almacenamiento de la información	como consecuencia del paso del tiempo	X								X	X
I11	Emanaciones electromagnéticas	hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.			X				X			

[23] Creada con base en la información en la propuesta de MagerIT [18].

Tabla 69. Catálogo de amenazas **[5]** (Continuación)

AMENAZA			TIPO ACTIVO AMENAZADO						DIMENSIÓN AFECTADA			
ID	Nombre amenaza	Descripción	Información	Aplicaciones	Infraestructura	Personas	Servicios	Capital financiero	Confidencialidad	Integridad	Disponibilidad	Confiabilidad
	Errores y fallos no intencionados											
E1	Errores de los usuarios	equivocaciones de las personas cuando usan los servicios, datos, etc.	X	X			X			X	X	X
E2	Errores del administrador	equivocaciones de personas con responsabilidades de instalación y operación	X	X	X		X		X	X	X	X
E3	Errores de monitorización (log)	inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ...	X	X			X			X		
E4	Errores de configuración	introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	X	X	X		X		X	X	X	
E7	Deficiencias en la organización	cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.				X					X	
E8	Difusión de software dañino	propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.		X					X	X	X	
E9	Errores de re-encaminamiento	envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.		X	X		X		X	X		
E10	Errores de secuencia	alteración accidental del orden de los mensajes transmitidos		X	X		X			X		
E14	Escapes de información	la información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	X	X	X				X			
E15	Alteración de la información	alteración accidental de la información.	X							X		
E16	Introducción de información incorrecta	inserción accidental de información incorrecta.	X							X		
E17	Degradación de la información	degradación accidental de la información.	X							X		
E18	Destrucción de información	pérdida accidental de información.	X								X	X
E19	Divulgación de información por indiscreción	revelación por indiscreción.	X						X			
E20	Vulnerabilidades de los programas (software)	defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.		X					X	X	X	X
E21	Errores de mantenimiento / actualización de programas (software)	defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante		X						X	X	X
E23	Errores de mantenimiento / actualización de equipos (hardware)	defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.			X						X	X
E24	Caída del sistema por agotamiento de recursos	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.			X		X				X	X
E28	Indisponibilidad accidental del personal	ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, ...				X					X	X

Tabla 69. Catálogo de amenazas **[5]** (Continuación)

AMENAZA			TIPO ACTIVO AMENAZADO						DIMENSIÓN AFECTADA			
ID	Nombre amenaza	Descripción	Información	Aplicaciones	Infraestructura	Personas	Servicios	Capital financiero	Confidencialidad	Integridad	Disponibilidad	Confiabilidad
	Ataques intencionados											
A4	Manipulación de la configuración	prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	X	X	X		X		X	X	X	X
A5	Suplantación de la identidad del usuario	cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.		X	X		X		X	X		
A6	Abuso de privilegios de acceso	cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.		X	X		X		X	X		
A7	Uso no previsto	utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.		X	X		X	X			X	X
A8	Difusión deliberada de software dañino	propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.		X					X	X	X	
A9	Re-encaminamiento intencional de mensajes	envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.		X	X		X		X	X		
A10	Alteración de secuencia	alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.		X	X		X			X		
A11	Acceso no autorizado	el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	X	X	X		X	X	X	X		
A12	Análisis de tráfico	el atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina "monitorización de tráfico".			X				X			
A14	Interceptación de información (escucha)	el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.	X	X	X				X			
A15	Modificación de la información (intencional)	alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.	X							X		
A16	Introducción de falsa información	inserción interesada de información falsa, con ánimo de obtener un beneficio o causar un perjuicio.	X							X		
A17	Corrupción de la información (intencional)	degradación intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.	X							X		
A18	Destrucción la información (intencional)	eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	X								X	X
A19	Divulgación de información (intencional)	revelación intencional de información.	X						X			

Tabla 69. Catálogo de amenazas **[5]** (Continuación)

AMENAZA			TIPO ACTIVO AMENAZADO						DIMENSIÓN AFECTADA			
ID	Nombre amenaza	Descripción	Información	Aplicaciones	Infraestructura	Personas	Servicios	Capital financiero	Confidencilidad	Integridad	Disponibilidad	Confiabilidad
A22	Manipulación de programas	alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.		X					X	X		
A24	Denegación de servicio	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.			X		X				X	X
A25	Robo	la sustracción de información provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de activos información, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información	X		X			X	X		X	X
A26	Ataque destructivo	vandalismo, terrorismo, acción militar, ... Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.	X		X		X				X	X
A27	Ocupación no autorizada	cuando las instalaciones son invadidas por personas que no han sido autorizadas			X				X		X	
A28	Indisponibilidad deliberada del personal	ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, ...				X					X	
A29	Extorsión	presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.				X			X	X		
A30	Ingeniería social	abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.				X			X	X		

Amenazas sobre activos tipo Información.

Apoyados en MagerIT, se identifican las amenazas que pueden ocurrir sobre los activos de tipo Información (Tabla 70).

Tabla 70. Amenazas sobre activos de información **[5]**[24]

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIABILIDAD
		N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7 I.10	N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7 I.10
E.2 E.3 E.14 E.19	E.1 E.2 E.3 E.15 E.16 E.17	E.1 E.2 E.4 E.18	E.1 E.2 E.18
A.4 A.11 A.14 A.19	A.4 A.11 A.15 A.16 A.17	A.4 A.18 A.25 A.26	A.4 A.18 A.25 A.26

Amenazas sobre activos tipo Aplicaciones.

Apoyados en MagerIT se identifican (Tabla 71) las amenazas pueden que ocurrir sobre los activos de tipo Aplicación.

Tabla 71. Amenazas sobre activos tipo de aplicación **[5]**[25]

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIABILIDAD
E.2 E.4 E.8 E.9 E.14 E.20	E.1 E.2 E.4 E.8 E.9 E.10 E.20 E.21	E.1 E.2 E.4 E.8 E.20 E.21	E.1 E.2 E.20 E.21
A.4 A.5 A.6 A.8 A.9 A.11 A.14 A.22	A.4 A.5 A.6 A.8 A.9 A.10 A.11 A.22	A.4 A.7 A.8	A.4 A.7

[24] Creada con base en la MagerIT [19].
[25] Creado con base en la propuesta de MagerIT [19].

Amenazas sobre activos tipo Infraestructura.

Apoyados en MagerIT se identifican (Tabla 72) las amenazas que pueden ocurrir sobre los activos de tipo Infraestructura.

Tabla 72. Amenazas sobre activos tipo de infraestructura **[5]**[26]

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIABILIDAD
I.11		N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7 I.8 I.9	N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7
E.2 E.4 E.9 E.14	E.2 E.4 E.9 E.10	E.2 E.4 E.23 E.24	E.2 E.22 E.23
A.4 A.5 A.6 A.9 A.11 A.12 A.14 A.25 A27	A.4 A.5 A.6 A.9 A.10 A.11	A.4 A.7 A.24 A.25 A.26 A.27	A.4 A.7 A.24 A.25 A.26

Amenazas sobre activos tipo Personas.

Apoyados en MagerIT se identifican (Tabla 73) las amenazas pueden ocurrir sobre los activos de tipo persona.

Tabla 73. Amenazas sobre activos tipo persona **[5]**

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIABILIDAD
		E.7 E.28	E.28
A.29 A.30	A.29 A.30	A.28	

[26] Creada con base en la propuesta de MagerIT [19].

Amenazas sobre activos tipo Servicios.

Apoyados en MagerIT se identifican (Tabla 74) las amenazas pueden ocurrir sobre los activos de tipo servicios.

Tabla 74. Amenazas sobre activos tipo servicio **[5]**[27]

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIABILIDAD
		N.1 N.2 N.*	N.1 N.2 N.*
		I.1 I.2 I.*	I.1 I.2 I.*
		I.3 I.4	I.3 I.4
		I.5	I.6
		I.6	I.7
		I.7	I.8
		I.10	I.9
E.2	E.1	E.1	E.1
E.4	E.2	E.2	E.2
E.9	E.4	E.4	E.24
	E.9	E.24	
	E.10		
A.4	A.4	A.4	A.4
A.5	A.5	A.7	A.7
A.6	A.6	A.24	A.24
A.9	A.9		A.26
A.11	A.10		
	A.11		

Amenazas sobre activos tipo Capital financiero

Apoyados en MagerIT se identifican (Tabla 75) las amenazas pueden ocurrir sobre los activos de tipo Capital Financiero.

Tabla 75. Amenazas sobre activos tipo capital financiero **[5]**

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIABILIDAD
A.11	A.11	A.7	A.7
A.25		A.25	A.25

[27] Creada con base en MagerIT [19].

ANEXO E. SELECCIÓN DE AMENAZAS.

Una vez identificados y valorados los activos, se seleccionan aquellos que represente mayor valor para el o los procesos dentro del alcance del análisis y apoyados en las tablas de amenazas, se identifican las que afectan los atributos o dimensiones de mayor valor para cada activo en evaluación.

La Tabla 76 es el fragmento de una matriz donde se muestran las amenazas para un activo tipo infraestructura cuyo mayor valor está en la dimensión o atributo Confiabilidad.

Tabla 76. Amenazas para activo tipo infraestructura **[5]**

ID ACTIVO	IDENTIFICACIÓN			VALOR CONSOLIDADO ACTIVO					AMENAZAS	
	Nombre activo	Propietario	Administrador	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	TOTAL	ID	DESCRIPCIÓN
1	Planta telefónica	Servicios generales	Administrador telefonía	1.8	3.3	2.8	3.8	11.7	N.1 N.2 N.*	incendios: posibilidad de que el fuego causado por un desastre natural acabe con recursos del sistema.inundaciones: posibilidad de que el agua acabe con recursos del sistema.otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc
									I.1 I.2 i:*	incendios: posibilidad de que el fuego generado por fallas industriales acabe con recursos del sistema.escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.otros desastres debidos a la actividad humana: explosiones, derrumbes, ... contaminación química, ... sobrecarga eléctrica, fluctuaciones eléctricas, ... accidentes de tráfico, ...
									I.3 I.4	vibraciones, polvo, suciedad, ...interferencias de radio, campos magnéticos, luz ultravioleta, ...
									I.5	fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.
									I.6	cese de la alimentación de potencia
									I.7	deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ...
									E.2	equivocaciones de personas con responsabilidades de instalación y operación
									E.23	defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.
									E.24	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
									A.4	prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
									A.7	utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
									A.24	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
									A.25	la sustracción de información provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de activos información, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información
									A.26	vandalismo, terrorismo, acción militar, ... Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

La Tabla 77 muestra las amenazas para un activo tipo personas.

Tabla 77. Amenazas para activo tipo personas **[5]**

ID ACTIVO	IDENTIFICACIÓN			VALOR CONSOLIDADO ACTIVO					AMENAZAS	
	Nombre activo	Propietario	Administrador	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	TOTAL	ID	DESCRIPCIÓN
3	Administrador LAN	Unidad de Tecnología	Unidad de tecnología	2.6	2.8	4	2	11.4	E.7	cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.
									E.28	ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, …
									A.28	ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, …
									A.29	presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
									A.30	abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.

La Tabla 78 muestra las amenazas para un activo tipo capital.

Tabla 78. Amenazas para activo tipo capital financiero **[5]**

ID ACTIVO	IDENTIFICACIÓN			VALOR CONSOLIDADO ACTIVO					AMENAZAS	
	Nombre activo	Propietario	Administrador	Confidencialidad	Integridad	Disponibilidad	Confiabilidad	TOTAL	ID	DESCRIPCIÓN
4	Caja menor	Unidad de Tecnología	Asistente Administrativo	1	1	1.8	2.1	5.9	A.7	utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
									A.11	el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
									A.25	la sustracción de información provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de activos información, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información

ANEXO F. EVALUACIÓN DE CONTROLES O SALVAGUARDAS.

Una vez identificados las amenazas, se debe identificar, primero si existe un control o salvaguarda que pueda mitigar su probabilidad o impacto y segundo cual puede ser su eficiencia. Una vez aplicada la Tabla 79 se presenta un fragmento de una matriz donde se muestran la evaluación de los controles o salvaguardas ya existentes para las amenazas de un activo tipo infraestructura (Tabla 80) cuyo mayor valor está en la dimensión o atributo Confiabilidad.

Tabla 79. Evaluación marginalidad salvaguarda **[5]**

Cualificación	Consideración	Eficiencia	Marginalidad
Muy Adecuado	El control o salvaguarda establecido tiene un diseño fuerte, es automático y se ha comprobado su efectividad	90%	0.1
Adecuado	El control o salvaguarda establecido tiene un diseño fuerte, **no** es automático, pero se ha comprobado su efectividad	70%	0.3
Moderado	El control o salvaguarda establecido tiene un diseño fuerte, no es automático o no se ha comprobado su efectividad	50%	0.5
Débil	El control o salvaguarda establecido **no** tiene un diseño fuerte, no es automático, pero se ha comprobado su efectividad	30%	0.7
Muy débil	El control o salvaguarda establecido no tiene un diseño fuerte, no es automático y no se ha comprobado su efectividad	10%	0.9

Tabla 80. Evaluación de los controles para las amenazas de un activo tipo infraestructura **[5]**

ID ACTIVO	IDENTIFICACIÓN			AMENAZAS		SALVAGUARDAS		
	Nombre activo	Propietario	Administrador	ID	DESCRIPCIÓN	Posee un control	Solidez del control	Nivel de mitigación
1	Planta telefónica	Servicios generales	Administrador telefonía	N.1 N.2 N.*	incendios: posibilidad de que el fuego causado por un desastre natural acabe con recursos del sistema.inundaciones: posibilidad de que el agua acabe con recursos del sistema.otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc	No	No existente	0.0
				I.1 I.2 i:*	incendios: posibilidad de que el fuego generado por fallas industriales acabe con recursos del sistema.escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.otros desastres debidos a la actividad humana: explosiones, derrumbes, ... contaminación química, ... sobrecarga eléctrica, fluctuaciones eléctricas, ... accidentes de tráfico, ...	Si	Adecuado	0.7
				I.3 I.4	vibraciones, polvo, suciedad, ...interferencias de radio, campos magnéticos, luz ultravioleta, ...	No	No existente	0.0
				I.5	fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.	Si	Moderado	0.5
				I.6	cese de la alimentación de potencia	Si	Muy Adecuado	0.9
				I.7	deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ...	Si	Muy Adecuado	0.9
				E.2	equivocaciones de personas con responsabilidades de instalación y operación	Si	Adecuado	0.7
				E.23	defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	Si	Adecuado	0.7
				E.24	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	Si	Moderado	0.5
				A.4	prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	Si	Adecuado	0.7
				A.7	utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.	Si	Moderado	0.5
				A.24	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	Si	Moderado	0.5
				A.25	la sustracción de información provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de activos información, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información	Si	Débil	0.3
				A.26	vandalismo, terrorismo, acción militar, ... Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.	Si	Muy débil	0.1

ANEXO G. VALORACIÓN DE RIESGO.

Aplicando para cada una de las amenazas identificadas las tablas de estimación de probabilidad o frecuencia de ocurrencia de la amenaza y de impacto o degradación del activo se pueden estimar los riesgos inherentes (Fórmula 5) y marginales (Fórmula 6).

Fórmula 5. Riesgo Inherente (ANEXO G)

$$RiesgoInherente = Frecuencia * Degradación$$

Fórmula 6. Riesgo marginal (ANEXO G)

$$RiesgoMarginal = RiesgoInherente + Marginalidad$$

Se tendrá como resultado una matriz donde se muestran los riesgos inherentes y marginales de un activo tipo infraestructura (Tabla 81) cuyo mayor valor está en la dimensión o atributo Confiabilidad.

Tabla 81. Riesgos inherentes y marginales de un activo tipo infraestructura **[5]**

ID ACTIVO	IDENTIFICACIÓN	AMENAZAS		SALVAGUARDAS			RIESGOS					
	Nombre activo	ID	DESCRIPCIÓN	Posee un control	Solidez del control	Nivel de mitigación	Probabilidad (Frecuencia)	Impacto (Degradación)	Valor probabilidad	Valor impacto	Riesgo Inherente	Riesgo Marginal
1	Planta telefónica	N.1 N.2 N.*	incendios: posibilidad de que el fuego causado por un desastre natural acabe con recursos del sistema.inundaciones: posibilidad de que el agua acabe con recursos del sistema.otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc	No	No existente	0.0	Poco frecuente	Catastrófico	0.4	1.0	0.40	0.4
		I.1 I.2 i:*	incendios: posibilidad de que el fuego generado por fallas industriales acabe con recursos del sistema.escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.otros desastres debidos a la actividad humana: explosiones, derrumbes, ... contaminación química, ... sobrecarga eléctrica, fluctuaciones eléctricas, ... accidentes de tráfico, ...	Si	Adecuado	0.7	Poco frecuente	Catastrófico	0.4	1.0	0.40	0.12
		I.3 I.4	vibraciones, polvo, suciedad, ...interferencias de radio, campos magnéticos, luz ultravioleta, ...	No	No existente	0.0	Poco frecuente	Moderado	0.4	0.6	0.24	0.24
		I.5	fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.	Si	Moderado	0.5	Normal	Mayor	0.6	0.8	0.48	0.24
		I.6	cese de la alimentación de potencia	Si	Muy Adecuado	0.9	Normal	Mayor	0.6	0.8	0.48	0.048
		I.7	deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ...	Si	Muy Adecuado	0.9	Normal	Menor	0.6	0.4	0.24	0.024
		E.2	equivocaciones de personas con responsabilidades de instalación y operación	Si	Adecuado	0.7	Frecuente	Moderado	0.8	0.6	0.48	0.144
		E.23	defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	Si	Adecuado	0.7	Muy frecuente	Menor	1.0	0.4	0.40	0.12
		E.24	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	Si	Moderado	0.5	Normal	Menor	0.6	0.4	0.24	0.12
		A.4	prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	Si	Adecuado	0.7	Poco frecuente	Moderado	0.4	0.6	0.24	0.072
		A.7	utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.	Si	Moderado	0.5	Frecuente	Menor	0.8	0.4	0.32	0.16
		A.24	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	Si	Moderado	0.5	Normal	Menor	0.6	0.4	0.24	0.12
		A.25	la sustracción de información provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de activos información, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información	Si	Débil	0.3	Poco frecuente	Menor	0.4	0.4	0.16	0.112
		A.26	vandalismo, terrorismo, acción militar, ... Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.	Si	Muy débil	0.1	Nada frecuente	Moderado	0.2	0.6	0.12	0.108