DISEÑO DE UN MARCO DE REFERENCIA ORIENTADO A LA PRESTACIÓN DE SERVICIOS DE GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN EN LA EMPRESA SOLINCOSTA

Jose Gómez Rebolledo *

Diego Jose Martinez Perez **

UNIVERSIDAD SIMÓN BOLÍVAR

* Ingeniero de Sistemas, Universidad Politécnico de la Costa Atlántica, Colombia. Estudiante, Especialización en Gestión de Tecnologías de la Información, Universidad Simón Bolívar, Colombia.

** Ingeniero de Sistemas, Universidad Cooperativa de Colombia, Colombia. Estudiante, Especialización en Gestión de Tecnologías de la Información, Universidad Simón Bolívar, Colombia.

CONTENIDO

1. RESUMEN

El uso de las TI en las empresas actualmente es obligatorio, debido a que su implementación ha pasado de ser un solo un mecanismo para mejorar los procesos, a convertirse en un conjunto de herramientas de primera necesidad para las empresas.

Para realizar una debida gestión de los recursos de TI se requiere del personal capacitado que se encargue de brindar la adecuada disponibilidad, continuidad y correcto funcionamiento del hardware, software, redes y telecomunicaciones que soportan los servicios de tecnología requeridos por las diferentes áreas de la empresa, sin embargo existen muchas empresas que no cuentan con un departamento de tecnología, por lo cual Solincosta ha centrado en identificar este tipo de empresas y ofrecerles sus servicios.

Esta propuesta está orientada al mejoramiento de la prestación del servicio que ofrece la empresa Soluciones Informáticas de la Costa (Solincosta) a sus empresas clientes, para ello se requiere contar con un modelo exclusivo de mejores prácticas de: Gestión de servicios de Tecnologías de la Información (TI), debido a que ofrece sus servicios bajo la modalidad de outsourcing. Para esto, tomamos marcos de referencia considerados como “buenas prácticas” y realizamos una articulación de estos; estos marcos son ISO/IEC 27002:2013, COBIT 2019 e ITIL 4.

2. PROBLEMA

2.1. Descripción

Actualmente la empresa SOLINCOSTA, se encuentra registrada como establecimiento de comercio y persona natural, esta misma por ser una empresa completamente nueva, sólo presta servicio de soporte de tecnologías de la información, en adelante soporte de TI, a dos empresas clientes: Cobuses SAS e Integrando talento humano SAS, la empresa SOLINCOSTA pretende incursionar nuevas empresas clientes, para ello quiere garantizar sus servicios bajo las mejores prácticas, tomando como insumo los marcos de referencias actuales que se puedan ajustar a su portafolio de servicios, para así realizar sus procesos de manera eficiente, actualmente su portafolio de servicios consta de:

- *Soporte de TI*
    - Mesa de ayuda a nivel de hardware o software: La empresa cliente se comunica vía llamada telefónica o WhatsApp para reportar alguna situación que requiera alguna intervención de soporte, el personal de soporte de la empresa SOLINCOSTA atiende el caso vía acceso remoto o presencial si es requerido, en este caso se agenda una visita según la disponibilidad del técnico, esta visita se realiza en el transcurso de día en el que fue reportado el caso, no se llevan registros de los casos soportados, ni las visitas realizadas.
    - Elaboración y ejecución de planes de mantenimiento a equipos de cómputo y/o periféricos: Se realiza una programación de mantenimiento semestral para CPUs e impresoras, se documenta la actividad realizada en la hoja de vida del equipo, custodiada en un gabinete que ha reservado la empresa cliente, destinado para guardar dicha documentación, de igual manera la empresa SOLINCOSTA inserta los registros de las actividades de mantenimiento en un archivo de Excel en línea.
    - Administración de hosting y dominio Cpanel: La empresa cliente adquiere un plan de hosting y dominio que brinda un panel de administración (Cpanel), este panel es administrado por la empresa SOLINCOSTA, bajo ese mismo panel se administra el sitio web de la empresa cliente.
- *Gestión de inventarios de activos de TI*
    - Control de inventario y registros de cambios de hardware: La empresa SOLINCOSTA realizó un formato que recopila la información de características, detalles y actividades de cambio de hardware o mantenimiento correctivo de cada activo de TI: (Computadores e impresoras), al igual que las hojas de vida son custodiadas en un gabinete ubicado en la empresa cliente, la empresa SOLINCOSTA en un documento de Excel en línea crea un libro por cada hoja de vida de un activo.
- *Seguridad de la Información*
    - Elaboración y ejecución de planes de Backups: Se realiza una programación de Backups para archivos en puestos de trabajo que se realiza mensual, a la base de datos

del sistema de información una vez por semana y a los correos electrónicos cada 15 días, esto se realiza de manera remota y se almacena la información en un dispositivo WD My Cloud de 2TB conectado a la Red LAN de la empresa cliente y almacenado físicamente en un rack de pared bajo llave.

- *Webmaster*
    - Construcción y administración del sitio web: Se realizan actividades de administración del sitio web: Publicación de contenido, y cambios en el sitio, los cuales son requeridos por el gerente o encargado de la empresa cliente, son solicitados vía llamada telefónica o WhatsApp, al realizar los cambios o publicaciones solicitadas son confirmadas por correo electrónico. No se llevan registros de los cambios o publicaciones realizadas.
- *Automatización de procesos*
    - Planificación y ejecución de soluciones tecnológicas que permitan la mejora de un proceso en específico, entre las cuales podemos implementar: Uso de una herramienta existente en el mercado o implementación de proyectos propios bajo tecnologías mixtas

3. Pregunta y preguntas secundarias

¿Cómo articular normas y marcos de referencia considerados como mejores prácticas para construir un marco de referencia propio y robusto orientado a la prestación de servicios de gestión de TI a clientes de la firma SOLINCOSTA?

La empresa SOLINCOSTA por ser una empresa nueva, con poca orientación para iniciar el proceso de gestión de TI a sus empresas clientes, expresa la necesidad de aprovechar las normas y marcos de referencia, reconocidas como mejores prácticas para crear un marco de referencia propio que le pueda servir como guía metodológica para la prestación de servicios de gestión de TI.

Inicialmente se deben estudiar los marcos de referencias y estándares aplicables al portafolio de servicios de la empresa Solincosta y luego de ello definir los procedimientos y sistemas de evaluación y control para la debida gestión de servicios de TI, de esa manera se realizará una articulación de estas normas y marcos de referencia para la construcción del nuevo marco de referencia a la medida de la empresa Solincosta.

4. OBJETIVOS

4.1. Objetivo General

Construir un modelo propio de prestación de servicios de gestión de tecnologías de la información para la mejora de la prestación de los servicios ofrecidos por Solincosta.

4.2. Objetivos Específicos

- ➢ Estudiar los marcos de referencias y estándares aplicables al portafolio de servicios de la empresa Solincosta.
- ➢ Establecer marcos de referencia y aspectos tratados que guarden relación con los servicios ofrecidos por Solincosta.
- ➢ Definir herramientas e indicadores a tener en cuenta para el mejoramiento continuo de los servicios ofrecidos.

5. MÉTODO

5.1. Determinación del método de análisis

Para SOLINCOSTA lo más importante es brindar un servicio de calidad, para ello no es suficiente contar con el recurso humano capacitado, también se debe contar con las herramientas necesarias para facilitar el proceso de gestión de TI a sus empresas clientes, lo cual le permitirá crecer gradualmente para obtener nuevas empresas clientes.

Contar con un modelo metodológico le permitirá a la empresa Solincosta apoyar a sus clientes en procesos de certificaciones, garantizar el buen uso de la información y aumentar la disponibilidad de recursos de TI con los que cuenta la empresa.

Nuestra propuesta se basa en utilizar tres marcos de referencia conocidos como “buenas prácticas”:

- ISO/IEC 27002:2013

  Esta norma contiene controles en seguridad de la información que vamos a tener en nuestro modelo.

- COBIT 2019

  COBIT nos ayudará a enmarcar los controles en los procesos catalizadores para buscar la alineación con los objetivos estratégicos.

- ITIL 4

  Del marco ITIL tomamos los principios básicos para la creación de nuestros servicios.

Revisión de otros autores

Para lograr un entendimiento de cómo articular varios modelos realizamos consultas de otros autores y revisamos sus formas de trabajar para dar lugar a la nuestra.

- La primera articulación revisada es la de Montaño, Combita, de la Hoz (2017), de esta se entiende que se debe buscar la relación entre los marcos seleccionados. El objetivo es satisfacer criterios de confidencialidad, disponibilidad e integridad de la información financiera que constituyen el objetivo fundamental de la Ley Sarbanes-Oxley. Para realizar la articulación arman una matriz donde en el eje de las X tienen un marco y en el eje de las Y, otro. Luego, de acuerdo, al objetivo de cada fila y columna se van realizando cruces donde el objetivo es similar, para poder determinar la similitud se necesita la experiencia del equipo de trabajo que está realizando la articulación. Por último se formulan los controles para cada una de las articulaciones, que para este caso son una serie de preguntas que deben tener en cuenta los auditores para garantizar la protección de los datos financieros.
- Otra revisión es la realizada al artículo de Montaño (2014) donde se articulan tres marcos conocidos, a nivel mundial, como “buenas prácticas”. Estos tres marcos son ISO 27000, COBIT e ITIL 3.0. Esta articulación trata de alinear dos mundos dentro de una compañía, el Plan Estratégico Corporativo (PEC) y el Plan Estratégico de Tecnología Informática (PETI). Este trabajo lo resumen en las siguientes fases:
  - Conocimiento de la organización
  - Selección de referentes conceptuales

- Construcción del instrumento de recolección de información
- Definición de métricas
- Establecimiento del avance del medio
- Definición del nivel deseado
- Aplicación del instrumento de recolección
- Establecimiento de la brecha entre el estado actual, el entorno y el estado deseado.

Estas fases las utilizamos como base para la creación de nuestro portafolio de Servicios de TI que prestaremos a nuestros clientes.

- La última revisión de otra articulación similar es la realizada por Montaño (2010) donde también se articula COBIT con ISO 27000. La propuesta está alineada con los trabajos revisados anteriormente y tomamos el concepto que desarrolla Montaño (2010) en sus trabajos para dar un enfoque objetivo a nuestro trabajo de creación del modelo para Solincosta.

En resumen, establecemos el punto de partida para determinar la metodología necesaria que requiere la construcción de nuestro marco de trabajo.

Solución para Solincosta

Nosotros tomamos como referencia el estándar ISO/IEC 27002:2013 para adoptar algunas prácticas en la gestión de seguridad de la información (ISO27002.ES, 2005) y los principios de la Biblioteca de Infraestructura de Tecnologías de Información ITIL (Mediagora, SL, 2012) para la gestión de servicios de tecnologías de la información, lo anterior sin detrimento de apropiar propuestas de otros marcos de referencia que se consideren pertinentes para robustecer el modelo planteado.

A continuación se mencionan las fases que se desarrollaron para la creación del modelo de gestión por servicios en la empresa Solincosta.

- Identificación de objetivos de control de la ISO/IEC 27002:2013 alineados con el portafolio de servicios
- Ubicación de objetivos de control en el marco de COBIT 2019
- Definición del portafolio de servicios de TI a gestionar en Solincosta

Identificación de objetivos de control de la ISO/IEC 27002:2013 alineados con el portafolio de servicios

Para cumplir con el objetivo trazado en el proyecto, el cual se basa en construir un modelo propio de prestación de servicios de gestión de tecnologías de la información, nos basamos en el alcance de las empresas clientes y el portafolio de servicios ofrecidos para así realizar una preselección de los controles publicados en la *en la norma ISO/IEC 27002:2013* que son aplicables en la construcción de nuestro modelo, la cual consta de *14 dominios, 35 objetivos de control y 114 controles.* De los 114 controles, fueron seleccionados 30.

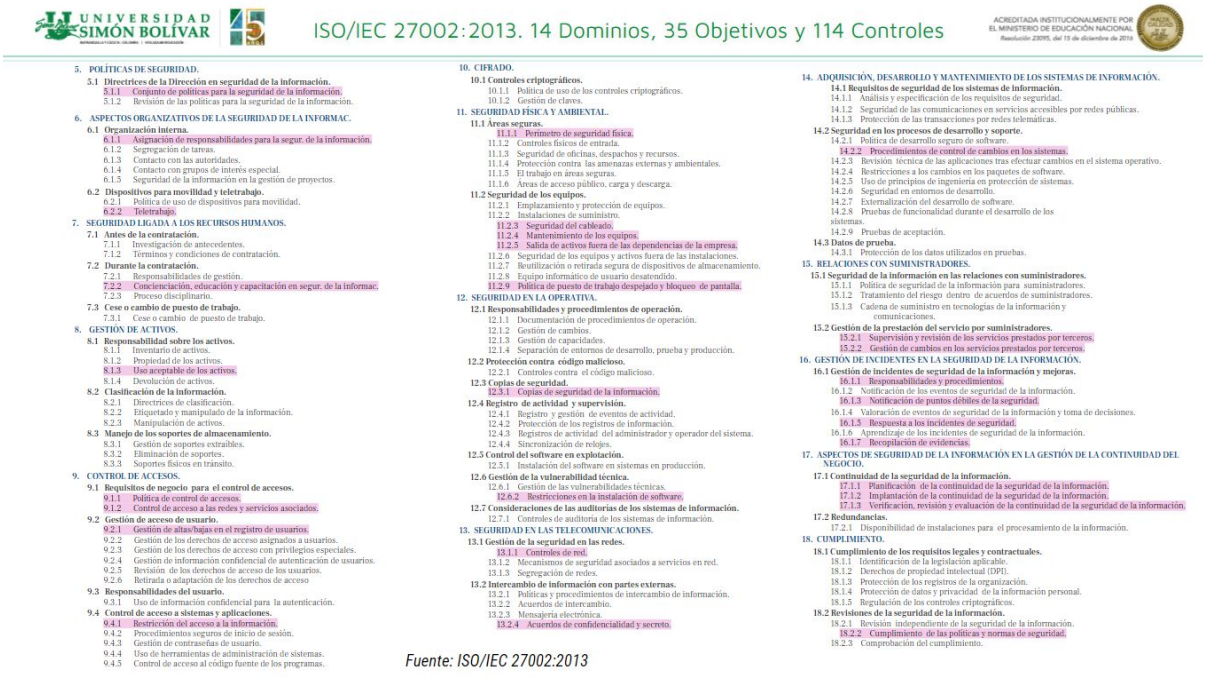

Imagen 1. *Dominios y Controles de ISO 27002:2013*

Ubicación de objetivos de control en el marco de COBIT 2019

Para agrupar los controles previamente seleccionados de la norma ISO/IEC 27002:2013, nos basamos en el modelo de referencia de procesos de COBIT 2019 para identificar cuales son los controles que apoyan a cada objetivo del modelo (ISACA, 2018).

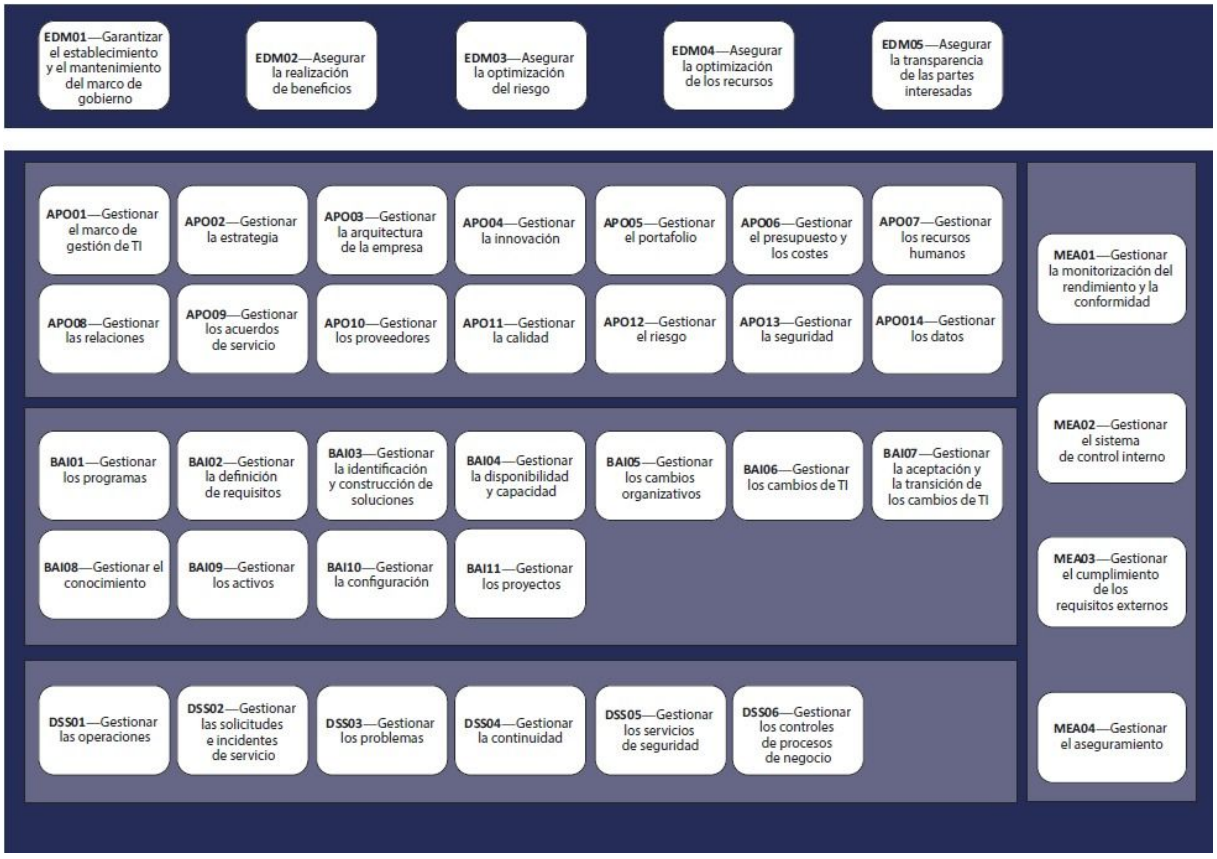

Imagen 2. *Dominios y procesos de Cobit 2019*

Integración

Objetivo de Gestión de COBIT 2019	Control de la norma ISO/IEC 27002:2013	Control Establecido
APO13 - Gestionar la Seguridad	Conjunto de políticas para la seguridad de la información	Crear un manual de seguridad de la información estandarizado para todas las empresas clientes, controlado por versiones y debidamente ilustrado para la fácil capacitación de los usuarios finales. Dentro del manual reservar una sección para establecer lineamientos particulares a los usuarios según la variabilidad que la empresa cliente pueda tener en materia de infraestructura, plataformas y alcance.
	Concienciación, educación y capacitación en seguridad de la información	Establecer un programa de capacitaciones y posteriormente evaluaciones aleatorias en la temática de seguridad de la información orientado al fortalecimiento de la cultura de seguridad de las TIC dentro de la organización.
	Política de Control de Accesos	Establecer el modelo del ciclo de vida del usuario dentro de dicho sistema durante su estancia permanente o temporal dentro de la organización
	Restricción del acceso a la información.	Determinar un manual de perfil de accesos en donde se categorice el usuario respecto al recurso a consultar o manipular
	Asignación de responsabilidades para la seguridad de la información.	Crear una matriz RACI para determinar roles y responsabilidades en función de todas las actividades encaminadas a la seguridad de la información
	Salida de activos fuera de las dependencias de la empresa.	Establecer el procedimiento para registrar todos los movimientos de activos al momento de salir o entrar a las instalaciones.
	Política de puesto de trabajo despejado y bloqueo de pantalla.	Establecer las configuraciones necesarias para contribuir al eficiente consumo de energía de equipos. Dichas configuraciones deben quedar registradas en el procedimiento de altas de puestos de trabajo

Tabla 1. Articulación APO013

Objetivo de Gestión de COBIT 2019	Control de la norma ISO/IEC 27002:2013	Control Establecido
DSS05 - Gestionar Servicios de Seguridad	Cumplimiento de las políticas y normas de seguridad.	Establecer las sanciones de acuerdo a su gravedad en conjunto al área de gestión humana, para su debido cumplimiento.
	Notificación de puntos débiles de la seguridad	Establecer rutinas de control de vulnerabilidades periódicamente

Tabla 2. Articulación DSS05

Objetivo de Gestión de COBIT 2019	Control de la norma ISO/IEC 27002:2013	Control Establecido
BAI04 - Gestionar la disponibilidad y la capacidad	Teletrabajo	Establecer los lineamientos necesarios para la creación y configuraciòn y mantenimiento del ambiente remoto, y establecer las rutinas de seguimiento para su enfatizar en su cumplimiento
	Uso aceptable de los activos.	Establecer los procesos de pre-compra basados en la edad del activo y designar responsabilidades de uso al usuario desde su primer contacto con un activo específico

Tabla 3. Articulación BAI04

Objetivo de Gestión de COBIT 2019	Control de la norma ISO/IEC 27002:2013	Control Establecido
APO12 - Gestionar el Riesgo	Seguridad del cableado	Definir los procesos que apunten a la efectiva instalación, mantenimiento y durabilidad del cableado, para la disminución del riesgo de intercepción, interferencia o posibles daños.
	Perímetro de seguridad física.	Establecer un checklist estandarizado a todas las empresas clientes de requisitos mínimos a cumplir para garantizar un determinado nivel de seguridad física. Crear una rutina de tareas de seguimiento.
	Controles de red	Establecer los debidos controles de segmentación para crear la barrera entre los recursos críticos y los recursos no críticos
	Restricciones en la instalación de software	Configurar un esquema de roles de usuarios administrados de manera local o por directorio activo para restringir las funciones de instalación a usuarios no autorizados.

Tabla 4. Articulación APO012

Objetivo de Gestión	Control de la norma	Control Establecido

de COBIT 2019	ISO/IEC 27002:2013	
APO14 - Gestionar los datos	Copias de seguridad de la información.	Crear un plan de Backups proyectado a un determinado periodo y establecer las tareas seguimiento para su debido cumplimiento.
	Mantenimiento de los equipos	Crear un plan de mantenimiento de equipos proyectado a un determinado periodo y establecer las tareas seguimiento para su debido cumplimiento.
	Respuesta a los incidentes de seguridad.	Establecer un plan de restauración estándar y crear las rutinas periodicidad de simulacros de restauraciòn de información para incrementar el nivel de madurez en recuperacion de incidentes
	Planificación de la continuidad de la seguridad de la información	Establecer un plan de acción para activar los servicios de contingencia que le puedan dar continuidad a los procesos, justificando el alcance y limitaciones correspondientes.
	Implantación de la continuidad de la seguridad de la información.	Establecer las normativas y realizar el seguimiento a la ejecución del plan de activación de servicios de contingencia para la continuidad del negocio
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Medir el resultado de la evaluación de la continuidad de la información estableciendo los márgenes de ganancias o pérdidas respecto a la continuidad de la seguridad de la información.

Tabla 5. Articulación APO014

Objetivo de Gestión de COBIT 2019	Control de la norma ISO/IEC 27002:2013	Control Establecido
APO08 - Gestión de las Relaciones	Acuerdos de confidencialidad y secreto	Establecer lineamientos para el control de procesos realizados por terceros estableciendo también acuerdos de confidencialidad en el caso de requerirse.

Tabla 6. Articulación APO08

Objetivo de Gestión de COBIT 2019	Control de la norma ISO/IEC 27002:2013	Control Establecido
BAI06 - Gestionar los cambios de TI	Procedimientos de control de cambios en los sistemas.	Documentar los cambios realizados para crear una base de conocimientos que nos permitirá reaccionar oportunamente ante una situación generada por cambios realizados

Tabla 7. Articulación BAI06

Objetivo de Gestión de COBIT 2019	Control de la norma ISO/IEC 27002:2013	Control Establecido
APO10 - Gestionar los proveedores	Supervisión y revisión de los servicios prestados por terceros	Establecer métricas de cumplimiento a los servicios prestados por proveedores y realizar el respectivo análisis de cumplimiento de indicadores para la toma de decisiones

Tabla 8. Articulación APO10

Objetivo de Gestión de COBIT 2019	Control de la norma ISO/IEC 27002:2013	Control Establecido
APO01 - Gestionar el marco de gestión de TI	Responsabilidades y procedimientos.	Realizar el debido seguimiento al cumplimiento de las buenas prácticas establecidas en el marco de gestión propio de Solincosta

Tabla 9. Articulación APO01

Objetivo de Gestión de COBIT 2019	Control de la norma ISO/IEC 27002:2013	Control Establecido
APO04 - Gestión de la innovación	Gestión de cambios.	Establecer un portafolio de proyectos que tengan como objetivo transformar los procesos manuales o ineficientes del negocio por procesos automatizados y eficientes adoptando el uso de las tecnologías de la información

Tabla 10. Articulación APO04

Objetivo de Gestión de COBIT 2019	Control de la norma ISO/IEC 27002:2013	Control Establecido
BAI08 - Gestión del conocimiento	Recopilación de evidencias.	Tener control total de las evidencias necesarias para los indicadores de controles de todos los servicios creados para el modelo de gestión. Establecer una base de conocimientos donde se registren los procedimientos, políticas y normas con sus respectivos historiales de cambios.

Tabla 11. Articulación BAI08

Definición del portafolio de servicios de TI a gestionar en Solincosta

A continuación listamos los servicios que la empresa Solincosta va a gestionar para dar soporte a las operaciones de sus clientes.

Para cada servicio definimos los siguientes aspectos:

- **Código**: establecemos una numeración en el orden de creación de los servicios antecedidos por la letra S (servicio).
- **Nombre**: Nombre del servicio.
- **Objetivos de COBIT 2019**: Objetivos seleccionados de COBIT 2019
- **Controles de ISO/IEC 27002:2013**: Controles seleccionados de ISO/IEC 27002:2013
- **Descripción**: Resumen del servicio
- **Objetivo**: Meta a cumplir con la prestación del servicio.
- **Indicadores de Control**: Medición que se realizará al servicio para dar cumplimiento del objetivo.
- **Herramientas**: Herramientas necesarias para la gestión del servicio.
- **Mapa de Proceso**: Establece el orden en el que se cumple las actividades.
- **Actores y Responsabilidades**: Matriz RACI de los objetivos de control seleccionados.

S01	**Servicio de cultura de seguridad**			
Objetivo de COBIT 2019	APO13. Gestionar la Seguridad			
Controles de ISO/IEC 27002:2013				
1	Conjunto de políticas para la seguridad de la información			
2	Concienciación, educación y capacitación en seguridad de la información			
3	Política de Control de Accesos			
4	Asignación de responsabilidades para la seguridad de la información.			
5	Restricción del acceso a la información.			
6	Restricción en la instalación de software			
7	Política de puesto de trabajo despejado y bloqueo de pantalla.			
8	Perímetro de seguridad física.			
Descripción			**Objetivo**	
Define la cultura de seguridad dentro de Solincosta para apropiar en los procesos de Outsourcing hacia los clientes y demás interesados.			Incluir los controles y restricciones de seguridad en las labores diarias de Solincosta, sus clientes y proveedores.	
Indicadores de Control				
	Nombre	**Valores de referencia**	**Resultado Esperado**	**Fórmula/Indicador**
1	Formación y capacitación	Capacitaciones Realizadas (CR) Capacitaciones Planificadas(CP)	100%	(CR / CP) * 100
2	Política de Seguridad de la Información	Documento Creado	SI	¿Documento creado?

3	Matriz de Responsabilidades	Matriz Establecida	SI	¿Matriz establecida?
4	Software y Restricciones	Controles Aplicados(CA) Controles Sugeridos (CS)	100%	(CA / CS) * 100

Herramientas		
1	Política de Seguridad de la Información	Es un documento donde se plasman todas las políticas y normas de seguridad que deben cumplir los empleados y terceros asociados en los procesos de outsourcing de TI. Será definido por Solincosta y para cumplimiento en todas sus operaciones. Cada cliente o proveedor deberá cumplir las políticas establecidas y se tomarán las acciones allí descritas en caso de incumplimiento por alguna de las partes.
2	Material de formación y capacitación	Solincosta contará con material de formación y capacitación para sus empleados. Este material está compuesto por videos, manuales y evaluaciones. Las evaluaciones deberán ser aprobadas por los empleados de solincosta, de esta forma se garantiza que se apropie el conocimiento y pueda ser aplicado en las operaciones con clientes y proveedores.
3	Matriz de responsabilidades	El personal de Solincosta tendrá responsabilidades que deberán tener en cuenta para dar cumplimiento al objetivo del servicio. Esta matriz está en el mismo servicio. Ver abajo
4	Restricciones y Software	En cada estación de trabajo se deben aplicar restricciones e instalar las herramientas de software necesarias para asegurar que la información de la compañía no se vea comprometida. Cada usuario tendrá un perfil, y de acuerdo a este se aplicarán más o menos reglas y herramientas de software. Otro conjunto de herramientas serán las necesarias para disminuir el uso de energía de cada estación de trabajo. Los salvapantallas automáticos también hacen parte de esta solución. Debe existir, dentro de las Políticas de Seguridad de la Información, un punto sobre no dejar la pantalla desbloqueada a levantarse del puesto de trabajo.
5	Actas de formación	Es un formato que captura la información de los participantes, temas de formación y cronograma de actividades a cumplir.

Mapa de Procesos

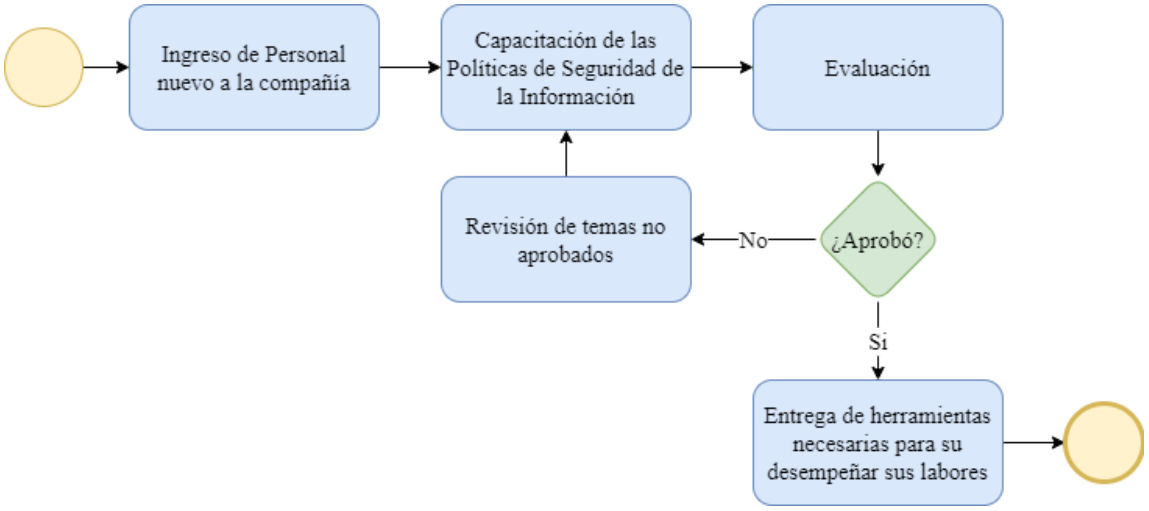

Diagrama 1. *Mapa de procesos de capacitación en Políticas de Seguridad de la Información*

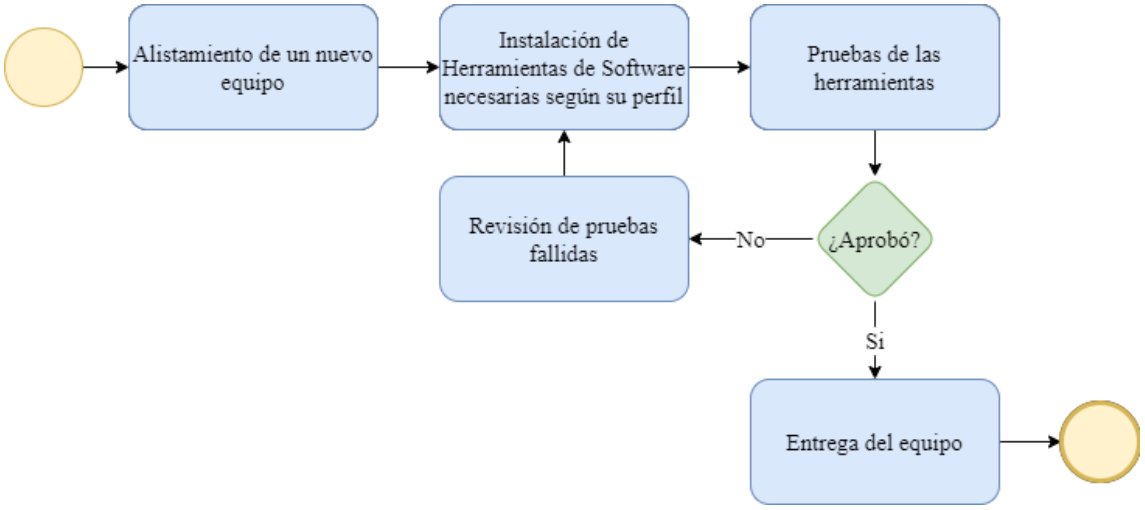

Diagrama 2. *Mapa de proceso de Instalación de herramientas de seguridad en los equipos de computo*

Actores y Responsables

Matriz de responsabilidades del servicio S01				
Objetivo de Control	**Coordinación de Operaciones**	**Director de Tecnologías**	**Coordinación de Soporte**	**Dirección de Servicios**
Conjunto de políticas para la seguridad de la información	C	A	R	
Concienciación, educación y capacitación en seguridad de la información		A		R
Política de Control de Accesos		A	R	
Asignación de responsabilidades para la seguridad de la información.		R		
Restricción del acceso a la información.	C	A	R	
Política de puesto de trabajo despejado y bloqueo de pantalla.		A	R	

Tabla 11. Servicio de cultura de seguridad

S02	**Servicio de conexiones externas**	
Objetivo de COBIT 2019	APO13. Gestionar la Seguridad BAI04. Gestionar la disponibilidad y la capacidad APO08. Gestión de las Relaciones	
Controles de ISO/IEC 27002:2013		
1	Salida de activos fuera de las dependencias de la empresa.	
2	Teletrabajo	
3	Acuerdos de confidencialidad y secreto	
Descripción		**Objetivo**
Establece el control sobre las conexiones externas hacia		Garantizar la seguridad de la información de cada

las redes y recursos de cada compañía desde sus clientes, proveedores y/o empleados. Minimiza el riesgo de fuga de información a terceros no involucrados en los distintos procesos llevados a cabo en las empresas.	compañía que requiera tener conexiones externas con sus clientes, proveedores y/o empleados.

Indicadores de Control

	Nombre	Valores de referencia	Resultado Esperado	Fórmula/Indicador
1	Buen uso de equipos con acceso remoto	Salidas de equipos (SE) Controles Aplicados (CA) Eventos de mal uso (EMU)	0%	[EMU / (SE * CA)] * 100
2	Acuerdos de confidencialidad	Acuerdos Firmados (AF) Acuerdos Respetados (AR)	100%	(AR / AF) * 100

Herramientas

1	Bitácora de salida y entrada de equipos	Registro de entradas y salidas de los equipos de la compañía donde se especifica el uso que se le dará al equipo mientras esté fuera de las instalaciones de la empresa, es necesario indicar el nombre y cargo de la persona que se hace responsable.
2	Acceso remoto	Se proporcionarán las herramientas necesarias para el acceso remoto a las redes internas de las empresas, garantizando la disminución del riesgo de las vulnerabilidades. Cada usuario deberá cumplir con las normas establecidas en las Políticas de Seguridad de la Información con respecto al acceso remoto.
3	Formatos de acuerdos de confidencialidad	Formatos en blanco de acuerdos de confidencialidad donde se describa el uso que se le dará a la información entregada por parte de la empresa a los clientes, proveedores, empleados o cualquier otro tercero que necesite acceso a esta. Estos acuerdos de confidencialidad deben estar alineados con la legislación para el tratamiento de datos. En estos acuerdos, se tendrá un espacio para las medidas que se tomarán en caso de incumplirlos.
4	Formato de control de salida y entrega de activos	Formato que especifica el tipo de control del activo (Salida/Entrada, entrega/recibido) con la respectiva relación de los activos y las fechas determinadas para la labor encomendada.

Mapa de Procesos

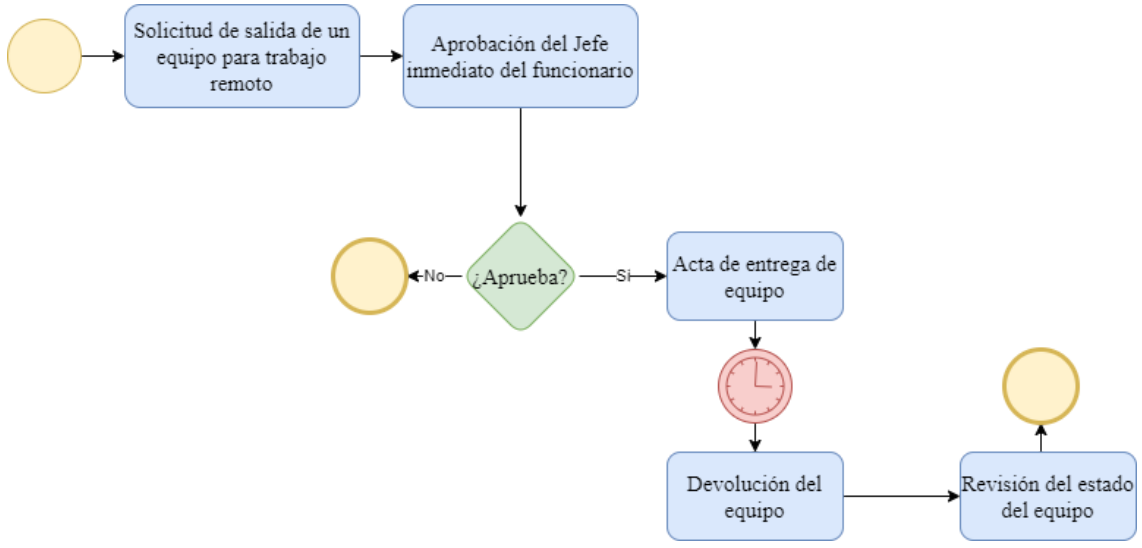

Diagrama 3. *Mapa de procesos de salida de un equipo de la compañía*

Actores y Responsables

Matriz de responsabilidades del servicio S02				
Objetivo de Control	Coordinación de Operaciones	Director de Tecnologías	Coordinación de Soporte	Dirección de Servicios
Bitácora de salida y entrada de equipos	I		R	
Acceso Remoto	R	C		
Formatos de Acuerdos de confidencialidad		R		

Tabla 12. Servicio de conexiones externas

S03	**Servicio de verificación y cumplimiento**			
Objetivo de COBIT 2019	DSS05. Gestionar Servicios de Seguridad APO01. Gestionar el marco de gestión de TI APO10. Gestionar los proveedores			
Controles de ISO/IEC 27002:2013				
1	Cumplimiento de las políticas y normas de seguridad.			
2	Notificación de puntos débiles de la seguridad			
3	Responsabilidades y procedimientos.			
4	Supervisión y revisión de los servicios prestados por terceros			
Descripción		**Objetivo**		
Define la forma en que se realizará el monitoreo de la normativa vigente en la compañía.		Hacer cumplir las normas establecidas en las Políticas de Seguridad de la Información.		
Indicadores de Control				
	Nombre	**Valores de referencia**	**Resultado Esperado**	**Fórmula/Indicador**
1	Cumplimiento de Auditorias	Auditorias Planificadas (AP) Auditorias Ejecutadas (AE)	100%	(AE / AP) * 100
2	Riesgos encontrados	Cantidad de hallazgos (CH)	0	CH
3	Manuales de funciones	Manuales de funciones establecidos (MFE)	SI	¿Manuales Establecidos?
4	Evaluación de proveedores	Fallas reportada (FR) Fallas solucionadas (FS) Tiempo de tolerancia (TT) Tiempo de respuesta (TR)	TR > TT	
Herramientas				
1	Plan de Auditorias	Plan de Auditoría y revisión de los procesos plasmados en los Documento de estandarización del proceso (S06). Estas auditorías dan lugar a planes de mejora a los procesos revisados.		
2	Métricas de Cumplimiento	Documentos por cada cliente donde se establecen los mínimos a cumplir por las partes interesadas para satisfacer sus necesidades. Estas métricas son las que se tienen en cuenta en los planes de auditoría, y de acuerdo a los resultados obtenidos se establecerán los controles y mejoras futuras.		
3	Manuales de funciones	Para realizar las auditorías es necesario tener los manuales de funciones de cada funcionario de la compañía. Estos documentos son entregados a los empleados al momento del ingreso e inducción del cargo.		
4	Acta de Auditoría Realizada	Documento donde quedará registro de las auditorías realizadas. En este se detalla la actividad realizada para la captura de información y sus evidencias. También se acompaña de los hallazgos para la mejora de los procesos y los compromisos adquiridos.		
Mapa de Procesos				

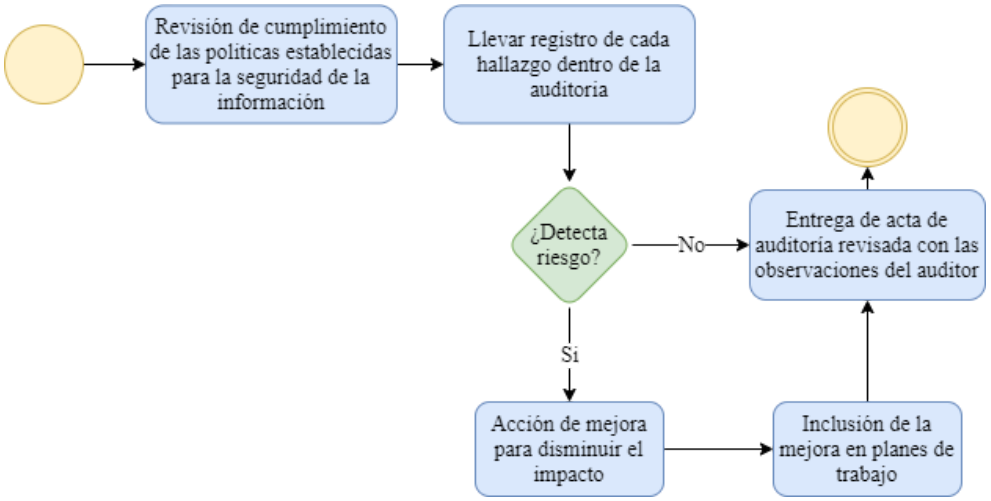

Diagrama 4. *Mapa de procesos de las Auditorías del cumplimiento de las PSI*

Actores y Responsables

Matriz de responsabilidades del servicio S03				
Objetivo de Control	Coordinación de Operaciones	Director de Tecnologías	Coordinación de Soporte	Dirección de Servicios
Plan de Auditorias	I	I	I	R
Métricas de Cumplimiento		I		R
Manuales de Funciones	C	R	C	C

Tabla 13. Servicio de verificación y cumplimiento

S04	**Servicio de preservación de la infraestructura**
Objetivo de COBIT 2019	BAI09. Gestión de Activos SS04. Gestión de la continuidad APO12. Gestionar el Riesgo

Controles de ISO/IEC 27002:2013	
1	Uso aceptable de los activos.
2	Mantenimiento de los equipos
3	Seguridad del cableado
4	Controles de Red

Descripción	**Objetivos**
Define la forma en que deberán ser tratados los activos de la empresa utilizados para tecnología.	Garantizar el buen uso de los activos de tecnología.

Indicadores de Control

	Nombre	**Valores de referencia**	**Resultado Esperado**	**Fórmula/Indicador**
1	Mantenimientos Preventivos	Mttos Planificados (MP) Mttos Ejecutados (ME)	100%	(ME / MP) * 100
2	Manuales de uso de equipos	Manuales creados y establecidos (MCE)	SI	¿Manuales creados y establecidos?
3	Compromisos no cumplidos	Compromisos incumplidos (CI) Compromisos establecidos (CE)	0%	(CI / CE) * 100
4	Normas para el cableado	Normativa establecida	SI	¿Normativa Creada y establecida?

Herramientas

1	Cronograma de mantenimiento preventivo	Plan de mantenimiento de los equipos de cómputo para garantizar el buen estado físico y lógico de los mismos. Este cronograma lo acompaña un instructivo donde se explica cómo se debe realizar el mantenimiento dependiendo el tipo de equipo y su exposición a vulnerabilidades, también se define la periodicidad con que son realizados. Las acciones de mejora, deberán estar soportadas por el técnico encargado y justificadas a los responsables del proceso.
2	Manuales de uso de los equipos de computo	Manuales donde se especifica la forma en que deberán ser tratados los equipos de cómputo para evitar el uso de los recursos de la compañía para fines personales. Estos manuales deberán estar basados en las Políticas de Seguridad de la Información. También se definirán las acciones que se podrían tomar en caso de no ser cumplidas las normas determinadas.
3	Actas de compromiso para el buen uso de los equipos	Cada empleado deberá firmar un acta de compromiso donde se hace responsable por el uso que le dará al equipo y se compromete a cumplir lo determinado en el acuerdo.
4	Normativa para la instalación del cableado de red	Para la instalación del cableado, se deben cumplir normas de seguridad física y lógica. Se especifica el tipo de material a utilizar, las normas a cumplir, en lo posible se debe certificar con una empresa. Si la empresa que contrata los servicios de Outsourcing con Solincosta ya tiene un cableado, se revisará que cumpla con las normas establecidas y se dará lugar a modificaciones si es necesario.
5	Acta de Mantenimiento Realizado	Acta donde se detallan las actividades realizadas durante el mantenimiento de los equipos de computo. El responsable del activo deberá recibir a satisfacción el equipo funcionando y en buen estado. Cualquier novedad del equipo, debe quedar registrada en esta acta. Datos importantes como fecha, hora y duración del mantenimiento deberán ser diligenciados también. Importante indicar el tipo de mantenimiento: preventivo o correctivo.

Mapa de Procesos

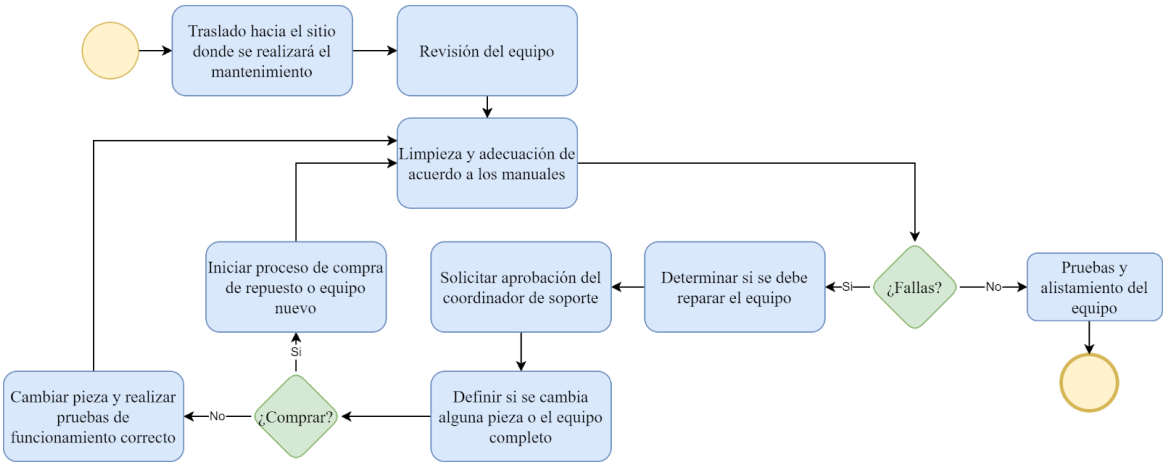

Diagrama 5. *Mapa de procesos de Ejecución del cronograma de mantenimiento*

Actores y Responsables

Matriz de responsabilidades del servicio S04

Objetivo de Control	Coordinación de Operaciones	Director de Tecnologías	Coordinación de Soporte	Dirección de Servicios
Cronograma de Mantenimiento Preventivo		I	R	C
Manuales de uso de los equipos de computo		R	C	
Actas de compromiso para el buen uso de los equipos		C	R	
Normativa para la instalación del cableado de red	I	R	I	I

Tabla 14. Servicio de preservación de la infraestructura

S05	**Servicio de monitoreo y resguardo de las redes**
Objetivo de COBIT 2019	APO12. Gestionar el Riesgo
Controles de ISO/IEC 27002:2013	
1	Control de acceso a las redes y servicios asociados.
2	Controles de red

Descripción	**Objetivo**
Establece las barreras necesarias que delimitan el uso de la infraestructura crítica y la no crítica	Limitar el uso de la infraestructura crítica para garantizar que no sea utilizada para realizar tareas que generan alto índice de vulnerabilidad, desaprovechamiento o mala utilización de la infraestructura crítica.

Indicadores de Control				
	Nombre	**Valores de referencia**	**Resultado Esperado**	**Fórmula/Indicador**
1	Política de control de acceso	Política de control de acceso establecida	SI	¿Política establecida?
2	Política de uso de canales	Política de uso de canales establecida	SI	¿Política establecida?
3	Eficiencia de la red	Uso de la red por usuario (URU) Uso recomendado por cada usuario (URR)	<=100%	(URU / URR) * 100

Herramientas		
1	Políticas de control de acceso	Documento que contiene las delimitaciones por roles y accesos a los recursos a nivel de: Segmentación, controles y uso de la red.
2	Políticas de separación y uso de canales alternos	Documento que contiene la planificación y gestión para el uso corporativo y ocasional de las redes, estableciendo políticas totalmente personalizadas dependiendo de la criticidad de la red.
3	Monitoreo de eficiencia	Rutina de monitoreo periódica que permite evaluar el consumo real por usuario o dependencia comparado con el consumo recomendado para establecer nuevos controles o revocar los innecesarios
4	Acta de monitoreo	Documento donde se registrará la evidencia de los monitores de eficiencia realizados a la(s) red(es). Cualquier novedad en el uso de la red, deberá estar soportada. Las acciones tomadas también quedarán en estas actas. Datos importantes como fecha, hora y duración de la prueba serán registrados también.

Mapa de Procesos

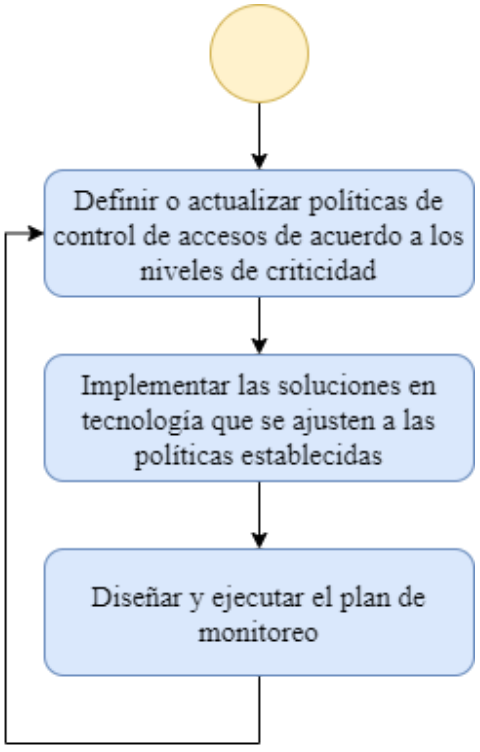

Diagrama 6. *Mapa de procesos de controles de red*

Actores y Responsables

Matriz de responsabilidades del servicio S05				
Objetivo de Control	**Coordinación de Operaciones**	**Director de Tecnologías**	**Coordinación de Soporte**	**Dirección de Servicios**
Definición de politicas de control de accesos	I	R		I
Definición de politicas de control de accesos	I	R	I	I
Creación de plan de monitoreo	R	A	I	I
Cumplimiento del plan de monitoreo		I	R	
Toma de decisiones	I	R	I	I

S06	**Servicio de Gestión de la Innovación**			
Objetivo de COBIT 2019		**APO04**. Gestión de la innovación **BAI06**. Gestionar los cambios de TI		
Controles de ISO/IEC 27002:2013				
1	Gestión del cambio			
2	Procedimientos de control de cambios en los sistemas.			
Descripción			**Objetivo**	
Define los procedimientos necesarios para transformar positivamente en materia de recursividad, tiempo y economía los procesos bases de funcionamiento del negocio			Transformar los procesos manuales o ineficientes del negocio por procesos automatizados y eficientes adoptando el uso de las tecnologías de la información	
Indicadores de Control				
	Nombre	**Valores de referencia**	**Resultado Esperado**	**Fórmula/Indicador**
1	Documento de estandarización de procesos	Documento creado y actualizado	SI	¿Documento actualizado?
2	Hoja de vida del proyecto	Proyectos Ejecutados con éxito (PE) Proyectos planificados (PP)	100%	(PE / PP) * 100
Herramientas				
1	Documento de estandarización del proceso	Documento que contiene de manera formal todo el procedimiento establecido por la empresa para el cumplimiento de actividades correspondientes a un proceso en específico.		
2	Hoja de vida del proyecto	Documento que contiene la planificación: (alcance, presupuesto, partes interesadas tiempos, objetivos y hoja de ruta) para la gestión de nuevas tecnologías que permitan el desarrollo de las actividades de los procesos a mejorar de manera más eficiente		
3	Actas de entrega para proyectos	Durante la ejecución de un proyecto se necesita realizar entregas parciales o totales a los interesados del proyecto, estas entregas deben estar soportadas en actas formales donde quedará el registro de las pruebas realizadas y los criterios de aceptación evaluados. Compromisos generados durante la entrega, serán registrados en el acta.		
Mapa de Procesos				

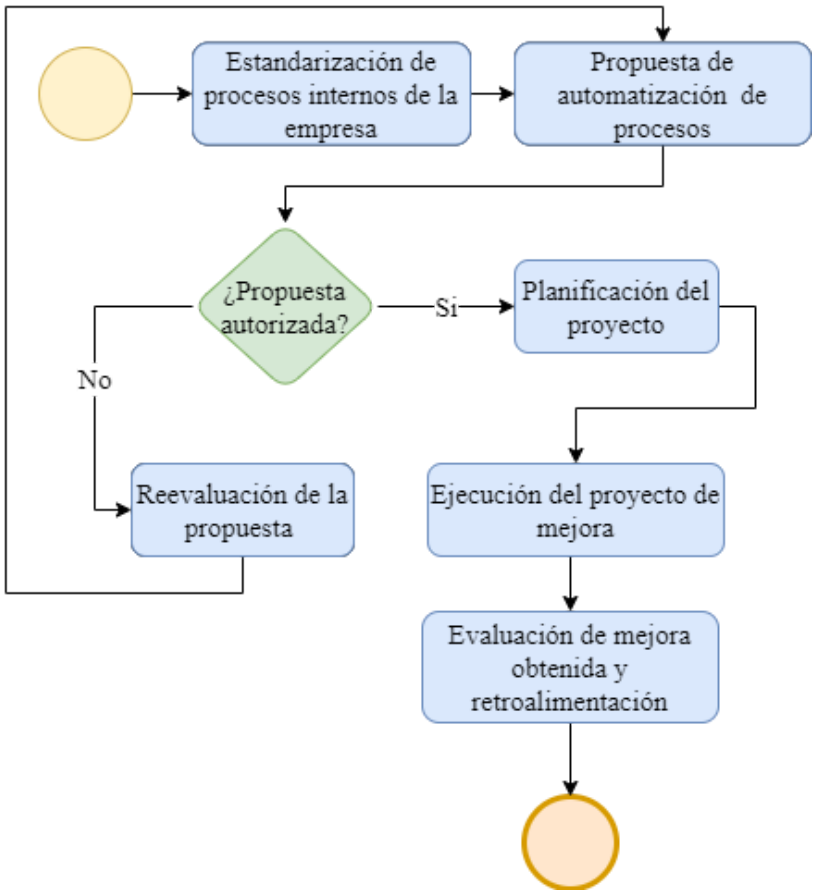

Diagrama 7. *Mapa de mejora de procesos*

Actores y Responsables

Matriz de responsabilidades del servicio S06				
Objetivo de Control	**Coordinación de Operaciones**	**Director de Tecnologías**	**Coordinación de Soporte**	**Dirección de Servicios**
Estandarización y documentación de procesos internos	R	I		I
Analisis de oportunidades de mejoras del proceso	R	C		I
Planificación y gestión del proyecto	C	R	I	I

Tabla 15. Servicio de Gestión de la Innovación

S07	**Servicio de Continuidad de Negocio**
Objetivo de COBIT 2019	APO14 - Gestionar los datos DSS04 - Gestión de la continuidad BAI08 - Gestión del conocimiento

Controles de ISO/IEC 27002:2013	
1	Copias de seguridad de la información.
2	Respuesta a los incidentes de seguridad.
3	Planificación de la continuidad de la seguridad de la información
4	Implantación de la continuidad de la seguridad de la información.
5	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
6	Recopilación de evidencias.

Descripción	**Objetivo**
Define los mecanismos necesarios para evitar la interrupción del negocio, actividades que activan los planes de contingencia para poner en marcha la estrategia de respuesta a los incidentes que pueden llegar a generar pérdidas.	Minimizar el margen de pérdida de información y pérdida de tiempo en el proceso de restauración o reactivación de la operación en caso de fallas y, en lo posible, sin dependencia del recurso humano de la compañía.

Indicadores de Control

	Nombre	**Valores de referencia**	**Resultado Esperado**	**Fórmula/Indicador**
1	Copias de seguridad	Copias Planificadas (CP) Copias Ejecutadas (CE)	100%	(CE / CP) * 100
2	Plan de restauración	Plan de restauración establecido	SI	¿Plan establecido?
3	Restauraciones Satisfactorias	Restauraciones Ejecutadas (RE) Restauraciones Satisfactorias (RS)	100%	(RS / RE) * 100
4	Servicios de contingencia	Servicios de contingencia establecidos	SI	¿Servicios establecidos?
5	Repositorio de Información	Repositorio de información creado	SI	¿Existe el repositorio de información?

Herramientas		
1	Plan de Copias de Seguridad	Documentación de la planificación elaborada para cada recurso lógico que se requiera salvaguardar, definiendo la periodicidad en la que se requiere realizar la actividad descrita en el plan.
2	Plan de Restauración	Documentación de la planificación elaborada para ejecutar las actividades de restauraciones de los backups realizados, sirve cómo filtro de errores de comprobación para verificar que la tarea se haya realizado satisfactoriamente.
3	Servicios de contingencia	Listado de todos los servicios de contingencia definidos por objetivos y plan de acción, para su oportuna ejecución en caso de requerirse
4	Métricas para el margen de tolerancia	Documento de acuerdos de niveles de servicio que especifica las métricas para tener una margen de tolerancia considerable para afectaciones del servicio
5	Repositorio de Información	Debe existir un repositorio con toda la información del área de TI de la compañía. El objetivo de este repositorio es eliminar la dependencia hacia las personas encargadas de realizar los procesos, lo ideal es que la dependencia se genere hacia la documentación; cualquier cambio en el recurso humano deberá ser transparente para la compañía buscando cumplir el objetivo del servicio: garantizar la continuidad del negocio. Todo el material archivado en el repositorio debe estar organizado y publicado (a quienes interese) de tal manera que sea fácil encontrar para su lectura y posterior modificación. Las

		evidencias y acta de todos los servicios deben estar archivados también. Otros documentos como: políticas de seguridad, normativas, información de referencia, mapas de proceso, matrices de responsabilidades deberán estar consignadas en el repositorio de información.

Mapa de Procesos

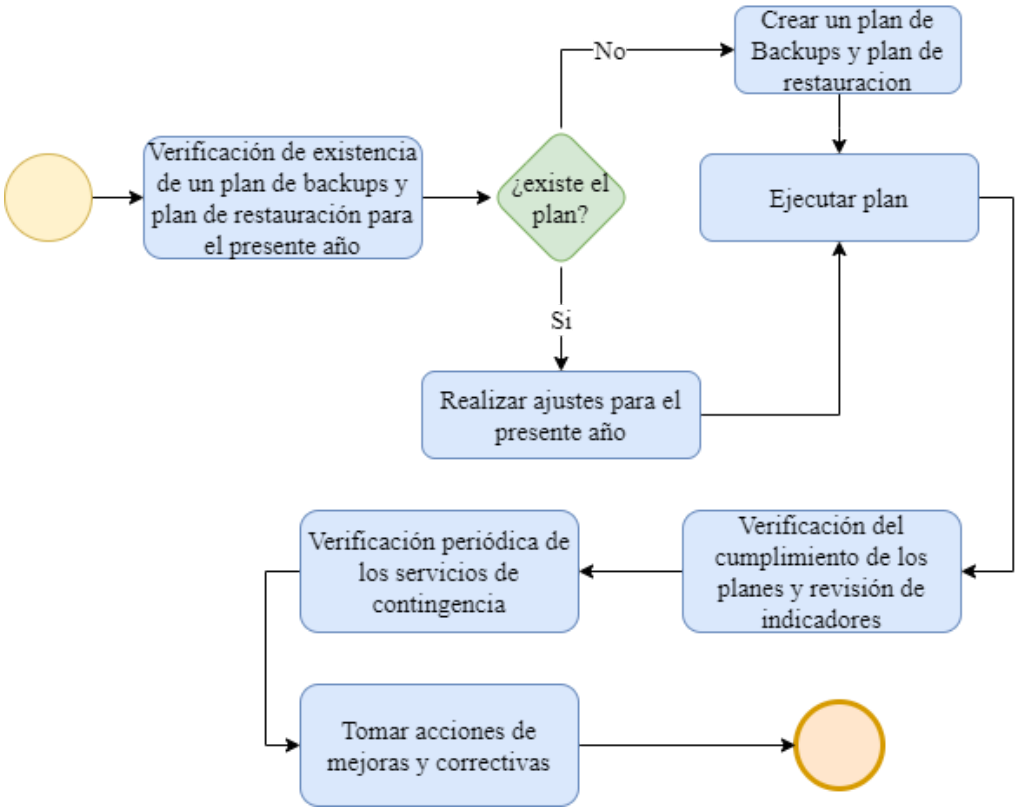

Diagrama 8. *Mapa de procesos de control y ejecucion d planes de backups y restauracion*

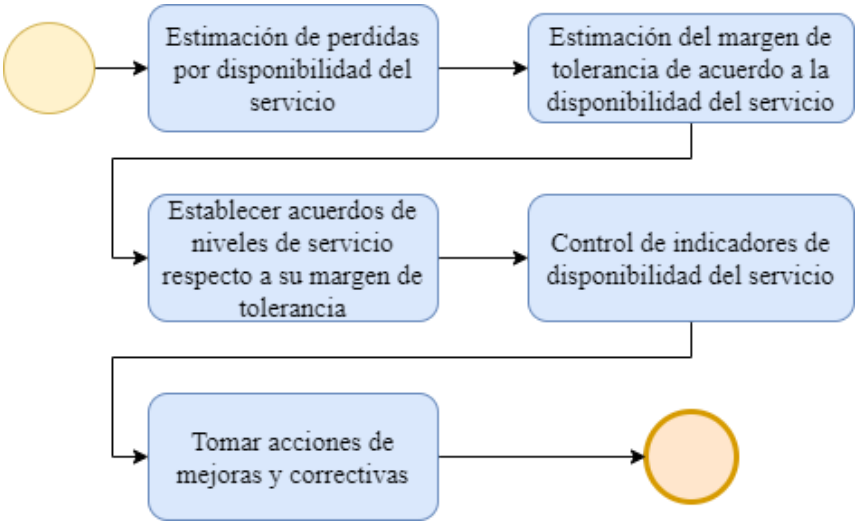

Diagrama 9. *Mapa de proceso de niveles de servicio*

Actores y Responsables

Matriz de responsabilidades del servicio S07				
Objetivo de Control	**Coordinación de Operaciones**	**Director de Tecnologías**	**Coordinación de Soporte**	**Dirección de Servicios**
Creación y actualización del plan de Backups	I	A	R	I
Creación y actualización del plan de restauración	I	A	R	I
Ejecución del plan de Backups		I	R	
Ejecución del plan de Restauración		I	R	
Verificación de cumplimiento de planes		R	C	
Revisión periodica de los servicios de contingencia			R	
Acciones correctivas y de mejora continua	I	R	I	I

Tabla 16. Servicio de Continuidad de Negocio

6. RESULTADOS Y DATOS OBTENIDOS

Como resultado del análisis de la operación de Solincosta y los marcos de trabajo utilizados como referencia damos lugar a un Marco de Trabajo personalizado para la empresa Solincosta; este marco de trabajo dió lugar, a su vez, a la creación de siete Servicios de TI enfocados a la gestión de proveedores, clientes, empleados de la compañía y seguridad de la información.

Teniendo en cuenta que nuestro primer marco de referencia es ISO/IEC 27002:2013, el enfoque principal del nuevo marco de trabajo es la seguridad de la información, siendo la información el activo más valioso para nuestros clientes. Desde ese enfoque se establecieron los controles y estrategias guiadas por los Objetivos de Gestión de COBIT 2019.

Para iniciar con la implementación del Marco de Trabajo de Solincosta basado en Servicios de TI, fue necesario realizar una medición de cada uno de estos teniendo en cuenta los niveles de madurez de CMMI (White, 2018).

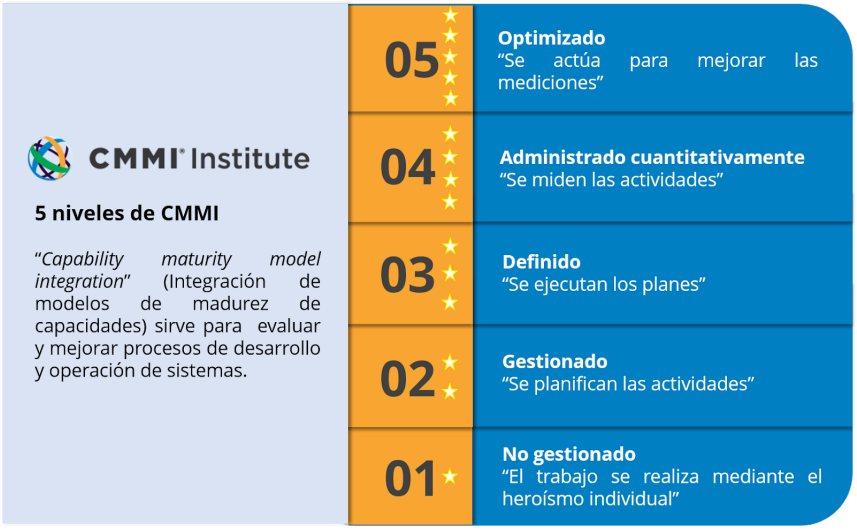

Imagen 3. *Niveles de madurez CMMI*

A continuación se listan los Servicios de TI que deben ofrecerse en Solincosta para dar soporte a sus operaciones sin poner en riesgo a las partes interesadas (clientes, proveedores).

ID	Nombre	Objetivo	Indicadores de Control	Nivel CMMI
S01	Servicio de cultura de seguridad	Incluir los controles y restricciones de seguridad en las labores diarias de Solincosta, sus clientes y proveedores.	4	Nivel 1
S02	Servicio de conexiones externas	Garantizar la seguridad de la información de cada compañía que requiera tener conexiones externas con sus clientes, proveedores y/o empleados.	2	Nivel 1
S03	Servicio de verificación y cumplimiento	Hacer cumplir las normas establecidas en las Políticas de Seguridad de la Información.	3	Nivel 1
S04	Servicio de preservación de la infraestructura	Garantizar el buen uso de los activos de tecnología.	4	Nivel 1
S05	Servicio de monitoreo y resguardo de las redes	Limitar el uso de la infraestructura crítica para garantizar que no sea utilizada para realizar tareas que generan alto índice de vulnerabilidad, desaprovechamiento o mala utilización de la infraestructura crítica.	3	Nivel 1
S06	Servicio de Gestión de la Innovación	Transformar los procesos manuales o ineficientes del negocio por procesos automatizados y eficientes adoptando el uso de las tecnologías de la información	2	Nivel 1
S07	Servicio de Continuidad de Negocio	Minimizar el margen de pérdida de información y pérdida de tiempo en el proceso de restauración o reactivación de la operación	4	Nivel 1
		Cantidad de Indicadores de Control	**22**	

Tabla 17. Relación de servicios con niveles de madurez

Se establece el nivel de madurez de todos los servicios porque actualmente no se encuentran documentos los procesos. Y tal como lo indica el nivel 1 de CMMI "*...Los procesos son nuevos y, a menudo, no están documentados, y las empresas no pueden repetir los procesos de manera confiable*" sucede en Solincosta. Es por esta misma razón que se toma la decisión de ejecutar este proyecto.

7. CONCLUSIONES

7.1. Conclusiones

Como resultado de este proyecto se obtiene el esquema de servicios de TI que deben ser gestionados por Solincosta para dar soporte a sus operaciones con clientes y proveedores. También pudimos determinar el nivel de madurez, basados en CMMI, que tiene actualmente Solincosta.

Para realizar esta articulación de los marcos de referencia fue necesario haber desarrollado todos los módulos del programa de Gestión de TI. Gracias al conocimiento aprendido y la experiencia que tenemos coordinando departamentos de tecnología logramos identificar cuales son los marcos de trabajo necesarios para aplicar en la creación del nuevo Marco de Referencia para Solincosta.

7.2. Recomendaciones

Para este proyecto solo queda recomendar la implementación de los siete servicios establecidos en la sección de Metodología.

Tener en cuenta los siguientes aspectos para la correcta implementación y uso del marco:

- Adopción de la cultura de gestión por servicios.
- Medición de los indicadores de control
- Plan de Auditorías

Estos deben ser tenidos en cuenta debido a la cultura actual de los funcionarios de la compañía, que ejecutan los procesos de acuerdo a su experiencia y sin un criterio establecido por la dirección. Una vez inicien el proceso de cambio, deben ser objetivos a la hora de tomar decisiones porque de estas dependerá el futuro de Solincosta.

Cabe resaltar que a medida que avanza el tiempo, hay otras compañías que posiblemente están implementando soluciones similares a esta o, incluso, ya estarán con un nivel de madurez mayor. Este punto es importante hacerlo ver a los funcionarios y directivos de Solincosta porque depende de ellos para que sea implementado en el menor tiempo posible garantizando los controles de seguridad esperados. Basado en esto, es prudente decir que es mejor renovarse que morir, adaptarse a los tiempos, desarrollar nuevas capacidades, la lucha es cruel y va dejando por el camino a los perdedores.

8. REFERENCIAS BIBLIOGRÁFICAS

ISO/IEC 27002:2013. (2005). ISO27002.ES.
https://www.iso27000.es/index.html

ITIL Intermediate - Gestión del servicio a lo largo del ciclo de vida. (2012). Mediagora, SL
ISBN: 978-84-8414-086-3

COBIT 2019: COBIT® 2019 FRAMEWORK: GOVERNANCE AND MANAGEMENT OBJECTIVES (2018). ISACA
ISBN 978-1-60420-764-4

White, S. (2018, 10 septiembre). CMMI maturity levels: A guide to optimizing development processes. CIO.
https://www.cio.com/article/3304245/cmmi-maturity-levels-a-guide-to-optimizing-development-processes.html

Montaño, Combita, de la Hoz (2017). Alineación de Cobit 5 Y Coso IC–IF para definición de controles basados en Buenas Practicas TI en cumplimiento de la Ley Sarbanes–Oxley.
http://www.revistaespacios.com/a17v38n23/17382303.html

Montaño (2014). Metodología Para Afinar El Modelo De Gobierno De Tecnologías De La Información En Las Organizaciones
https://revistas.uao.edu.co/ojs/index.php/REYA/article/view/120

Montaño (2010). Beneficios para el gobierno empresarial: Articulando COBIT con ISO 27000 para la exitosa implantación de un gobierno de TI
http://revistascientificas.cuc.edu.co/index.php/economicascuc/article/view/1192/0