EVALUACIÓN DE SEGURIDAD PARA EL PROCESO DE MESA DE AYUDA

TRABAJO DE GRADO

PABLO ESTEBAN RODRÍGUEZ FLÓREZ
WILLIAM ANDRÉS ZAMORA BOADA

Códigos

1032402116
1612010056

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
BOGOTÁ D.C
2017

EVALUACIÓN DE SEGURIDAD PARA EL PROCESO DE MESA DE AYUDA

TRABAJO DE GRADO

PABLO ESTEBAN RODRÍGUEZ FLÓREZ
WILLIAM ANDRÉS ZAMORA BOADA

Códigos

1032402116
1612010056

Asesor
ALEJANDRO CASTIBLANCO CARO

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
BOGOTÁ D.C
2017

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Bogotá D.C, 17 de septiembre de 2017

INTRODUCCIÓN

Mediante la elaboración de este trabajo se pretende realizar un análisis basado en el modelo de madurez registrado en el anexo 3 de la versión 5 del modelo de buenas prácticas de COBIT, sobre los controles con los que cuenta el proceso de mesa de ayuda de “la compañía”, para esto, se llevará a cabo un análisis detallado de cada uno de los controles implementados sobre dicho proceso y en base a la escala de medición propuesta por COBIT se establecerá un nivel de madurez para cada uno, adicional a esto y luego de llevar a cabo dicho análisis, se procederá a elaborar un documento con algunas directrices aplicables a los controles con niveles bajos de madurez.

Todo lo anterior se llevará a cabo con el fin de ayudar a “la compañía” a robustecer uno de sus procesos internos más importantes y con esto generar una mejor imagen frente a sus stakeholders.

ÍNDICE

Agradecimientos

Durante la elaboración de este trabajó atravesamos muchas etapas en las cuales siempre estuvimos acompañados de personas generosas, que gracias a su dedicación y energía aportaron una gran parte en el contenido, esquema, y resultados del mismo, agradecemos a todos los miembros de “La compañía” quienes nos acogieron en sus instalaciones y nos permitieron realizar el levantamiento de la información necesaria para llevar a cabo este proyecto, a nuestro docente, quien se encargó siempre de encaminarnos de nuevo por el camino correcto, a nuestros compañeros por los aportes en cada uno de los encuentros sincrónicos, a nuestras familias, amigos y demás personas que nos brindaron su apoyo siempre que lo necesitamos, sin todos ellos esto no hubiera sido posible.

1. RESUMEN EJECUTIVO

La compañía seleccionada para el proyecto, en la actualidad no ha realizado para el proceso de mesa de ayuda una evaluación a nivel de asimilación o de grado de cumplimiento respecto a los controles o buenas prácticas de seguridad existentes a nivel mundial; esta situación podría ocasionar riesgos asociados a la pérdida de disponibilidad, confidencialidad e integridad de la información.

Inicialmente para realizar el diagnóstico se realizará un entendimiento del proceso, identificando los participantes y los tipos de clientes, una vez realizada esta actividad se identificarán los controles y los riesgos a los cuales se encuentra expuesto el proceso evaluado, se tomará como referencia las buenas prácticas de los procesos de COBIT 5.

Una vez identificado los controles se realizará una evaluación de diseño de los controles que consiste en identificar las siguientes características:

- ¿Quién ejecuta el control?: Responsable de la aplicación del control
- Frecuencia del control: Identificar si el control se ejecuta diario, mensual, anual, semestral o esporádico
- ¿Como se ejecuta?: El control es automático, manual o semiautomático
- Documentación: Identificar si el control se encuentra documentado en un procedimiento y/o política.
- Evidencia: la ejecución del control deja soportes para análisis, auditorias y/o investigaciones.

El método de la evaluación del nivel de madurez consiste en evaluar los controles de seguridad desde un nivel de no-existente (0) hasta un nivel de optimizado (5), este valor se establecerá del resultado de las pruebas de diseño que se realizaron a los controles.

Para los controles que se identifiquen con oportunidades de mejora o que su nivel de madurez no es el adecuado para la seguridad de la información, se establecerán recomendaciones que ayuden a la remediación de las vulnerabilidades identificadas.

Dentro de los beneficios que puede adquirir la compañía se contemplan los siguientes:

- Soporte para dar cumplimiento a normatividad nacional e internacional.
- Apoyo para la implementación de elementos de Seguridad de la Información.
- Alineación con otros marcos de control o futuras certificaciones ISO 27000.
- Diferentes herramientas para apoyo en la medición de los niveles de madurez y pruebas de diseño y eficacia de los controles.
- Fácil identificación de riesgos y prácticas de control.

2. JUSTIFICACIÓN

La seguridad de la información actualmente se ha convertido en un apoyo fundamental para el cumplimiento de los objetivos estratégicos de las empresas, ya que con esto se logra un mayor reconocimiento frente a la competencia y tener mayor credibilidad y confianza en los clientes al momento de tomar una decisión para adquirir alguno de sus servicios.

El diagnóstico de seguridad al proceso de mesa de ayuda busca establecer el nivel de cumplimiento de los controles de seguridad que han implementado para mitigar los riesgos respecto a la confidencialidad, integridad y disponibilidad de la información.

Conocer el nivel de cumplimiento ayudará a la compañía a identificar e informar a la alta dirección las brechas de seguridad a las que se encuentra expuesta el proceso evaluado. Por lo tanto, se pueden definir planes de acción para llevar este proceso hasta un nivel de capacidad más aceptable y deseable para la compañía.

A continuación, casos de éxitos de empresas que realizarón una evaluación de los controles usando los niveles de madurez de COBIT.

Compañía	Beneficios	Fuente de consulta
Redeban Multicolor, Colombia	Realizó un Diagnostico a los procesos de TI por medio de una evaluación de madurez, con la cual logro mitigar riesgo que no se han identificado y logro una alineación entre el gobierno y la gestión de TI	Víctor Vásquez- Gerente Senior (Auditoría Interna) – 315-6073733
Scotiabank, Costa Rica	Fortalecimiento del alineamiento entre las estrategias de negocio y de TI, por medio de la coherencia entre dominios y procesos de COBIT Identificación de los controles claves que deben ser reforzados e implementados para asegurar un adecuado control interno para TI	http://www.isaca.org/KNOWLEDGE-CENTER/COBIT/COBIT-FOCUS/Pages/Implementacion-de-COBIT-4-0-en-Scotiabank-Costa-Rica.aspx?utm_referrer=
Ecopetrol S.A, Colombia	Se contrato un consultor externo para llevar a cabo la evaluación del nivel de madurez de COBIT.	http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-

	Ecopetrol logro consolidar el gobierno de TI, el riesgo y el cumplimiento regulatorio.	Ecopetrol.aspx
Banco Al Rajhi Bank, Arabia Saudita	El banco llevó a cabo una evaluación de capacidad de procesos basados en COBIT 5 e ISO 15504, para identificar las fortalezas y debilidades de los procesos existentes.	http://www.isaca.org/COBIT/focus/Pages/how-cobit-5-helped-al-rajhi-bank-to-meet-compliance-and-regulatory-requirements-spanish.aspx

Tabla 1- casos de éxito

3. MARCO TEORICO Y REFRENTES

Teniendo en cuenta el análisis a realizar, es pertinente tener claridad de los métodos y técnicas a emplear para llevar a cabo dicho proceso.

Existen varios marcos de referencia para tener en cuenta cuando de buenas prácticas de TI se habla, los estándares más utilizados en la actualidad son ITIL (biblioteca de infraestructura de tecnologías de información) y COBIT (objetivos de control para la información y tecnologías relacionadas), para este análisis puntualmente haremos uso del modelo COBIT, el cual es un modelo resultante de una investigación realizada por expertos de varios países del mundo y desarrollada por ISACA (asociación de auditoría y controles de sistemas de información).

En el apéndice 3 del libro de COBIT se muestra un modelo de madurez genérico, que permite calcular el estatus de los controles internos de una compañía," Muestra cómo la administración del control interno, y la conciencia de la necesidad de establecer mejores controles internos, por lo general evoluciona de algo ad hoc, hasta un nivel optimizado" (Cobit 4.0, 2005,p.184).

MODELO DE MADUREZ

El modelo de madurez propuesto por cobit se basa en una escala de 0 a 5 que permite, según algunos parámetros puntuales, establecer en qué nivel de madurez se encuentra, tanto el status de ambiente de control interno, como el establecimiento de controles internos utilizando las siguientes directrices:

Nivel de madurez	Estatus del ambiente de control interno	Establecimiento de controles internos
0 No existente O INEXISTENTE	No se reconoce la necesidad del control interno. El control no es parte de la cultura o misión organizacional. Existe un alto riesgo de deficiencias e incidentes de control.	No existe la intención de evaluar la necesidad del control interno. Los incidentes se manejan conforme van surgiendo.
1 Inicial / ad hoc	Se reconoce algo de la necesidad del control interno. El enfoque hacia los requerimientos de riesgo y control es ad hoc y desorganizado, sin comunicación o supervisión. No se identifican las deficiencias. Los empleados no están concientes de sus responsabilidades.	No existe la conciencia de la necesidad de evaluar lo que se necesita en téminos de controles de TI. Cuando se llevan a cabo, son solamente de forma ad hoc, a alto nivel y como reacción a incidentes significativos. La evaluación sólo se enfoca al incidente presente.

2	Repetible pero intuitivo	Existen controles pero no están documentados. Su operación depende del conocimiento y motivación de los individuos. La efectividad no se evalúa de forma adecuada. Existen muchas debilidades de control y no se resuelven de forma apropiada; el impacto puede ser severo. Las medidas de la gerencia para resolver problemas de control no son consistentes ni tienen prioridades. Los empleados pueden no estar concientes de sus responsabilidades.	La evaluación de la necesidad de control sucede solo cuando se necesita para ciertos procesos seleccionados de TI para determinar el nivel actual de madurez del control, el nivel meta que debe ser alcanzado, y las brechas existentes. Se utiliza un enfoque de taller informal, que involucra a los gerentes de TI y al equipo participante en el proceso, para definir un enfoque adecuado hacia el control para los procesos, y para generar un plan de acción acordado.
3	Proceso definido	Existen controles y están documentados de forma adecuada. Se evalúa la efectividad operativa de forma periódica y existe un número promedio de problemas. Sin embargo, el proceso de evaluación no está documentado. Aunque la gerencia puede manejar la mayoría de los problemas de control de forma predecible, algunas debilidades de control persisten y los impactos pueden ser severos. Los empleados están concientes de sus responsabilidades de control.	Los procesos críticos de TI se identifican con base en impulsores de valor y de riesgo. Se realiza un análisis detallado para identificar requisitos de control y la causa raíz de las brechas, así como para desarrollar oportunidades de mejora. Además de facilitar talleres, se usan herramientas y se realizan entrevistas para apoyar el análisis y garantizar que los propietarios de los procesos de TI son realmente los dueños e impulsan al proceso de evaluación y mejora.
4	Administrado y medible	Existe un ambiente efectivo de control interno y de administración de riesgos. La evaluación formal y documentada de los controles ocurre de forma periódica. Muchos controles están automatizados y se realizan de forma periódica. Es probable que la gerencia detecte la mayoría de los problemas de control, aunque no todos los problemas se identifican de forma rutinaria. Hay un seguimiento consistente para manejar las debilidades de control identificadas. Se aplica un uso de la tecnología táctico y limitado a los controles automatizados.	Se define de forma periódica qué tan críticos son los procesos de TI con el apoyo y acuerdo completo por parte de los propietarios de los procesos correspondientes. La evaluación de los requisitos de control se basa en las políticas y en la madurez real de estos procesos, siguiendo un análisis meticuloso y medido, involucrando a los participantes clave. La rendición de cuentas sobre estas evaluaciones es clara y está reforzada. Las estrategias de mejora están apoyadas en casos de negocio. El desempeño para lograr los resultados deseados se supervisa de forma periódica. Se organizan de forma ocasional revisiones externas de control.
5	Optimizado	Un programa organizacional de riesgo y control proporciona la solución continua y efectiva a problemas de control y riesgo. El control interno y la administración de riesgos se integran a las prácticas empresariales, apoyadas con una supervisión en tiempo real, y una rendición de cuentas completa para la vigilancia de los controles, administración de riesgos, e implantación del cumplimiento. La evaluación del control es continua y se basa en auto-evaluaciones y en análisis de brechas y de causas raíz. Los empleados se involucran de forma pro-activa en las mejoras de control.	Los cambios en el negocio toman en cuenta que tan críticos son los procesos de TI, y cubren cualquier necesidad de re-evaluar la capacidad del control de los procesos. Los propietarios de los procesos realizan auto-evaluaciones de forma periódica para confirmar que los controles se encuentran en el nivel correcto de madurez para satisfacer las necesidades del negocio, y toman en cuenta los atributos de madurez para encontrar maneras de hacer que los controles sean más eficientes y efectivos. La organización evalúa por comparación con las mejoras prácticas externas y busca asesoría externa sobre la efectividad de los controles internos. Para procesos críticos, se realizan evaluaciones independientes para proporcionar seguridad de que los controles se encuentran al nivel deseado de madurez y funcionan como fue planeado.

Figura 1. Modelo de madurez. Tomado de COBIT 4. 0.

Esta escala de medición está basada en el estándar **ISO/IEC 15504 Software Engineering – Process Assessment Standard (SPICE)**, creado en 1991 por el comité internacional de estándares de ingeniería de software y sistemas

ISO/IEC 15504

La norma ISO 15504 es un estándar que puede ser utilizado en cualquier tipo de organización y permite abarcar varios objetivos dentro de la evaluación de procesos como:

- Determinar el nivel de madurez de los procesos de la compañía.
- Ayuda a la mejora de los procesos implementados.
- Validar el nivel de cumplimiento para ciertos requisitos del ciclo de vida de desarrollo de software.

Adicional a esto, la norma ISO 15504 es una norma que permite establecer un proceso de mejora continua, ya que proporciona una serie de directrices para poder realizar mejoras sobre los problemas detectados.

La escala de calificación propuesta para la norma ISO 15504 se basa más en el nivel de cumplimiento que se tiene para cada proceso en relación a los objetivos del mismo, en esta escala el nivel 0 implica que el proceso evaluado no es capaz de conseguir sus objetivos y el 5 indica que el proceso analizado es capaz de conseguir sus objetivos y además se encuentra mejorando continuamente, así como se evidencia en la siguiente imagen:

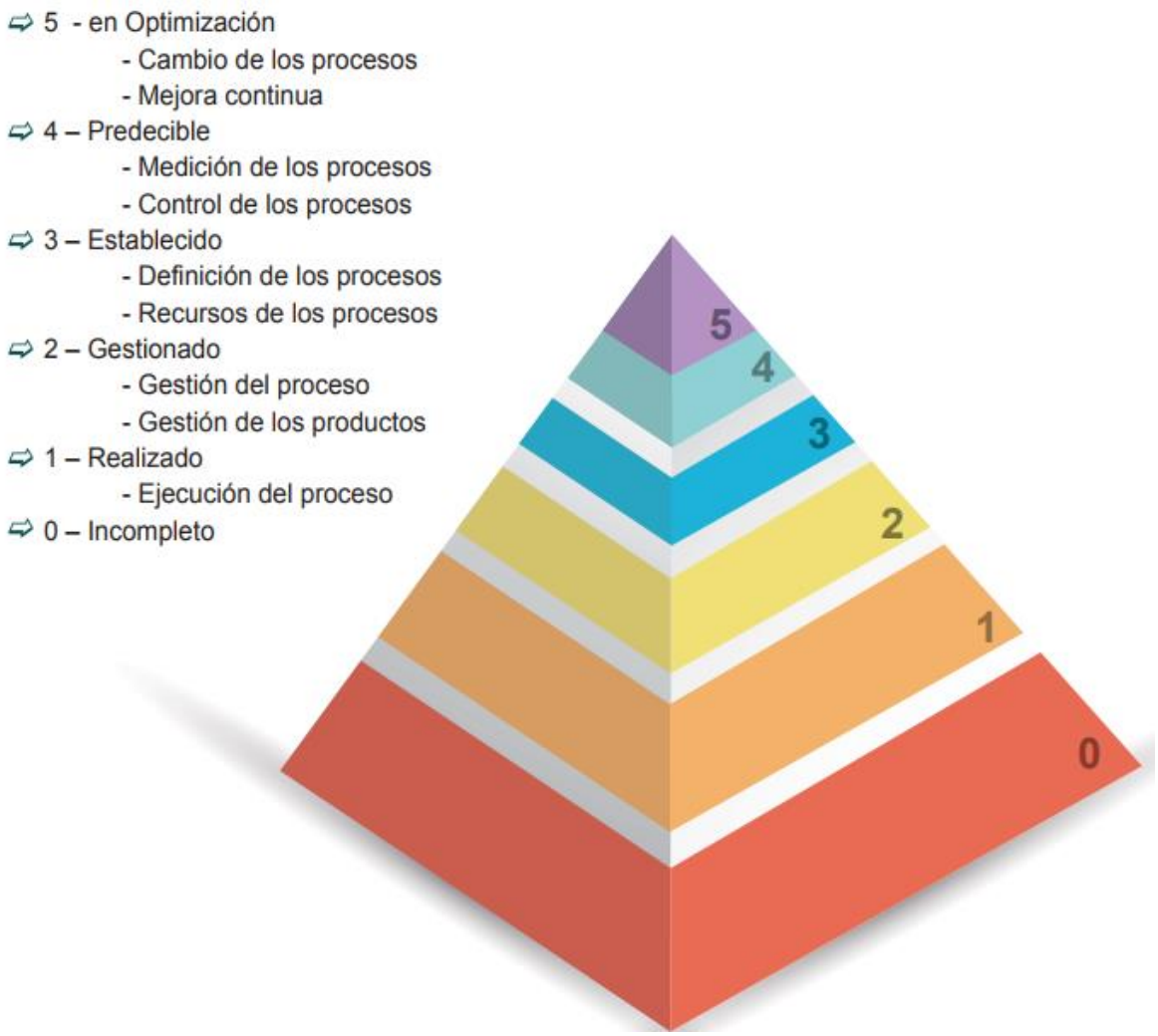

Imagen 1. Niveles de madurez según ISO 15504. Tomado de EQA. (2017). Niveles de capacidad

En conclusión, para llevar a cabo el análisis planteado en este documento, se hará uso de una combinación entre COBIT y la norma ISO 15504, con el fin de llevar a cabo un correcto análisis del proceso de mesa de ayuda de “la compañía” permitiendo determinar metodológicamente el nivel de madurez en el que se encuentran los controles implementados en la actualidad como se muestra en la siguiente imagen:

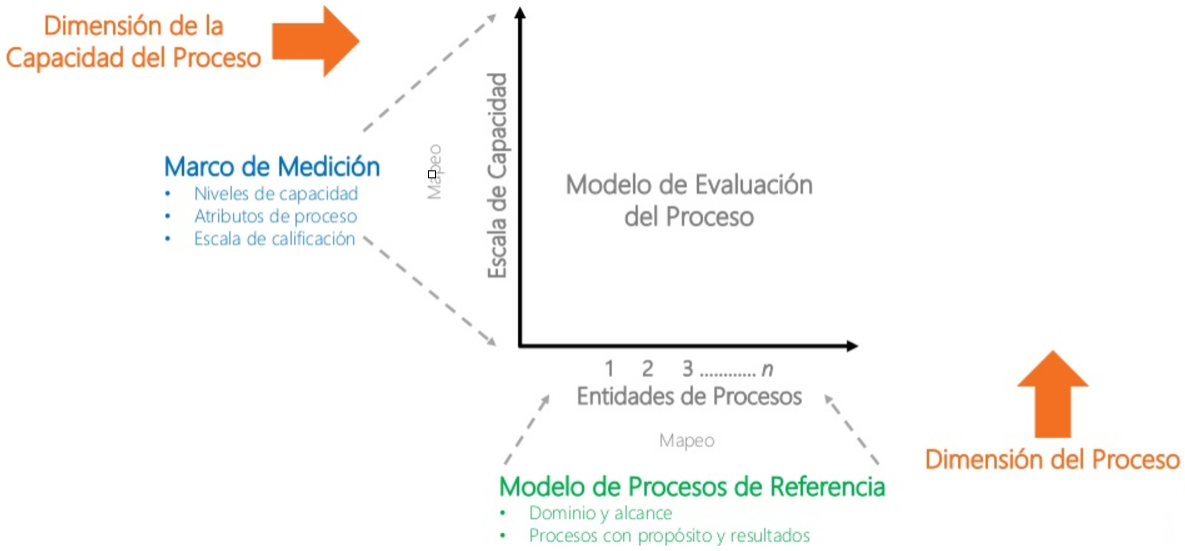

Imagen 2. Modelo de evaluación. Tomado de Lorenzo Armenta Fonseca. (2014).

4. METODOLOGÍA

Para el fortalecimiento de los mecanismos de los controles de seguridad del proceso de mesa de ayuda desarrollaremos una metodología con un enfoque integrado de Gobierno, Riesgos y Cumplimiento, relacionadas con la Seguridad en la Información, las cuales serán la base para generar las recomendaciones.

Como marcos de referencia para el desarrollo del proyecto se usará el modelo de COBIT, considerado como el más reconocido por su alineación con estándares y marcos de referencia, como ITIL, Serie ISO/IEC 27000., entre otros.

En la siguiente tabla se realizará una relación de los controles de COBIT a evaluar y los principios de la Seguridad de la Información:

Objetivos de Control de COBIT	**Principios de Seguridad de la Información**		
	Confidencialidad	**Integridad**	**Disponibilidad**
Alinear, Planificar y Organizar (APO)			
APO13- Gestionar la seguridad.	X	X	X
Construir, Adquirir e Implementar (BAI)			
BAI04 - Gestionar la Disponibilidad y la Capacidad			X
BAI08 - Gestionar el Conocimiento	X		X
Entrega, Servicio y Soporte (DSS)			
DSS04 – Gestionar la Continuidad			X
DSS05 - Gestionar servicios de seguridad.	X	X	X

Tabla Objetivos de control vs principios

El trabajar con este marco de referencia tendrá varios beneficios entre los cuales destacamos:

- Soporte para dar cumplimiento a normatividad nacional e internacional.
- Apoyo para la implementación de elementos de Seguridad de la Información.
- Alineación con otros marcos de control o futuras certificaciones ISO 27000.

- Diferentes herramientas para apoyo en la medición de los niveles de madurez y pruebas de diseño y eficacia de los controles.

- Fácil identificación de riesgos y prácticas de control.

A continuación, las fases que tendrá el proyecto:

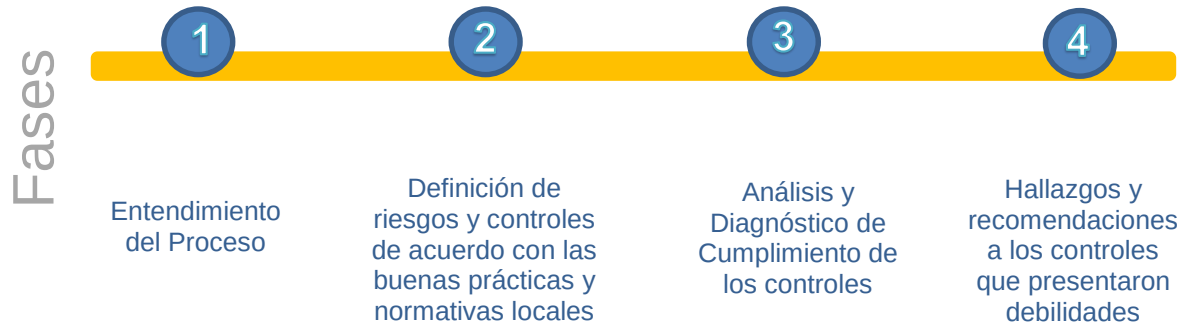

Imagen 3 Realizado por los autores del proyecto

Fase 1: Entendimiento del Proceso

Obtener el entendimiento del proceso de mesa de ayuda de la organización, identificar los servicios que presta y los tipos de cliente que se tiene.

Identificar las políticas, procedimientos y personas clave asociadas al proceso que se está evaluando.

Fase 2: Definición de riesgos y controles de acuerdo con las buenas prácticas y normativas locales

Luego del entendimiento del proceso se identificarán los controles a evaluar de acuerdo con las buenas prácticas.

Para el desarrollo de nuestro proyecto seleccionamos algunos procesos de gestión que se definen en COBIT 5, adicionalmente se analizarán los servicios que ofrecen, con fin de identificar que normatividad deben cumplir.

Fase 3: Análisis y Diagnóstico del cumplimiento

Realizar entrevistas y recopilar información para cada uno de los elementos de control relacionados en el alcance e identificar brechas de cumplimiento con las buenas prácticas y con la circular de la SFC.

Realizar pruebas de diseño, que consisten en identificar si los controles de seguridad cumplen con las siguientes características:

- ¿Que actividades se ejecutan para mitigar el o los riesgos?
- ¿Como se ejecuta el control?
- ¿Quién ejecuta el control?, ¿la persona que ejecuta el control es la adecuada?
- ¿Con que frecuencia se ejecuta?
- ¿Se deja evidencia de la ejecución del control?
- ¿El control se encuentra documentado en un procedimiento y/o política?

Luego de las pruebas, se identificarán las brechas de diseño, para cada uno de los controles que se evaluaron y se les dará un valor de acuerdo con su nivel de madurez como lo establece COBIT 4.0

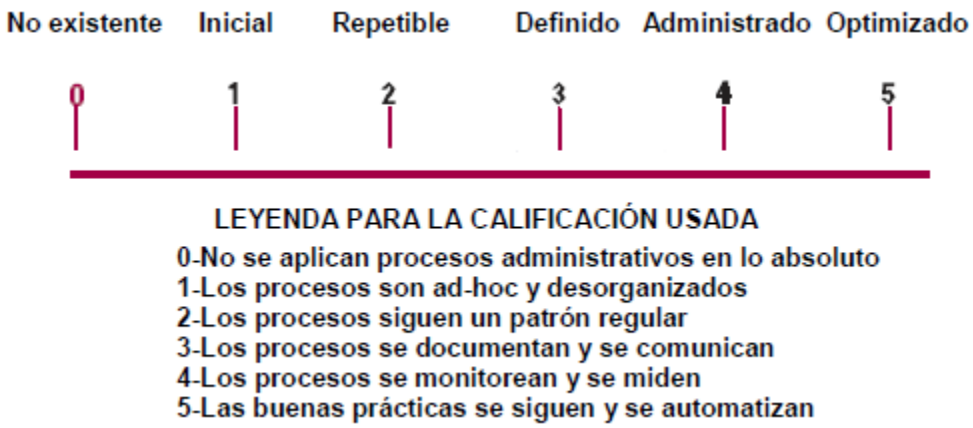

Imagen 4. Tomada de Cobit 4.0

Para los controles que presenten alguna oportunidad de mejora o su nivel de madurez no es el adecuado para el proceso se generaran recomendaciones que ayuden al cumplimiento del control y la mitigación de riesgos de seguridad.

Fase 4: Hallazgos y recomendaciones a los controles que presentaron debilidades

Para los controles de seguridad que presenten una oportunidad de mejora, se documentaran teniendo en cuenta los siguientes aspectos:

- **Título del hallazgo**: Situación encontrada
- **Criterio**: Se describe el deber ser (política, procedimiento, mejor práctica)
- **Condición:** Se describe el estado actual identificado.
- **Causa**: Se especifica la causa raíz de la situación que permite que ocurra el hallazgo.
- **Consecuencias:** Se describe el riesgo o exposición en que se encuentra la compañía frente al hallazgo identificado.
- **Recomendación:** Por cada oportunidad de mejora que se identifique, se realizará una recomendación aplicando los conocimientos y/o buenas prácticas referentes a la seguridad de la información, con el fin de que sirva de insumo para el fortalecimiento y mitigación de riesgos del proceso de mesa de ayuda

5. RESULTADOS Y DISCUSIÓN

FASE 1: Entendimiento del Proceso

El proceso de mesa de ayuda es una parte fundamental del área de servicios tecnológicos que se centra en la atención de requerimientos de servicio generados por los clientes de "la compañía" por medio de correos electrónicos o llamadas telefónicas, en la actualidad el grupo encargados de la atención de dichos requerimientos se encuentra conformado por 5 ingenieros y un líder que se encarga de dirigirlos y apoyarlos, cada uno de los requerimientos solicitados cuenta con un tiempo máximo de solución denominado SLA (Service-Level Agreement) que varía dependiendo de la dificultad y criticidad del mismo. De acuerdo a la criticidad del requerimiento existen 2 niveles de escalamiento uno interno y otro externo, el escalamiento interno consiste en escalar el requerimiento a los ingenieros de soporte para que estos con su experiencia y conocimiento den una pronta solución sin incumplir los SLA's, el escalamiento externo es directamente con el fabricante del equipo y normalmente se da cuando el requerimiento se encuentra relacionado con bugs del software o hardware del dispositivo.

Internamente en la mesa de ayuda se manejan 2 grupos de trabajo denominados grupo azul y grupo rojo, en el grupo azul se encuentran los 2 ingenieros más nuevos del grupo y por ende con menor nivel de conocimiento, este grupo se encarga de atender los requerimientos más sencillos, el grupo rojo está conformado por los otros 3 ingenieros del grupo y a diferencia del grupo azul, el grupo rojo se encarga de los casos más difíciles que se presentan.

Internamente se cuenta con una herramienta de IBM llamada ESS TIVOLI, esta herramienta sirve como repositorio de toda la información de los clientes de la compañía y como es de esperarse, allí también se crean y documentan todos los casos escalados a través de la mesa de ayuda, es importante aclarar que la herramienta cuenta cierta segmentación a nivel de perfiles que permite que los empleados, dependiendo de su cargo y are a la que pertenezcan tengan acceso solo a la información que requieren.

En el siguiente diagrama de flujo se explica puntualmente cual es el flujo que aplica en la actualidad el proceso de mesa de ayuda para la atención de los requerimientos generados por los

clientes de la compañía y el esquema de permisos que se tiene configurado actualmente sobre la herramienta ESS TIVOLI:

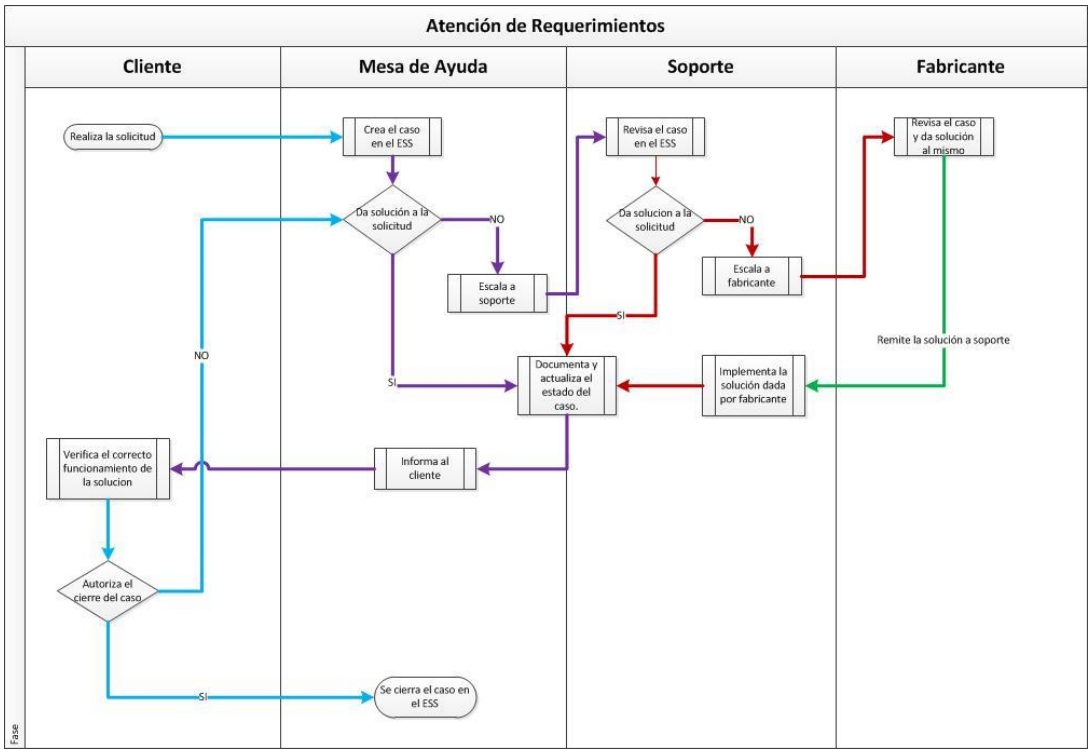

Imagen 5. Diagrama de Flujo Atención de requerimientos

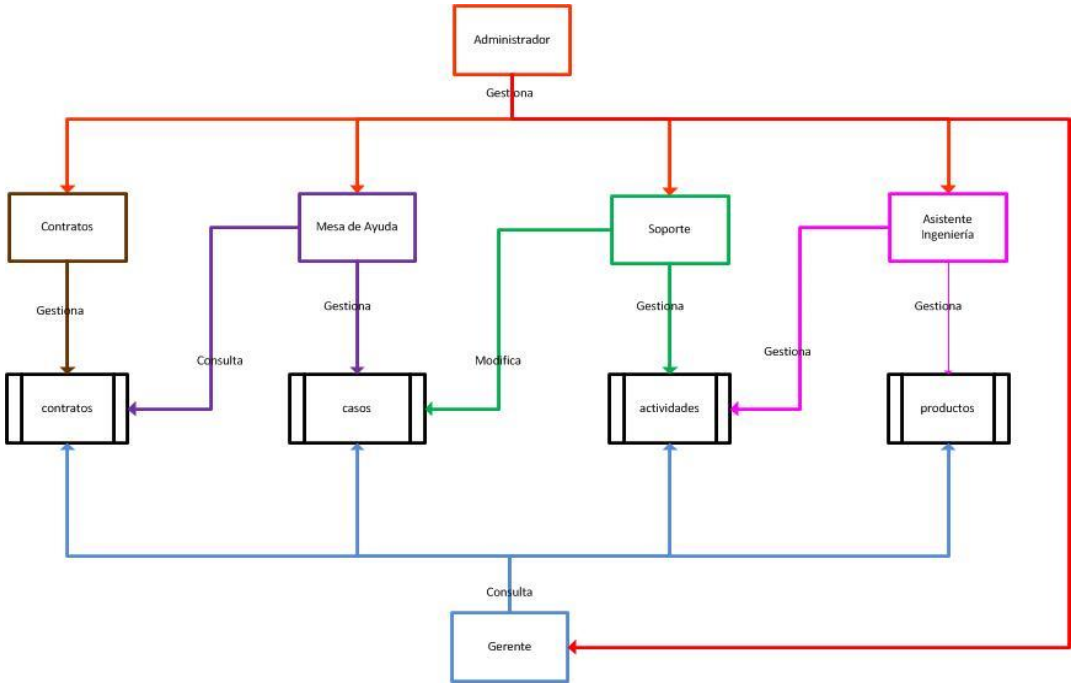

Imagen 6. Diagrama de Procesos de la Aplicación ESS Tivoli

FASE 2: Identificación de riesgos y controles de acuerdo con las buenas prácticas y normativas locales

Luego del entendimiento del proceso de mesa de ayuda, se seleccionas los controles que serán evaluados.

Se identificó que la compañía en el proceso de mesa de ayuda presta el servicio de atención al cliente para entidades que son inspeccionadas y vigiladas por la Superintendencia Financiera de Colombia (SFC), por lo tanto, están obligadas a cumplir el numeral 4.7 Centro de atención telefónica (Call Center, Contact Center), del capítulo décimo segundo de la Circular Externa 042 de 2012.

De acuerdo con lo anterior, se evaluarán los siguientes controles de la Circular 042:

Control	Objetivo de Control
4.7.1	Destinar un área dedicada exclusivamente para la operación de los recursos necesarios en la prestación del servicio, la cual deberá contar con los controles físicos y lógicos que impidan el ingreso de personas no autorizadas, así como la extracción de la información manejada.
4.7.2	Impedir el ingreso de dispositivos que permitan almacenar o copiar cualquier tipo de información, o medios de comunicación, que no sean suministrados por la entidad.
4.7.3	Dotar a los equipos de cómputo que operan en el centro de atención telefónica de los elementos necesarios que impidan el uso de dispositivos de almacenamiento no autorizados por la entidad. Igualmente, se deberá bloquear cualquier tipo de conexión a red distinta a la usada para la prestación del servicio
4.7.4	Garantizar que los equipos de cómputo destinados a los centros de atención telefónica solo serán utilizados en la prestación de servicios por ese canal.
4.7.5	En los equipos de cómputo usados en los centros de atención telefónica no se permitirá la navegación por Internet, el envío o recepción de correo electrónico, la mensajería instantánea, ni ningún otro servicio que permita el intercambio de información, a menos que se cuente con un sistema de registro de la información enviada y recibida. Estos registros deberán ser conservados por lo menos ocho (8) meses o en el caso en que la información respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto

Imagen 7. Controles CE042

Para la evaluación de los controles Seguridad de la Información del proceso de mesa de ayuda, se identificó los dominios, proceso y prácticas que aplican. Para tal fin se analizó las actividades que se ejecutan en este proceso, donde se evidenció que han implementado controles de ITIL y de la norma ISO 27002.

En el entendimiento del proceso de mesa de ayuda se identificó una matriz de riesgos y controles que ha definido la compañía para este proceso, cabe aclarar que la matriz se ajustó y se hicieron algunos cambios por temas de confidencialidad, adicionalmente para los riesgos no se muestra su calificación. Ver anexo 1

Con los controles que ha definido la compañía se realizó un mapeo que muestra la relación entre las secciones de ITIL del proceso de mesa de ayuda y los objetivos de control de COBIT que se asocian y que se van a evaluar.

ITIL		COBIT	Principios de Seguridad		
Asunto	Proceso Compañía	Proceso	Confidencialidad	Integridad	Disponibilidad
Diseño de servicio	Gestión de Seguridad de la Información	DSS04.07 Gestionar acuerdos de respaldo.			x
	Gestión de la Continuidad del Servicio	DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance DSS04.04 Ejercitar, probar y revisar el plan DSS04.06 Proporcionar formación en el plan de continuidad. DSS04.08 Ejecutar revisiones post-reanudación.			x
	Gestión del nivel de servicio	BAI04.02 Evaluar el impacto en el negocio. BAI04.03 Planificar requisitos de servicios nuevos o modificados	x		
	Gestión de Capacidad	BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia.			x
Transición del Servicio	Gestión de la liberación y distribución	BAI08.02 Identificar y clasificar las fuentes de información. BAI08.05 Evaluar y retirar la información.	x		x
	Gestión de conocimiento del servicio	BAI08.03 Organizar y contextualizar la información, transformándola en conocimiento.			x

Imagen 8. Mapeo ITIL y COBIT

También se realizó el mapeo entre el ISO/IEC 27002 y los objetivos de control de COBIT que serán evaluados en este proyecto

ISO 27002		COBIT
Objetivo	**Controles**	**Proceso**
A.5 Politicas de seguridad de la información	A.5.1 Orientación de la dirección para la gestión de la seguridad de la información	APO13.01 Establecer y mantener un SGSI. APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.
	A.5.1.2 Revisión de las políticas para la seguridad de la información	APO13.03 Supervisar y revisar el SGSI.
A.6 Organización de la seguridad de la información	A.6.2.1 Política para dispositivos móviles	DSS05.03 Gestionar la seguridad de los puestos de usuario final.
A.12 Seguridad de las operaciones	A.12.2.1 Controles contra códigos maliciosos	DSS05.01 Proteger contra software malicioso (malware).
A.13 Seguridad de las comunicaciones	A.13.1 Gestión de la seguridad de las redes	DSS05.02 Gestionar la seguridad de la red y las conexiones.
	A.13.1.1 Controles de redes	
	A.13.1.2 Seguridad de los servicios de red	
	A.13.1.3 Separación en las redes	
A.11 Seguridad física y del entorno	A.11.1.1 Perimetro de seguridad física	DSS05.05 Gestionar el acceso físico a los activos de TI.
	A.11.1.2 Controles de acceso físico	
	A.11.1.3 Seguridad de oficinas, recintos e instalaciones	
	A.11.1.4 Protección contra amenazas externas y ambientales	
	A.11.1.5 Trabajo en áreas seguras	
	A.11.1.6 Áreas de despacho y carga	
	A.11.2.1 Ubicación y protección de los equipos	DSS05.03 Gestionar la seguridad de los puestos de usuario final.
	A.11.2.2 Servicios de suministro	
	A.11.2.3 Seguridad del cableado	
	A.11.2.4 Mantenimiento de equipos	
	A.11.2.5 Retiro de activos	
	A.11.2.6 Seguridad de equipos y activos fuera de las instalacior	
	A.11.2.7 Disposición segura o reutilización de equipos	
	A.11.2.8 Equipos de usuarios desatendidos	
	A.11.2.9 Política de escritorio limpio y pantalla limpia	
A.9 Control de acceso	A.9.1.1 Política de control de acceso	DSS05.04 Gestionar la identidad del usuario y el acceso lógico.
	A.9.1.2 Acceso a redes y a servicios en red	
	A.9.2.1 Registro y cancelación del registro de usuarios	
	A.9.2.2 Suministro de acceso de usuarios	
	A.9.2.3 Gestión de derechos de acceso privilegiado	
	A.9.2.4 Gestión de información de autenticación secreta de us	
	A.9.2.5 Revisión de los derechos de acceso de los usuarios	
	A.9.2.6 Retiro o ajuste de los derechos de acceso	
A.8 Gestión de activos	A.8.2.1 Clasificación de la información	DSS05.06 Gestionar documentos sensibles y dispositivos de salida.
	A.8.2.2 Etiquetado de la información	
	A.8.2.3 Manejo de activos	
A.12 Seguridad de las operaciones	A.12.4.1 Registro de eventos	DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.
	A.12.4.2 Protección de la información de registro	
	A.12.4.3 Registros del administrador y del operador	

Imagen 9. Mapeo ISO 27002 y COBIT

Fase 3: Análisis y Diagnóstico del cumplimiento

Las actividades que se ejecutaron para realizar la prueba de los controles fueron:

Imagen 10 actividades pruebas de control

Todas las pruebas se documentaron en un papel de trabajo, que contiene la evidencia de las pruebas de recorrido que se hicieron, al finalizar en cada documento se dio una conclusión indicando si el control evaluado cumple con los requerimientos de un control o si este presenta alguna oportunidad de mejora que ayude al funcionamiento de la seguridad de la información del proceso que se está evaluando. Ver anexo 2

Calificación Proceso Mesa de Ayuda

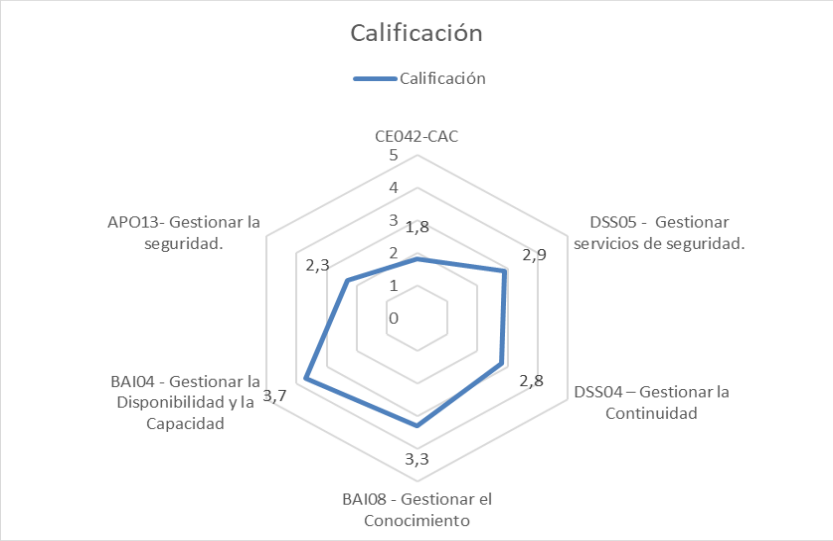

Imagen 11 Calificación Elementos

Según la valoración de niveles de madurez de COBIT y la evaluación de seguridad del proceso de mesa de ayuda, presenta un nivel de madurez de 2,8 sobre 5. “Repetible” debido a se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

Los procesos evaluados presentaron las siguientes calificaciones:

Nivel de madurez 2- Repetible.

- Circular 042 - Centro de atención telefónica (Call Center, Contact Center)
- APO13- Gestionar la seguridad.
- DSS05- Gestionar servicios de seguridad.
- DSS04 Gestionar la Continuidad

Donde se identifica que la compañía ha desarrollado procedimientos para su cumplimiento de los procesos de seguridad que se definen para el ambiente de control del centro de atención al cliente.

Sin embargo, se evidenció que los controles implementados presentan oportunidades de mejora en cuanto a la falta de entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad del cumplimiento a los funcionarios de la compañía.

Nivel de madurez 3 - Cumple, pero tiene aspectos por mejorar

- BAI04 - Gestionar la Disponibilidad y la Capacidad
- BAI08 - Gestionar el Conocimiento

Se identifican que los procedimientos se han estandarizado y documentado y se han difundido a través de entrenamiento.

Sin embargo, se deja que el personal de mesa de ayuda decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados, pero formalizan las prácticas existentes.

A continuación, se muestra la calificación de cada uno de los procesos por cada uno de los elementos que se evaluaron:

Circular 042 - Centro de atención telefónica (Call Center, Contact Center):

Elemento	Calificación
4.7.1-Área exclusiva para call center	2,0
4.7.2- Control de medios de almacenamiento	1,0
4.7.3-Control de ingreso de dispositivos de almacenamiento	2,0
4.7.4-Uso adecuado de los equipos	2,0
4.7.5-Control de acceso a internet	2,0
Total Promedio	**1,8**

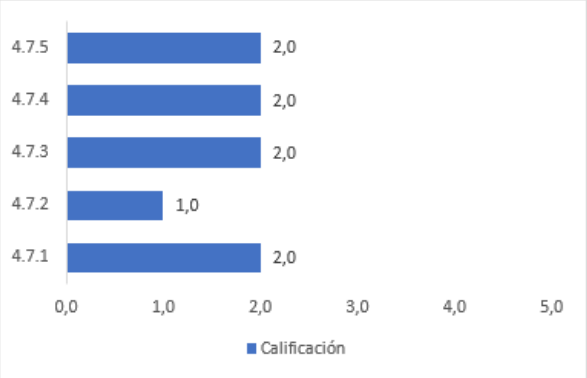

Imagen 12 Calificación CE042

APO13- Gestionar la seguridad.

Control #	Calificación
APO13.01	3,0
APO13.02	3,0
APO13.03	1,0
Total Promedio	**2,3**

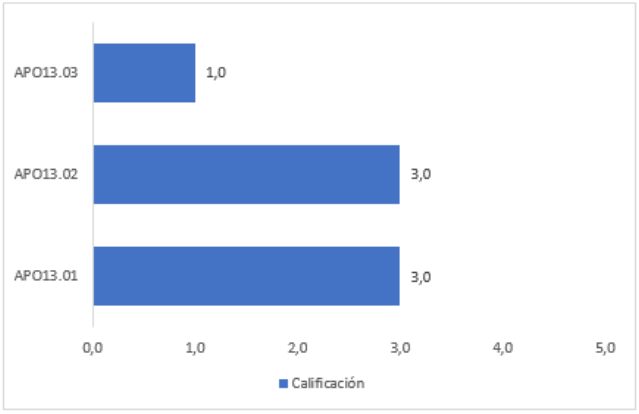

Imagen 13 Calificación APO13

BAI04 - Gestionar la Disponibilidad y la Capacidad

Elemento	Calificación
BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia.	4,0
BAI04.02 Evaluar el impacto en el negocio.	3,0
BAI04.03 Planificar requisitos de servicios nuevos o modificados	4,0
Total Promedio	**3,7**

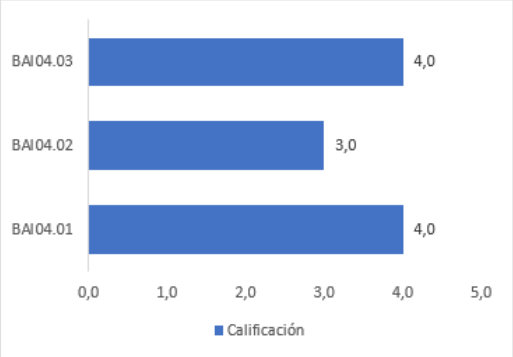

Imagen 14 Calificación BAI04

BAI08 - Gestionar el Conocimiento

Elemento	Calificación
BAI08.02 Identificar y clasificar las fuentes de información.	3,0
BAI08.03 Organizar y contextualizar la información, transformándola en conocimiento.	3,0
BAI08.05 Evaluar y retirar la información.	4,0
Total Promedio	**3,3**

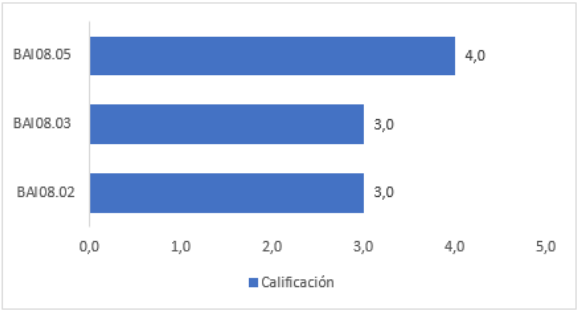

Imagen 15 Calificación BAI08

DSS04 – Gestionar la Continuidad

Elemento	Calificación
DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance	4,0
DSS04.04 Ejercitar, probar y revisar el plan de continuidad.	2,0
DSS04.06 Proporcionar formación en el plan de continuidad.	2,0
DSS04.07 Gestionar acuerdos de respaldo.	4,0
DSS04.08 Ejectuar revisiones post-reanudación.	2,0
Total Promedio	**2,8**

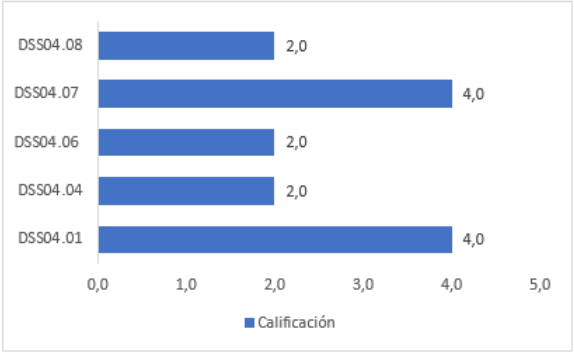

Imagen 16 Calificación DSS04

DSS05 - Gestionar servicios de seguridad.

Control #	Calificación
DSS05.01	1,0
DSS05.02	3,0
DSS05.03	3,0
DSS05.04	3,0
DSS05.05	3,0
DSS05.06	3,0
DSS05.07	4,0

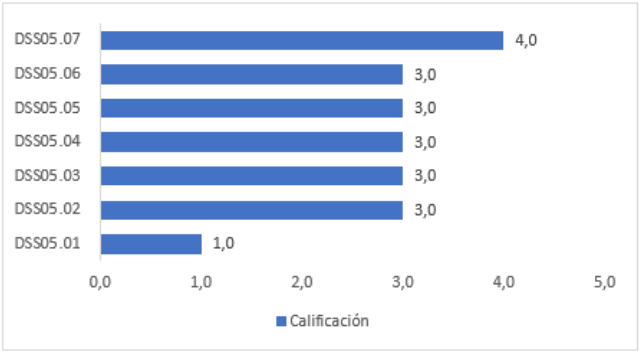

Imagen 17 Calificación DSS05

Fase 4: Hallazgos y recomendaciones a los controles que presentaron debilidades

La calificación de los controles se realizó de acuerdo con la siguiente tabla:

0 – No Existente	
0	Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido que existe un problema a resolver.
1 - Inicial	
1	Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar, en su lugar existen enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso a caso. El enfoque general de la organización es desorganizado.
2 - Repetible	
2	Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.
3 – Cumple pero tiene aspectos por mejorar	
3	Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados, pero formalizan las prácticas existentes.
4 - Administrado	
4	Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera aislada o fragmentada.
5 – Óptimo	
5	Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida

A continuación, se registran los controles que presentan alguna oportunidad de mejora.

Control	Hallazgo	Calificación	Referencia
Circular 042 - Centro de atención telefónica (Call Center, Contact Center)			
4.7.1	Ausencia de un área exclusiva para el centro de atención al cliente	2	Ver anexo 3.1

Control	Hallazgo	Calificación	Referencia
4.7.2	Ausencia de controles que restrinjan el ingreso de dispositivos	1	Ver anexo 3.1
4.7.3	Ausencia de mecanismos de seguridad en el centro de atención al cliente	2	Ver anexo 3.1
4.7.4	Uso indebido en los equipos de cómputo del centro de atención al cliente	2	Ver anexo 3.1
4.7.5	Ausencia de controles para la navegación de internet en el centro de atención al cliente	2	Ver anexo 3.1
APO13- Gestionar la seguridad.			
APO13.01	No alineación del SGSI con el proceso de mesa de ayuda	3	Ver anexo 3.2
APO13.02	Falta de riesgos de seguridad de la información al proceso de mesa de ayuda	3	Ver anexo 3.2
APO13.03	Falta de revisión y evaluación de los controles de seguridad	1	Ver anexo 3.2
BAI04 - Gestionar la Disponibilidad y la Capacidad			
BAI04.02	Debilidades en la evaluación del impacto en cuanto a la disponibilidad y capacidad del proceso de mesa de ayuda	3	Ver anexo 3.3
BAI08 - Gestionar el Conocimiento			
BAI08.02 BAI08.03	Debilidades en la clasificación de activos de información al proceso de mesa de ayuda	3	Ver anexo 3.4
DSS04 – Gestionar la Continuidad			
DSS04.04	Falta de ejecución de pruebas de continuidad al proceso de mesa de ayuda	2	Ver anexo 3.5
DSS04.06	Falta de formación a las partes implicadas para la contingencia	2	Ver anexo 3.5
DSS04.08	Ausencia de revisiones post-reanudación de continuidad del negocio.	2	Ver anexo 3.5
DSS05 - Gestionar servicios de seguridad			
DSS05.01	Soporte Windows Server 2003	1	Ver anexo 3.6

Tabla Resumen hallazgos

6. CONCLUSIONES

El diagnóstico del nivel de cumplimiento normativo y de exposición a riesgos de seguridad de la información del proceso de mesa de ayuda, fue vital para lograr la identificación de brechas y oportunidades de mejora en los controles de seguridad, adicionalmente se generaron recomendaciones que ayudan a la mitigación de los riesgos identificados

La medición de los controles con los niveles de madurez de COBIT, permitió conocer en que calificación de seguridad se encuentra el proceso de mesa de ayuda y que procesos necesitan una mayor atención y cuales ya se encuentran en un nivel adecuado.

Se establecieron recomendaciones que se encuentran alineadas a las buenas prácticas de seguridad y al cumplimiento regulatorio, que ayudarán a que el proceso de mesa de ayuda se encuentre en un nivel de madurez más adecuado y acorde con los servicios que ofrece.

Por último, con la evaluación del nivel de madurez, se logra alinear el Sistema de Gestión de Seguridad de la Información con el proceso de mesa de ayuda, por medio de la identificación de los controles claves que deben ser reforzados e implementados para asegurar una adecuada gestión de seguridad.

En el desarrollo del proyecto se aplicaron los conceptos y conocimientos adquiridos durante toda la especialización de seguridad de la información, principalmente en la evaluación de controles y las recomendaciones realizadas.

7. BIBLIOGRAFÍA

COBIT 5. (2012). United States of America: ISACA.

COBIT 5 Guía Catalizadora. (2012). United States of America: ISACA.

COBIT 4.0. (2005). Estados Unidos de América: ISACA.

TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. CÓDIGO DE PRÁCTICA PARA CONTROLES DE SEGURIDAD DE LA INFORMACIÓN. (2013). Bogotá: ICOTEC.

CAPÍTULO DÉCIMO SEGUNDO: REQUERIMIENTOS MÍNIMOS DE SEGURIDAD Y CALIDAD PARA LA REALIZACIÓN DE OPERACIONES. (2012). Bogotá: SUPERINTENDENCIA FINANCIERA DE COLOMBIA.

The ITIL® V3 factsheet benchmark guide. (2009). Brisbane, Australia.

Isaca.org. (2017). COBIT Case Study: Implementing COBIT for IT Governance, Risk and Compliance at Ecopetrol S.A.. [online] Available at: http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-Ecopetrol.aspx

Isaca.org. (2017). Implementación de COBIT 4.0 en Scotiabank, Costa Rica. [online] Available at: http://www.isaca.org/KNOWLEDGE-CENTER/COBIT/COBIT-FOCUS/Pages/Implementacion-de-COBIT-4-0-en-Scotiabank-Costa-Rica.aspx?utm_referrer=

Isaca.org. (2017). Cómo COBIT 5 ayudó a Al Rajhi Bank a alcanzar los requerimientos de cumplimiento y regulatorios. [online] Available at: http://www.isaca.org/COBIT/focus/Pages/how-cobit-5-helped-al-rajhi-bank-to-meet-compliance-and-regulatory-requirements-spanish.aspx

8. ANEXOS

ANEXO 1- Matriz de Riesgos y Controles

Anexo
1-Analisis_de_riesgo

ANEXO 2- Plan de auditoria

Anexo 2-Plan de
auditoria..xlsx

ANEXO 3- Hallazgos y recomendaciones

Anexo 3.1

Evaluación cumplimiento Circular 042 - Centro de atención telefónica (Call Center, Contact Center):

Calificación		2
Código	**Hallazgo**	**Recomendación**
4.7.1	**Ausencia de un área exclusiva para el centro de atención al cliente** La circular 042 de SFC ha establecido en el numeral 4.71 "Destinar un área dedicada exclusivamente para la operación de los recursos necesarios en la prestación del servicio, la cual deberá contar con los controles físicos y lógicos que impidan el ingreso de personas no autorizadas, así como la extracción de la información manejada." De acuerdo con lo anterior, se identificó que la compañía no cuenta un área exclusiva para desarrollo de estas actividades, debido a que esta área es compartida para la prestación de otros servicios. El no contar con área exclusiva podría ocasionar perdida de confidencialidad de la información de la compañía, e ingreso de personas no autorizadas a las áreas restringidas.	La compañía debe identificar los clientes que se encuentren vigilados por SFC y a los cuales se les presta el servicio de atención al cliente. Una vez identificados se de disponer de controles físicos y lógicos que impidan que personas no autorizado tenga acceso a la información de los clientes. Como controles físicos se recomienda se establezcan factores de doble autenticación, como por ejemplo tarjeta de acceso y dispositivos biométricos, para los controles lógicos establecer una gestión de identidades para que los usuarios ingresen de acuerdo

Calificación		2
Código	**Hallazgo**	**Recomendación**
		con su perfil con un usuario y una contraseña cumpliendo la política de contraseñas que ha establecido la compañía.

Calificación		1
Código	**Hallazgo**	**Recomendación**
4.7.2	**Ausencia de controles que restrinjan el ingreso de dispositivos** La circular 042 de SFC ha establecido en el numeral 4.7.2 “Impedir el ingreso de dispositivos que permitan almacenar o copiar cualquier tipo de información, o medios de comunicación, que no sean suministrados por la entidad.” De acuerdo con lo anterior, se puedo evidenciar que se puede ingresar dispositivos electrónicos tales como: celulares y memorias USB sin ningún problema, adicionalmente el personal encargado de esta área no tiene conocimiento que exista una directriz gerencial para el impedimento de ingreso de estos dispositivos al área de mesa de ayuda. El no contar con controles que impida o controlen el ingreso de dispositivos electrónicos, puede ocasionar sustracción de información que pueda causar pérdidas para la compañía.	Establecer dentro de la política de seguridad de la información criterios que indiquen que requerimientos se deben cumplir para ingreso de las instalaciones donde se presta el servicio de atención al cliente y que consecuencias tiene el incumplir estas medidas. Toda actualización de la política debe estar aprobado por la alta gerencia de la compañía. Se deben realizar revisiones periódicas para verificar el cumplimiento de la política.

Calificación		2
Código	**Hallazgo**	**Recomendación**
4.7.3	**Ausencia de mecanismos de seguridad en el centro de atención al cliente** La circular 042 de SFC ha establecido en el numeral 4.7.3 “Dotar a los equipos de cómputo que operan en el centro de atención telefónica de los elementos necesarios que impidan el uso de dispositivos de almacenamiento no autorizados por la entidad. Igualmente, se deberá bloquear cualquier tipo de conexión a red distinta a la usada para la prestación del servicio”	Establecer dentro de la política de seguridad de la información criterios que indiquen que requerimientos se deben cumplir para el uso de los equipos de cómputo en el área de atención al cliente y que consecuencias tiene el incumplir estas medidas. Toda actualización de la política debe estar aprobado por la alta gerencia de la compañía.

Calificación		2
Código	**Hallazgo**	**Recomendación**
	De acuerdo con lo anterior, se puedo evidenciar que no existe ningún control de seguridad que impida el retiro de información por medio de los puertos USB de los equipos de cómputo, debido a la compañía no identificado este tipo de controles para esta área El no contar con controles que impida el retiro de información, puede ocasionar perdida de información o daño en los equipos de cómputo.	Se deben realizar un bloqueo de puertos USB para la extracción de información, en caso de que se necesite extraer información es necesario contar con una USB autorizada por la compañía, esta debe estar personalizada y será usada únicamente para fines laborales. Establecer un log de auditoria que registre el día que se extrajo la información, el equipo y nombre de los archivos, toda esta información se debe revisar de manera periódica notificando cualquier incumplimiento a la política.

Calificación		2
Código	**Hallazgo**	**Recomendación**
4.7.4	**Uso indebido en los equipos de cómputo del centro de atención al cliente** La circular 042 de SFC ha establecido en el numeral 4.7.4 “Garantizar que los equipos de cómputo destinados a los centros de atención telefónica solo serán utilizados en la prestación de servicios por ese canal”. De acuerdo con lo anterior, se evidenció que los equipos de cómputo de esta área son usados para uso personal de los empleados, identificando archivos que no hacen parte para la prestación del servicio, debido a la ausencia de planes de sensibilización por parte del oficial de seguridad de la información de la compañía. La anterior situación podría ocasionar retrasos en operación, debido a la ejecución de programas que pueden consumir la memoria de los equipos de computo	Sensibilizar a los funcionarios del proceso de mesa de ayuda, para que estos hagan un buen uso de los equipos de cómputo y la importancia que esto tiene para prestar un óptimo y mejor servicio al cliente. Se deben realizar revisiones periódicas a los equipos y tomar las medidas necesarias en cado de un incumpliendo a la política de seguridad

Calificación		2
Código	**Hallazgo**	**Recomendación**
4.7.5	**Ausencia de controles para la navegación de internet en el centro de atención al cliente** La circular 042 de SFC ha establecido en el numeral 4.7.4 “En los equipos de cómputo usados en los centros de atención telefónica no se permitirá la navegación por Internet, el envío o recepción de correo electrónico, la mensajería instantánea, ni ningún otro servicio que permita el intercambio de información, a menos que se cuente con un sistema de registro de la información enviada y recibida. Estos registros deberán ser conservados por lo menos ocho (8) meses o en el caso en que la información respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto”. De acuerdo con lo anterior, se evidenció que la compañía no ha implementado mecanismos de conservación de la información para la envió y recepción de la información, adicionalmente en los equipos de cómputo se permite la navegación de internet sin ninguna restricción. Esta situación se presenta por el desconocimiento y falta de implementación de controles que impidan la navegación de internet. La anterior situación podría ocasionar, perdida de confidencialidad de la información de la compañía. Uso inadecuado de los dispositivos que pueden ocasionar retrasos en la operación	Si la compañía permite la navegación de internet al área de mesa de ayuda, esta debe tener en cuenta el cumplimiento e implementación de los siguientes controles: • Registro de información de la navegación de internet que realizan los funcionarios, esta debe estar almacenada en un servidor restringido. • Se ben realizar copias de seguridad del registro de información. • Monitoreo de las páginas que son visitadas por los funcionarios. • Restringir ciertas páginas web que puedan consumir el ancho de banda.

Anexo 3.2

APO13- Gestionar la seguridad.

Calificación		3
Código	**Hallazgo**	**Recomendación**
APO13.01	**No alineación del SGSI con el proceso de mesa de ayuda**	Buscar alinear el proceso de mesa de ayuda con el SGSI de la compañía, identificando las partes interesadas y los activos

Calificación		3
Código	**Hallazgo**	**Recomendación**
	La compañía ha establecido un SGSI, donde se ha definido una clasificación de activos de información, análisis de riesgos, definición de métricas de seguridad, una política de seguridad de la información, entre otros aspectos. Sin embargo, se identificó que el proceso de mesa de ayuda no se encuentra alineado al SGSI, debido que se evidencia que el alcance la política se encuentra delimitada en algunos procesos, adicionalmente no se identificaron riesgos asociados al cumplimiento regulatorio. La anterior situación podría ocasionar, desalineación del SGSI con el proceso de mesa de ayuda que pueden ocasionar fallas y/o incumplimos en la prestación del servicio	de información y si mismo realizar un análisis de riesgo

Calificación		3
Código	**Hallazgo**	**Recomendación**
APO13.02	**Falta de riesgos de seguridad de la información al proceso de mesa de ayuda** La compañía ha establecido un SGSI, donde se ha definido una clasificación de activos de información, análisis de riesgos, definición de métricas de seguridad, una política de seguridad de la información, entre otros aspectos. Sin embargo, se identificó que la matriz de riesgos y controles que ha definido la compañía, no se encuentra ningún riesgo y control asociado al cumplimiento regulatorio, debido a que no se ha realizado una revisión y actualización a la matriz de riesgos. La anterior situación podría ocasionar, materialización de amenazas, vulnerabilidades, riesgos no determinados para lo más importante en cualquier organización los Activos de Información. Robo de Información, Fraudes internos y externos, entre otros.	Realizar un inventario de clientes y de los servicios que se les presta y determinar que regulaciones deben cumplir y si esto se encuentra dentro del alcance del contrato. Una vez identificado estos clientes, se debe realizar un levantamiento de riesgos y determinar su probabilidad e impacto alineado a la metodología de riesgo que ha establecido la compañía. Con los riesgos identificados se deben identificar con el dueño del proceso los controles de seguridad que se deben implementar. Por último, anualmente o en caso de un cambio o inclusión

Calificación		3
Código	**Hallazgo**	**Recomendación**
		de un nuevo proceso, se debe actualizar la matriz de riesgos y controles.

Calificación		1
Código	**Hallazgo**	**Recomendación**
APO13.03	**Falta de revisión y evaluación de los controles de seguridad** La compañía ha definido controles y riesgos para el proceso de mesa de ayuda. Sin embargo, a la fecha de nuestra revisión no se ha realizado ninguna evaluación a los controles por un área diferente al de mesa de ayuda. La anterior situación podría ocasionar, problemas en la prestación del servicio por fallos en infraestructura no detectados y ocurrencia de incidentes.	Realizar anualmente o semestralmente una evaluación de los controles del proceso de mesa de ayuda, con el fin de identificar si los controles son los adecuados o si estos se están ejecutando correctamente y que esto sirva de insumo para la evaluación del riesgo residual. Esta revisión debe ser realizada por área diferente y con el conocimiento necesario para evaluar los controles de seguridad.

Anexo 3.3

BAI04 - Gestionar la Disponibilidad y la Capacidad

Calificación		3
Código	**Hallazgo**	**Recomendación**
BAI04.02	**Debilidades en la evaluación del impacto en cuanto a la disponibilidad y capacidad del proceso de mesa de ayuda** La compañía ha identificado los servicios críticos del proceso de mesa de ayuda y estos se encuentran documentados. Sin embargo, para los servicios de atención al cliente, se presentan debilidades debido a que no se han realizado actualización e identificación de nuevos clientes y a los cuales se les presta este servicio. Lo anterior podría ocasionar, pérdida en la calidad y eficiencia en el proceso de mesa de ayuda	Realizar revisiones periódicas y cuando se presentan cambios en la prestación del servicio, con el fin de identificar los impactos que tendrá el servicio en cuanto a disponibilidad y a capacidad. Estas medidas ayudan a reforzar los controles implementados o tomar medidas que ayuden a la prestación de un mejor servicio.

Anexo 3.4

BAI08 - Gestionar el Conocimiento

Calificación		3
Código	**Hallazgo**	**Recomendación**
BAI08.02 **BAI08.03**	**Debilidades en la clasificación de activos de información al proceso de mesa de ayuda** La compañía ha identificado y clasificado los activos de información y estas se encuentran documentadas. Sin embargo, se evidenció que no se cuenta con un inventario de activos críticos clasificados de acuerdo con la criticidad de la información y definiendo su propietario para el servicio de mesa de ayuda Lo anterior podría ocasionar, pérdida en la calidad y eficiencia en el proceso de mesa de ayuda	Definir, documentar y formalizar dentro del procedimiento de clasificación de activos de información, los siguientes criterios: • Tipificación de escalas de clasificación, ejemplo (Confidencial, interno y público). • Responsabilidades, quienes serían los propietarios de la información, quienes los custodios y quienes deben monitorear el cumplimiento de este procedimiento con las actividades asociadas. • Directrices para el etiquetado de la información de acuerdo con el nivel de clasificación. • Directrices para el manejo de la información de acuerdo con el nivel de clasificación. • Definición de esquemas de control de acuerdo con el nivel de clasificación. El inventario deberá ser actualizado por lo menos una vez al año o cada vez que se presenten cambios significativos en la organización

Anexo 3.5

DSS04 – Gestionar la Continuidad

Calificación		2
Código	**Hallazgo**	**Recomendación**
DSS04.04	**Falta de ejecución de pruebas de continuidad al proceso de mesa de ayuda** La compañía ha establecido un cronograma de pruebas al proceso de mesa de ayuda, sin embargo, al presente año no se ha ejecutado ninguna prueba del proceso de mesa de ayuda. Lo anterior podría ocasionar, demora en la activación del plan de contingencia por inconvenientes que se presentaron por no realizar las pruebas previas.	Publicar el cronograma de pruebas. Realizar las pruebas dentro del tiempo planeado en el cronograma. Incluir a la mayor parte de funcionarios, responsables, directivos en las pruebas para que todos sepan las actividades que se deben realizar. Establecer planes de acción y de mejora que permitan asegurar que el centro alterno y el plan de contingencia estará disponible. Realizar seguimiento continuo a los planes implementados.

Calificación		2
Código	**Hallazgo**	**Recomendación**
DSS04.06	**Falta de formación a las partes implicadas para la contingencia** La compañía ha establecido un plan de continuidad del negocio, ha definido un cronograma de pruebas al proceso de mesa de ayuda, sin embargo, por la falta de ejecución de pruebas aún se desconocen las partes implicadas en caso de algún evento que haga que se active el plan. Lo anterior podría ocasionar, ineficiencia en la puesta en ejecución del BCP por desconocimiento de los colaboradores en la actividad que deben desempeñar.	Publicar el cronograma de pruebas. Incluir a la mayor parte de funcionarios, responsables, directivos en las pruebas para que todos sepan las actividades que se deben realizar. Con la ayuda de la ejecución de las pruebas se pueden identificar otros funcionarios que no se tenían en cuenta en la planeación

Calificación		2
Código	**Hallazgo**	**Recomendación**
DSS04.08	**Ausencia de revisiones post-reanudación de continuidad del negocio.**	Publicar el cronograma de pruebas.

Calificación		2
Código	**Hallazgo**	**Recomendación**
	Si bien, la compañía ha establecido un plan, un cronograma para la continuidad del negocio para el proceso de mesa de ayuda, la falta de ejecución de pruebas no hace posible identificar que escenarios y que actividades se deben de hacer luego de la reanudación del servicio. Lo anterior podría ocasionar, fallo en el volumen de datos y en el tiempo en que se puede realizar la recuperación, por falta de actualización de estos objetivos	Realizar las pruebas dentro del tiempo planeado en el cronograma. Establecer planes de acción y de mejora que permitan asegurar que el centro alterno y el plan de contingencia estará disponible. Realizar seguimiento continuo a los planes implementados.

Anexo 3.6

DSS05 - Gestionar servicios de seguridad.

Calificación		1
Código	**Hallazgo**	**Recomendación**
DSS05.01	**Soporte Windows Server 2003** En la página oficial de Microsoft se informó, que desde el 14 de julio de 2015 se finalizó el soporte técnico para Windows Server 2003. Dentro de los servidores que se tiene para el proceso de mesa de ayuda se encuentran en ambiente productivo, servidores con el sistema operativo de Windows Server 2003. Estos servidores no cuentan con plan de migración en la actualidad y los antivirus que tiene la compañía no son compatibles con este sistema operativo. Lo anterior podría ocasionar, robo de información, equipos no actualizados a tiempo y en riesgo de infección de virus	Establecer un plan de migración de estos servidores a una versión que cuente con el soporte técnico por parte del proveedor.