Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de proyecto de investigación aplicada 2

Modelo de evaluación de la capacidad de gestión de la Seguridad de la Información en una organización

Trejos Sosa David Guillermo

Mayo, 2018

Declaración Jurada

Por medio de la presente, declaro que el trabajo titulado *Modelo de evaluación de la capacidad de gestión de la Seguridad de la Información en una organización* presentado a la Universidad Cenfotec es realizado por mi persona y no ha sido publicado previamente.

En igual sentido, declaro que el trabajo de investigación es original y que todos los datos y referencias a trabajos ya publicados con anterioridad han sido debidamente identificados e incluidos en la bibliografía.

Afirmo, asimismo, que los materiales presentados no se encuentran protegidos por derechos de autor; y en caso de que así lo estuvieran, me hago responsable de cualquier litigo o reclamo relacionado con la violación de derechos de propiedad intelectual, exonerando de toda responsabilidad a la Universidad Cenfotec.

Finalmente, se indica que este trabajo es de carácter confidencial y deben considerarse las medidas necesarias para la protección de la información de la organización en donde se aplicó la metodología.

Autorizo a la Universidad Cenfotec a utilizar dicho trabajo para reproducirlo, editarlo, distribuirlo, exhibirlo y comunicarlo en el país y en el extranjero, por medios impresos, electrónicos, Internet o cualquier otro medio, para propósitos académicos y sin fines de lucro, una vez cumplidos los 3 años de restricción por confidencialidad.

David Guillermo Trejos Sosa

Firma:

Dedicatoria

A:

Dios, por enseñarme que la vida no es fácil y por las experiencias que han enseñado valores para poder salir adelante con esta maestría tan difícil.

Mi madre, que sin ella no hubiera logrado ningún objetivo académico ni laboral, porque ella ha creído en mí y en los buenos y malos momento siempre me apoyó. Mamá gracias por darme una carrera más, todo esto te lo debo a ti.

Agradecimientos

A mi tutor, por la gran ayuda para culminar este proyecto y todas las recomendaciones para culminar este proyecto con eficiencia y eficacia.

A mi amigo Luis Vargas por la ayuda incondicional cuando la necesite, y los consejos importantes para salir adelante.

A mi hermano mayor Luis Enrique por el apoyo que necesité para poder llevar a cabo esta meta tan importante.

A mi jefe Alejandro por el apoyo brindado durante los dos años y medio que duró la maestría, además de las técnicas que me facilitó para realizar este trabajo.

A mi familia en general por su apoyo y buenos deseos.

A mi pareja y mi hijo por ser la inspiración para salir adelante con este objetivo de vida.

Hoja de aprobación del proyecto

Tabla de contenido

Contenido

Índice de cuadros

Índice de ilustraciones

Lista de palabras claves (palabras técnicas)

COBIT: por las siglas en idioma inglés de *Control Objectives for Information and Related Technologies*; es una propuesta de ISACA de mejores prácticas relacionadas con TI.

ISO 27002: Norma de seguridad de la información, que presenta los controles.

ISACA es el acrónimo de Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información), una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información.

Riesgo: Evento que puede repercutir en algún área del negocio.

SBR: Supervisión basada en riesgos.

Supen: Superintendencia de Pensiones.

TI: Tecnologías de información.

TIC: Tecnologías de información y comunicación

Resumen ejecutivo

Como una necesidad de las organizaciones de tener una mayor visibilidad de los procesos de seguridad de la información, se creó una metodología que mide la capacidad de gestión de seguridad de la información usando como referencia las normas ISO/IEC 27001 y Cobit 5 para la seguridad de la información.

Se realizó una comparación entre ambas normas y se utilizaron los controles que más se adecuaban para que el resultado de la evaluación fuera el más preciso.

Una vez escogidos los procesos de evaluación, se creó la metodología de cálculo basada en riesgos para que esta pueda recibir como entrada los datos necesarios y que de manera cuantitativa muestre el nivel de capacidad de gestión según la evaluación de cada proceso de control.

Esta evaluación se aplicó en los procesos de la Operadora de Pensiones complementarias de la Caja Costarricense del Seguro Social, y el resultado se utilizó como insumo para que la comisión de tecnologías de información de la Operadora pudiera realizar su perfil tecnológico basándose en las calificaciones.

CAPÍTULO I: INTRODUCCIÓN

1.1. Introducción

En los últimos 18 años las empresas e instituciones han cambiado de forma drástica la manera en que comparten la información, conectan a las personas, brindan servicios en línea y realizan transacciones, evidenciando un crecimiento tecnológico que va paralelo a los inevitables ataques cibernéticos realizados por delincuentes informáticos. Para poder prevenir ataques informáticos, es fundamental gestionar la seguridad de la información de manera integral y que el crecimiento de la misma vaya de la mano con los avances tecnológicos.

Para poder tener una gestión exitosa de la seguridad de la información es necesario crear una cultura de seguridad en los habitantes costarricenses. Este cambio de cultura no solo debe evidenciarse en la población, el mismo debe ser liderado por las entidades financieras, instituciones públicas y privadas, que deben garantizar que el manejo los datos críticos y sensibles se gestiona de forma segura.

Debe quedar claro que la seguridad informática y la seguridad de la información son campos complementarios, esto por porque la seguridad informática es solo una pequeña parte del amplio mundo de la seguridad de la información, este trabajo de investigación aplicada se enfocará principalmente en la gestión de la seguridad de la información, y cómo se debe desarrollar en las instituciones y empresas específicamente la Operadora de Pensiones Complementarías de la CCSS.

El desarrollo de la investigación utilizará como referencia los estándares ISO 27001 y COBIT 5, aprovechando los diferentes controles que estos proponen, para definir las mejores prácticas que deberían utilizarse para asegurar que la gestión de la seguridad de la información se está realizando de manera satisfactoria en la Operadora de Pensiones Complementarías de la CCSS.

De igual manera, con la investigación de las mejores prácticas se desarrollará una metodología que permita evaluar la capacidad de gestión de seguridad de la información que tiene una institución o empresa y aplicarla para observar los resultados reales que está va a facilitar. La aplicación de la metodología se aplicará en la Operadora de Pensiones Complementarias de la CCSS.

1.2. Planteamiento del tema de estudio

El uso de las nuevas tecnologías en las instituciones y empresas del país ha facilitado la oferta de los servicios que estas ofrecen a sus clientes y afiliados, creando así una necesidad de regular estas actividades para proteger la confidencialidad, integridad y disponibilidad de los datos.

Para cubrir parte de la necesidad de regular a las instituciones y empresas que utilizan sus plataformas de servicios por medio de tecnologías de información, el *Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF)* creó el *REGLAMENTO GENERAL DE GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN (**RGGTI**)*, el 17 de abril de 2017, establece los requerimientos mínimos para gestionar las tecnologías de la información por parte de las entidades supervisadas y reguladas del sistema financiero costarricense.

Adicionalmente para complementar el uso de las tecnologías en el país se creó la, *LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES Ley n.º 8968,* cuyo objetivo es garantizar a cualquier persona el respeto de sus derechos fundamentales en el manejo de sus datos personales y la *Ley 9048 Delitos Informáticos y Conexos* para todos los costarricenses que quieran violentar la ley utilizando medios informáticos.

Con el reglamento indicado anteriormente, la Ley ***8968 Protección de la Persona frente al tratamiento de sus Datos Personales y su Reglamento*** y la Ley **9048 Delitos Informáticos y Conexos**, se busca asegurar la confidencialidad, integridad, disponibilidad y auditabilidad de la información, a través de la implementación de un *Sistema de Gestión de Seguridad de la Información* (SGSI) que deben crear y mantener todas las instituciones reguladas y supervisadas.

Actualmente para poder evaluar la capacidad de gestión del SGSI de las instituciones, no existe ninguna metodología que se enfoque en este objetivo. Esto porque se evalúa la seguridad informática como un todo y no específicamente la seguridad de la información como tal, que es un campo más amplio.

Es por este motivo que se plantea la creación de una metodología cuyo objetivo es ayudar a las instituciones a medir su capacidad de gestión real de la seguridad de la

información y adicionalmente para que puedan realizar sus propias evaluaciones y mitigar cualquier riesgo crítico que sea identificado.

1.3. Antecedentes

El tema de seguridad de la información en Costa Rica no ha alcanzado el grado de capacidad y entendimiento necesario para desarrollarlo de manera adecuada y comprender las necesidades que se requieren para poder cumplir con las mejores prácticas de seguridad de la información según la normativa nacional.

Muchos expertos de seguridad en tecnologías de información no logran distinguir la diferencia entre la *seguridad de la información* y la *seguridad informática*, que son dos conceptos complementarios, pero en su implementación son diferentes. Esta metodología podrá ser un soporte para los auditorías internas y externas de las organizaciones.

1.4. Formulación del problema

El RGGTI, y la Ley DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES Ley n.º 8968, indican la línea que deberán seguir las instituciones para proteger la información confidencial.

El RGGTI solicita contar con un Sistema de Gestión de Seguridad de la Información; actualmente muchas organizaciones no tienen claro cómo desarrollar una metodología o herramienta que logre medir la capacidad de gestión de la seguridad de la información.

1.5. Justificación

Los estándares a nivel mundial de seguridad informática y seguridad de la información emitidos por ISACA(info) son referentes a nivel mundial, por este motivo el Consejo Nacional de Supervisión del Sistema Financiero propone el RGGTI el

cual es de aplicación obligatoria por todas las instituciones reguladas por SUGEF, SUGEVAL, SUGESE y SUPEN.

El RGGTI, indica en los siguientes lineamientos lo siguiente:

- 2.12 Gestionar la Seguridad,

  > *Definir, operar y supervisar un sistema para la gestión de la seguridad de la información. Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa (SNP)*

- 4.5 Gestionar Servicios de Seguridad,

  > *Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad. Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.*

Para poder cumplir estos dos lineamientos la mayoría de las instituciones primero necesitan medir la capacidad de gestión que tienen y de ahí formular planes para minimizar los riesgos encontrados para poder cumplir de manera adecuada con la protección de la información.

Es por lo anterior que existe la necesidad de crear una metodología que pueda medir la capacidad de gestión de la seguridad de la información.

1.6. Objetivos del proyecto

1.6.1. Objetivo General

Proponer un modelo que permita evaluar el umbral de riesgo de la seguridad de la información en la Operadora de Pensiones Complementarias de la Caja Costarricense del Seguro Social (OPC CCSS).

1.6.2. Objetivos específicos

Para desarrollar efectivamente el objetivo general, es necesario trazar metas específicas. Dichas metas se traducen en los siguientes objetivos específicos:

- Identificar el estado actual de los procesos de seguridad de la información.
- Determinar las áreas que deben cubrir los aspectos de la seguridad de la información en una organización.
- Investigar usando como referencia las mejores prácticas y normas internacionales, procesos que permitan evaluar el nivel de capacidad de seguridad de la información.
- Desarrollar un modelo para evaluar el nivel de capacidad de seguridad de la información en la OPC CCSS.
- Aplicar el modelo elaborado en algunos de los componentes de seguridad de la información de la OPC CCSS.

1.7. Alcances y Limitaciones

1.7.1. Alcance

Este proyecto de investigación aplicada creará una metodología para medir el nivel de capacidad de gestión de Seguridad de la Información en la OPC CCSS, utilizando la norma ISO 27001 y COBIT 5.

1.7.2. Limitaciones

El tiempo de aplicación de la metodología no es suficiente para cubrir todas las áreas que la seguridad de la información requiere, por lo que la aplicación de la metodología se realizará solo en algunos puntos y no en su totalidad.

Los resultados de la aplicación del modelo de medición de capacidad de gestión de la seguridad de la información, no se publicarán en este documento dado que son de carácter confidencial.

CAPÍTULO II: MARCO TEÓRICO

2.1. Marco situacional

El desarrollo teórico permite retroalimentar al lector, sobre la guía documental y teórica que se utilizó como base para el desarrollo del proyecto. La intención principal es la de facilitar la comprensión de los fundamentos conceptuales que sirvieron como base para su formulación.

La Operadora de Pensiones Complementarias de la Caja Costarricense del Seguro Social fue creada según los artículos 39, 44 y 74 de la Ley de Protección al Trabajador, donde se determina que la Caja Costarricense de Seguro Social está obligada a crear una Operadora de Pensiones, a efecto de que administre un fondo de capitalización laboral, que proteja a los trabajadores que se encuentren en los supuestos de los artículos 39 y 44 de la Ley.

La OPC CCSS, es supervisada por la Superintendencia de Pensiones, según lo detalla el artículo 42 de la Ley Protección al Trabador y en el artículo 36 de la Ley del Régimen Privado de Pensiones Complementarias.

La OPC CCSS debe cumplir con lo estipulado por la Superintendencia de Pensiones, para poder administrar los fondos de pensiones de los costarricenses.

2.1.1. Misión de la OPC CCSS

Administramos su futuro hoy, con servicios de calidad, en procura del mayor bienestar de nuestros clientes.

2.1.2. Visión de la OPC CCSS

Ser su mejor Operadora de Fondos de Pensiones en rentabilidad, servicio y seguridad para su futura pensión.

2.1.3. Funciones de la OPC CCSS

Administrar el aporte mensual que realiza el patrono equivalente al 3% del salario del trabajador, más los rendimientos obtenidos por la gestión de Inversiones que hace el área de inversiones de la OPC CCSS.

Entregar el fondo de capitalización laboral al afiliado cuando este lo solicite por terminar la relación laboral con su patrono ya sea por renuncia, despido o pensión. De igual manera durante la relación laboral ininterrumpida con el mismo patrono, cada cinco años y por fallecimiento, entregarlo a los beneficiarios designados.

Administrar el fondo obligatorio creado para complementar la pensión que la persona recibirá al pensionarse o jubilarse según lo aportado del 1% trabajador y el 3.25% del patrono y los rendimientos que se generen por la gestión de Inversiones que realice la OPC CCSS.

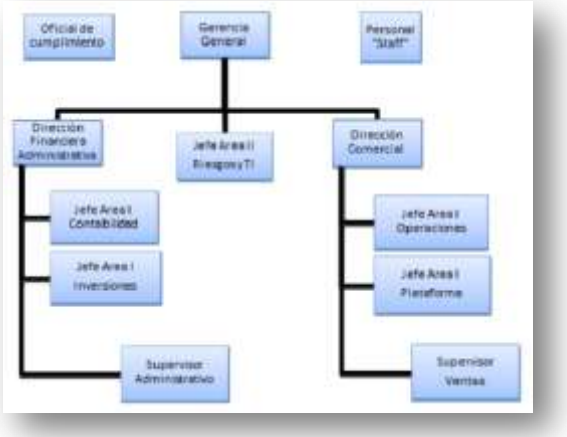
Entregar el fondo obligatorio de pensión complementaria al afiliado, cuando este cumpla la edad establecida por la CCSS.

2.1.4. Tipo de Estructura

La OPC CCSS tiene una estructura organizacional que determina con claridad cada una de las diferentes áreas existentes y sus respectivas jerarquías.

A continuación, se presenta la organización funcional de la Operadora de Pensiones:

Figura No.1: Organigrama Institucional



2.2. Marco Teórico

Dado que el objetivo principal de esta investigación es evaluar la capacidad de gestión de Seguridad de Información en la *OPC CCSS*, será necesario plantear algunos conceptos para poder apoyar la lectura de esta investigación.

Se conocerán los conceptos básicos necesarios para el entendimiento del desarrollo de este proyecto de investigación aplicada.

Se describirán aspectos relevantes de los estándares de Seguridad de la Información y se definirán los términos y las etapas de los estándares que se utilizarán como referencia para el modelo. Por último, se mostrará cómo funcionará la metodología de medición basada en riesgos.

2.2.1. Seguridad de la Información

La seguridad de la información es el conjunto controles asociados a los procesos de la organización que permiten resguardar y proteger la información para mantener la confidencialidad, integridad, disponibilidad y auditabilidad.

Confidencialidad: es la propiedad que previene la divulgación de la información y los no autorizados. De esta manera se busca asegurar el acceso a la información únicamente por los usuarios que cuenten con la debida autorización.

Disponibilidad: es una característica, cualidad o condición de la información de encontrarse a disposición de los elementos que deban acceder a ella, sean personas, procesos o aplicaciones; en general, la disponibilidad es el acceso a la información en el momento preciso y solicitado.

Integridad: es una característica que busca asegurar que la información y los datos que la proveen estén libres de modificaciones no autorizadas; manteniendo la información correcta y veraz.

2.2.2. Estándares internacionales de Seguridad de la Información

Toda la información en cualquiera de sus estados, ya sean físicos o digitales, representan parte de los activos más importantes de una organización. Lograr mantener y mejorar la seguridad de la información es esencial para alcanzar el éxito, lograr continuidad y mantener una ventaja competitiva.

Cuando se implanta un SGSI, la organización logra plantear objetivos de seguridad precisos y muestra una evaluación de los riesgos a los que se encuentra expuesta la información.

Es por estos motivos que, varias organizaciones a nivel mundial crean estándares que apoyen a las organizaciones en materia de seguridad.

International Organization for Standardization International Electrotechnical Commission, *ISO/IEC*, es la organización que se encarga de crear y actualizar los estándares que proporcionan un marco de gestión de la seguridad de la información utilizable para cualquier tipo de organización, privada o pública, pequeña o grande.

Information Systems Audit and Control Association, *ISACA*, es la asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información.

ISO/IEC 27001 es un estándar para la seguridad de la información aprobado y publicado como estándar internacional en octubre de 2005 por *International ISO/IEC*, y especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un SGSI.

COBIT 5, tiene tres procesos específicos los procesos APO13 Gestionar la seguridad, DSS04 Gestionar la continuidad y DSS05 Gestionar los servicios de seguridad proporcionan una guía básica acerca de cómo definir, operar y monitorizar un SGSI. ISACA asume que la seguridad de la información se encuentra presente a lo largo de toda la empresa, con aspectos de seguridad dentro de cada actividad y proceso realizado.

Por lo tanto, ISACA proporciona la nueva guía para el gobierno y la gestión corporativa de la seguridad de la información, "***COBIT 5 para Seguridad de la Información".***

Para esta investigación se utilizarán como referencia la norma *ISO/IEC 27001* y la nueva guía se ISACA, *COBIT 5 para Seguridad de la Información.*

2.2.3. Evaluación de riesgos

Riesgo es el impacto y la probabilidad de que una amenaza pueda afectar de manera adversa la consecución de los objetivos.

En la norma ISO/IEC 27002 "Código de buenas prácticas para la gestión de la seguridad de información" en su control 41 Evaluación de riesgos de seguridad indica que se deben de identificar, cuantificar y priorizar los riesgos según los criterios establecidos para la aceptación del riesgo y según los objetivos relevantes para la organización. Los resultados de dichas evaluaciones deberían de guiar y determinar las acciones y prioridades para la dirección de cara a la gestión de los riesgos.

La evaluación de riesgos incluye la aproximación sistemática para estimar la magnitud de los riesgos (análisis de riesgos) y el proceso de comparación de los riesgos estimados contra los criterios de riesgos para determinar la importancia de los riesgos.

2.2.4. COBIT

Control Objetives for Information and related Tecnology, COBIT, por sus siglas en inglés es, "Objetivos de Control para Tecnología de Información" y según IT Governance Institute,

"COBIT es un marco de referencia globalmente aceptado para el gobierno de TI basado en estándares de la industria y las mejores prácticas. Una vez implementado, los ejecutivos pueden asegurarse de que se ajusta de manera eficaz con los objetivos del negocio y dirigir mejor el uso de TI para obtener ventajas comerciales.

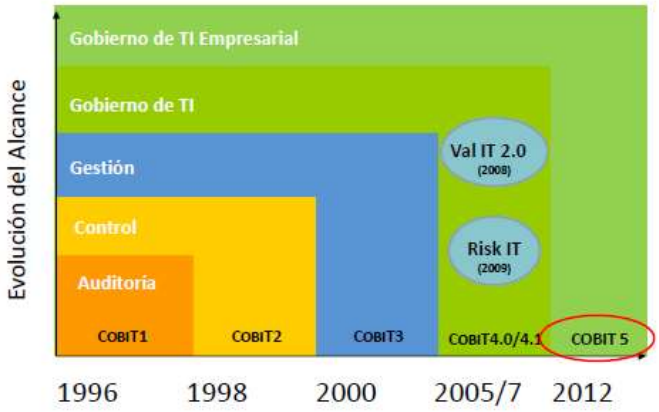
COBIT brinda un lenguaje común a los ejecutivos de negocios para comunicar las metas, objetivos y resultados a los profesionales de auditoría, informática y otras disciplinas.”

COBIT detalla las Guías de Gerencia que incluyen:

- **Factores críticos de éxito** que son acciones importantes para la administración y control de los procesos de TI.
- **Indicadores clave de desempeño** que proporcionarán medidas de éxito que permitirán a la gerencia conocer si un proceso de TI está alcanzando los requerimientos de negocio.
- **Medidas Comparativas** que definen los niveles de madurez a ser utilizadas por la gerencia para determinar el nivel actual de madurez de TI en la empresa; además para programar el nivel de madurez que se desea lograr; por lo demás incluye también una función de sus riesgos y objetivos; todo lo anterior proporciona una base de comparación de las prácticas de control de TI de la organización contra empresas similares o la industria.

El proyecto COBIT salió a la luz el año 1995, con el fin de crear un producto global que pudiese tener un impacto sobre el campo de visión de los negocios, así como sobre los controles de los sistemas de información implantados. En la ilustración siguiente se muestra la evolución que ha tenido COBIT desde su nacimiento.

Figura No.2: Evolución de COBIT, según ISACA



La primera edición del COBIT, fue publicada en 1996 y fue vendida en 98 países de todo el mundo. Esta primera versión fue orientada a apoyar los procesos de auditoría. Conceptualmente la auditoría, en general, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y cumple las condiciones que le han sido prescritas. En esta primera versión de COBIT pretende ser una herramienta de trabajo para el auditor de TI donde detallará a través de objetivos de control los aspectos evaluables de las tecnologías de información desde el punto de vista auditor de TI.

La segunda edición publicada en abril de 1998 desarrolla y mejora lo que poseía la anterior mediante la incorporación de un mayor número de documentos de referencia fundamentales, nuevos y revisados de objetivos de control de alto nivel, intensificando las líneas maestras de la auditoría; además introdujo un conjunto de herramientas de implementación, así como documentación completamente organizada de todos los contenidos de la gestión de TI.

Esta segunda versión su objetivo principal es controlar diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos,

estándares y normas fijados por la Dirección de la Organización y/o la Dirección de Informática, así como los requerimientos legales. La misión del control interno informático es asegurarse de que las medidas que se obtienen de los mecanismos implantados por cada responsable sean correctas y válidas.

El Control Interno Informático suele ser un órgano dotado de personas y medios materiales cuyos objetivos del Control Interno Informático, son los siguientes:

- Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- Asesorar sobre el conocimiento de las normas.
- Colaborar y apoyar el trabajo de Auditoría Informática, así como de las auditorías externas al grupo.
- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informático, lo cual no debe considerarse como que la implantación de los mecanismos de medida y la responsabilidad del logro de esos niveles se ubique exclusivamente en la función de Control Interno, sino que cada responsable de objetivos y recursos es responsable de esos niveles, así como de la implantación de los medios de medida adecuados.

En el año 2000, ISACA presenta la versión 3 de COBIT donde se resalta que la administración efectiva de la información y de la Tecnología de Información relacionada se convierte en un elemento crítico para el éxito y la supervivencia de las organizaciones.

Para muchas organizaciones, la información y la tecnología que la soporta, representan los activos más valiosos de la empresa. Es más, en nuestro competitivo y rápidamente cambiante ambiente actual, la Gerencia ha incrementado sus expectativas relacionadas con la entrega de servicios de TI. Por lo tanto, la administración requiere

niveles de servicio que presenten incrementos en calidad, en funcionalidad y en facilidad de uso, así como un mejoramiento continuo y una disminución de los tiempos de entrega; al tiempo que demanda que esto se realice a un costo más bajo.

A diferencia que las dos versiones anteriores cuya vida útil fue de dos años cada una, COBIT versión 3 estuvo en el mercado por 5 años, consolidando su uso en el medio industrial con mayor amplitud.

En el año 2005, ISACA saca a la luz COBIT en su versión 4, esta versión asegura que las TI estén alineadas con los objetivos de negocio, sus recursos sean usados responsablemente y sus riesgos administrados de forma apropiada. El mayor cambio de esta versión es que tiene un enfoque basado en procesos. Para esto COBIT propuso un marco de trabajo o alcance 37 controles divididos en cuatro dominios:

- **PLANEAR Y ORGANIZAR**. Cubre las estrategias y de la organización, identificando la manera en que las TI pueda contribuir al logro de los objetivos del negocio.
- **ADQUIRIR E IMPLEMENTAR.** Las soluciones de las TI necesitan ser identificadas, desarrolladas o adquiridas, así como la implementación e integración en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes son necesarios para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.
- **ENTREGAR Y DAR SOPORTE.** Se preocupa de la entrega de los servicios requeridos, la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales.
- **MONITOREAR Y EVALUAR.** Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del Gobierno.

Para el año 2012 se presenta a la comunidad tecnológica la versión 5 de COBIT que provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus

objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. Además, esta versión se presenta de un modo genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público.

COBIT 5 declara que las empresas existen para crear valor para sus partes interesadas; para esto los negocios deben de:

- Crear beneficios financieros para empresas comerciales o de servicio público para las entidades de gobierno.
- Optimización de riesgo, administrando los eventos que podrían afectar la operativa de la organización.
- Optimizando los recursos, de tal forma que estos sean usados eficiente y eficazmente en la organización.

Para el logro de los objetivos anteriores COBIT 5 divide su marco de trabajo o alcance en cinco dominios:

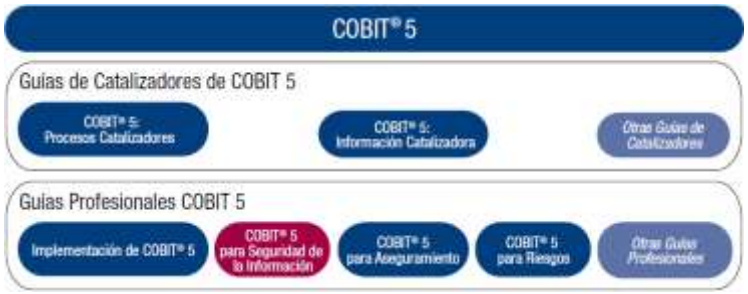
- EVALUAR, ORIENTAR Y SUPERVISAR. Abarca los procesos de gobierno de tal forma que se cumplan con los objetivos de las partes interesadas (entrega de valor, optimización del riesgo y de recursos) e incluye prácticas y actividades orientadas a evaluar opciones estratégicas, proporcionando la dirección de TI y supervisando las salidas de cada proceso.
- ALINEAR, PLANIFICAR Y ORGANIZAR. Cubre las estrategias y de la organización, identificando la manera en que las TI pueda contribuir al logro

de los objetivos del negocio. La visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada.

- CONSTRUIR, ADQUIRIR E IMPLEMENTAR. Las soluciones de las TI necesitan ser identificadas, desarrolladas o adquiridas, así como la implementación e integración en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes son necesarios para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.
- ENTREGAR Y DAR SERVICIO Y SOPORTE**.** Se preocupa de la entrega de los servicios requeridos, la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales.
- SUPERVISAR, EVALUAR Y VALORAR**.** Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del Gobierno.

COBIT 5 para Seguridad de la Información, basado en el marco de COBIT 5, se enfoca en la seguridad de la información y proporciona una guía más detallada y práctica para los profesionales de seguridad de la información y otras partes interesadas a todos los niveles de la empresa.

Figura No.3: Familia de guías de COBIT 5



2.2.4.1. Catalizadores de COBIT 5

COBIT 5 para seguridad de la información se basa en los mismos principios que el marco de COBIT 5.

1. Satisfacer las necesidades de las partes interesadas.
2. Cubrir la empresa de extremo a extremo.
3. Aplicar un marco de referencia único integrado.
4. Hacer posible un enfoque holístico.
5. Separar el gobierno de la gestión.

Figura No.4: Principios de COBIT 5

2.2.4.2. Satisfacer las necesidades de las partes interesadas

Las empresas deben crear valor para sus partes interesadas, incluidas las partes interesadas de seguridad de la información; y como cada empresa tiene objetivos diferentes, se debe utilizar la metodología de cascada de metas para personalizar COBIT 5 al contexto de la organización.

COBIT 5 para Seguridad de la Información, habla de metas específicas de seguridad de la información para los procesos como apoyo a las necesidades de la organización.

2.2.4.3. Cubrir la empresa de extremo a extremo

COBIT 5 para Seguridad de la Información cubre a todas las partes interesadas, funciones y procesos que forman parte de la empresa y son relevantes para la seguridad de la información.

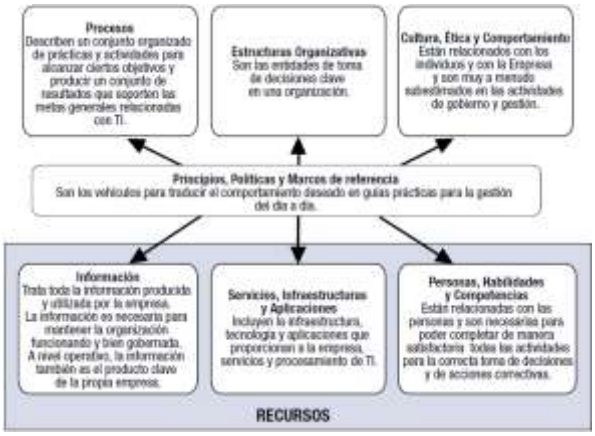
2.2.4.4. Aplicar un marco de referencia único integrado

COBIT 5 para Seguridad de la Información reúne conocimientos previamente distribuidos entre los diferentes marcos y modelos de ISACA (COBIT, BMIS, Risk IT, Val IT) con guías de otros importantes estándares relacionados con la seguridad de la información tales como la serie ISO/IEC 27000, el Estándar de Buenas Prácticas para Seguridad de la Información de ISF y el SP800-53A del U.S. National Institute of Standards and Technology (NIST).

2.2.4.5. Hacer posible un enfoque holístico

La Seguridad de la Información requiere de un enfoque holístico que tenga en cuenta varios componentes que interactúan. Se define un conjunto de catalizadores para apoyar la implementación de un sistema de gobierno y gestión global para las TI y la seguridad de la información. Estos catalizadores influyen individual y colectivamente en que se cumplan los objetivos planteados por el gobierno corporativo. Se necesita el siguiente modelo de interacción holístico:

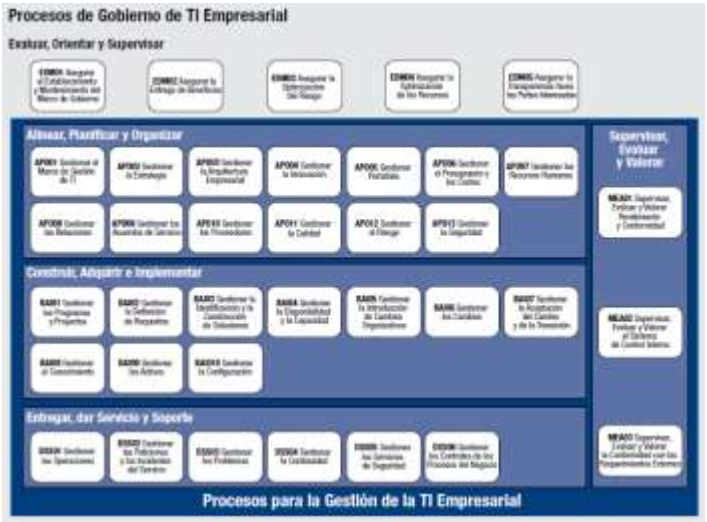
Figura No.5: Interacción holística de los Catalizadores de COBIT 5



2.2.4.6. Separar el gobierno de la gestión

En la práctica, los diferentes roles del gobierno y gestión de la seguridad de la información se hacen visibles mediante el modelo de procesos de COBIT 5, que incluye procesos de gestión y procesos gobierno, cada grupo con sus propias responsabilidades.

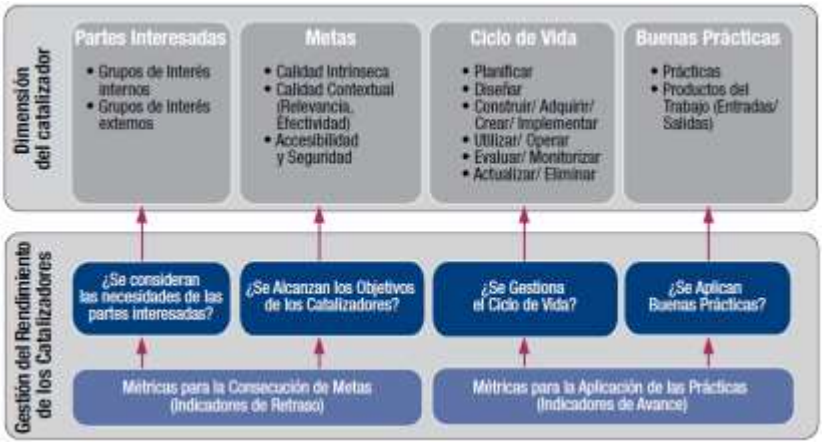
Figura No.6: Modelo de referencia de procesos de COBIT 5



2.2.4.7. Uso de catalizadores de COBIT 5 para implantar la seguridad de la información.

Se aplican los catalizadores de COBIT 5 para implantar un efectivo y eficiente gobierno y gestión de la seguridad de la información en la empresa. Estos catalizadores tienen un conjunto de dimensiones comunes, como permitir a una entidad manejar sus complejas interacciones y facilitar resultados exitosos de los catalizadores.

Figura No.7: Catalizadores COBIT 5



COBIT 5 para Seguridad de la información proporciona orientación específica en relación con todos los catalizadores:

1. Las políticas, principios y marcos de referencia de seguridad de la información.
2. Los procesos, incluyendo detalles y actividades específicos de seguridad de la información.
3. Las estructuras organizativas específicas de seguridad de la información.

4. En términos de cultura, ética y comportamiento, los factores determinantes para el éxito del gobierno y la gestión de la seguridad de la información.

5. Los tipos de información específicos de la seguridad de la información para permitir el gobierno y la gestión de la seguridad de la información en la empresa.

6. Las capacidades de servicio necesarias para proporcionar seguridad de la información y las funciones relacionadas con la empresa.

7. Las personas, habilidades y competencias específicas para seguridad de la información.

2.2.5. ISO/IEC 27001

Norma internacional que ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI).

2.2.5.1. Enfoque basado en procesos

La norma promueve la adopción de un enfoque basado en procesos, para establecer el SGSI de la organización; e insta a sus usuarios a hacer énfasis en la importancia de:

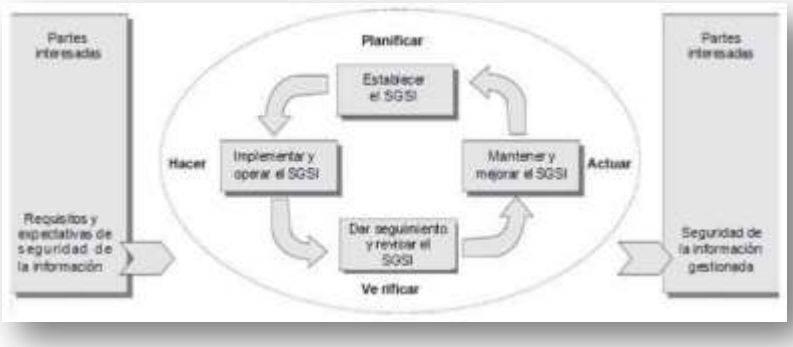
a) comprender los requisitos de seguridad de la información del negocio y la necesidad de establecer la política y objetivos para la seguridad de la información;

b) implementar y operar controles para manejar los riesgos de seguridad de la información de una organización en el contexto de los riesgos globales del negocio de la organización;

c) realizar el seguimiento y la revisión del desempeño y eficacia del SGSI

d) la mejora continua basada en la medición de objetivos.

Figura No.8: Modelo PHVA aplicado a los procesos de SGSI



Planificar (establecer el SGSI) Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información del SGSI, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.

Hacer (implementar y operar el SGSI) Implementar y operar la política, los controles, procesos y procedimientos del SGSI.

Verificar (dar seguimiento y revisar el SGSI) Valorar y, en donde sea aplicable, medir el desempeño del proceso contra la política, los objetivos, la experiencia práctica del SGSI y reportar los resultados a la dirección, para su revisión.

Actuar (mantener y mejorar el SGSI) Emprender acciones correctivas y preventivas basadas en los resultados de la auditoría interna del SGSI, la revisión por la dirección u otra información pertinente, para lograr la mejora continua del SGSI.

2.2.5.2. Definiciones para complementar la seguridad de la información según ISO/IEC

Evento de seguridad de la información: ocurrencia de un estado identificado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o la falla de salvaguardas, o una situación previamente desconocida que pueda ser relevante para la seguridad.

Incidente de seguridad de la información: evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Riesgo residual: riesgo restante después del tratamiento del riesgo.

Aceptación del riesgo: decisión de asumir un riesgo.

Análisis de riesgo: uso sistemático de la información para identificar las fuentes y estimar el riesgo.

Evaluación del riesgo: proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Gestión del riesgo: actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

Tratamiento del riesgo: proceso de selección e implementación de medidas para modificar el riesgo.

2.2.5.3. Sistema de gestión de seguridad de la información

La organización debe establecer, implementar, operar, dar seguimiento, revisar, mantener y mejorar un SGSI documentado, en el contexto de las actividades globales del negocio de la organización y de los riesgos que enfrenta.

- **Establecimiento del SGSI**: La organización deberá,
    - Definir el alcance y límites del SGSI según las características del negocio.
    - Definir una política de SGSI.
    - Definir el enfoque de la organización para la valoración del riesgo.
    - Identificar los riesgos.
    - Analizar y evaluar los riesgos.
    - Identificar y evaluar las opciones para el tratamiento de los riesgos.
    - Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.
    - Obtener la aprobación de la dirección sobre los riesgos residuales propuestos.
    - Obtener autorización de la dirección para implementar y operar el SGSI.
    - Elaborar una Declaración de Aplicabilidad.
- **Implementación y operación del SGSI**: La organización deberá,
    - Formular un plan para el tratamiento del riesgo.
    - Implementar el plan de tratamiento del riesgo.
    - Definir cómo medir la eficacia de los controles.
    - Implementar programas de formación y de toma de conciencia.
    - Gestionar la operación del SGSI.

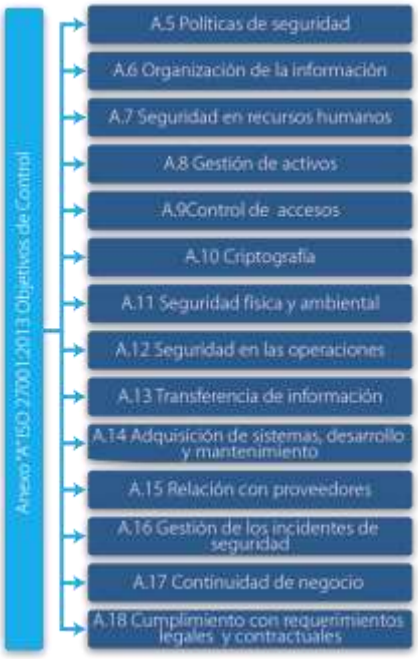
- Gestionar los recursos del SGSI.
- Implementar procedimientos para dar respuesta oportuna a los incidentes de seguridad.

- **Seguimiento y revisión del SGSI**: La organización deberá,
  - Ejecutar procedimientos de seguimiento y revisión.
  - Emprender revisiones regulares de la eficacia del SGSI.
  - Medir la eficacia de los controles.
  - Revisar las evaluaciones de los riesgos a intervalos planificados.
  - Realizar auditorías internas del SGSI a intervalos planificados.
  - Realizar una revisión por la dirección del SGSI.
  - Actualizar los planes de seguridad.
  - Registrar acciones y eventos que podrían tener impacto en la eficacia o el desempeño del SGSI.
- **Mantenimiento y mejora del SGSI**: La organización deberá,
  - Implementar las mejoras identificadas en el SGS.
  - Emprender las acciones correctivas y preventivas adecuadas.
  - Comunicar las acciones y mejoras a todas las partes interesadas.
  - Asegurarse de que las mejoras logren los objetivos previstos.

2.2.5.4. Objetivos de control ISO/IEC 27001

Los objetivos de control y los controles se han obtenido y alineado directamente con los de la norma ISO/IEC 27002. Estos objetivos no son exhaustivos y la organización puede considerar necesarios otros controles adicionales. Los objetivos de control y controles se deben seleccionar como parte del proceso del SGSI.

Figura No.9: Objetivos de control ISO/IEC 27001



2.2.6.Definición del contexto organizacional interno y externo

Para la definición de un contexto interno en una organización se debe incluir la declaración de la misión, visión, políticas, objetivos, estrategias, metas, roles y responsabilidades, estructura, normativas entre otros.

De igual manera el contexto interno interactúa con el contexto externo, por lo tanto, se deben de considerar aspectos como la competencia, regulaciones legales que apliquen, economía, política, tecnología, cultura y los demás aspectos que se consideren necesarios.

Para el logro de esta parte se deben de utilizar fuentes de información tales como la documentación existente en la organización relacionada con calidad, seguridad, planeación estratégica y continuidad; también las entrevistas con altos mandos, entrevistas con el personal, visitas a instalaciones y las demás que se consideren necesarias.

El objetivo de esta etapa es conocer a la organización y así determinar que puede afectarla a nivel interno y externo. Por otra parte, en esta etapa se define que se requiere proteger y utilizando los recursos actuales, como podría darse esa protección para establecer el nivel de aceptación de riesgo al cual están dispuestos, así como determinar los alcances y limitaciones existentes.

2.2.7. Proceso de auditoría basada en riesgos

La auditoría basada en riesgos consiste en revisar las cosas que realmente importan en su organización. Constituye el desarrollo de los procesos de identificación y evaluación de las potenciales situaciones adversas (riesgos) de una organización, para proveer soluciones de Auditoría TI respecto al logro de los objetivos de la organización y de esta forma brindar un servicio de valor agregado.

Auditoría de sistemas basado en riesgos, se compone de una serie de pasos tal y como se muestra en la siguiente ilustración.

Figura No.10: Fases de una auditoría de sistemas basada en riesgos

2.2.8. Valorización de riesgos

Se deben identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, definidos en el plan estratégico y en el plan anual operativo y adicionalmente analizar el efecto posible de los riesgos identificados, su importancia y la probabilidad de que ocurran.

Establecer los mecanismos necesarios para el funcionamiento adecuado de la valoración del riesgo.

En la valoración se pueden usar técnicas cuantitativas y/o cualitativas para la estimación de riesgos y hay formas variadas de presentación de la información como los vectores de ataque o las matrices, todo depende de los requerimientos, conocimientos, recursos y habilidades del personal de la organización.

CAPÍTULO III: METODOLOGÍA DEL ANÁLISIS DEL PROBLEMA

3.1 Tipo de investigación

Comentario [RAA1]: ¿???????

3.1.1 Finalidad

La metodología a utilizar para alcanzar los objetivos propuestos en este proyecto de investigación aplicada según la clasificación de (Dankhe, 1986), por una parte es descriptiva porque desarrolla una descripción del fenómeno estudiado a partir de sus características y a su vez explorativa porque permite medir, examinar, evaluar y recolectar información de la situación actual de la Seguridad de la Información en la OPC CCSS; además, investigar y proponer una metodología para medir el nivel de capacidad de gestión de seguridad de la información y al aplicar dicha metodología determinar las brechas de seguridad de la información.

3.1.2 Enfoque Sistemático

Este proyecto de investigación aplicada valorará los riesgos de la Seguridad de la Información mediante una metodología que podrá ser de aplicación general para cualquier tipo de organización.

3.1.3 Carácter

El presente proyecto de investigación aplicada, y en sus primeras etapas es de carácter descriptivo y consiste en describir una situación actual, lo que comprende la definición, observación, registro, análisis e interpretación de las condiciones presentes para el momento del estudio, así, la presente investigación pretende estudiar el escenario actual de la seguridad de la información que se aplica a la OPC CCSS.

Adicionalmente, este proyecto será de carácter explicativo; según Carlos Muñoz R. “las investigaciones explicativas son más profundas, y el investigador cuenta con mayores fuentes de información para realizarlas, por lo que la atención *se centra en encontrar los orígenes, causas o factores determinantes del hecho investigado ”*. (Carlos Muñoz R. Fundamentos para teoría general del derecho, primera edición. 1996, p. 108).

La investigación explicativa se desarrolla en forma estructurada abarcando entre sus objetivos la exploración, descripción y correlación; en sí, se trata de encontrar las causas de un determinado suceso o evento y las condiciones como este se manifiesta.

Por esta razón se aplicará este tipo de investigación, aunque en este proyecto el interés es crear una metodología que mida la capacidad de gestión de la seguridad de la información de la OPC CCSS y se pueda aplicar a diferentes organizaciones. Esta metodología busca definir una herramienta que mida la capacidad que la organización tiene en su seguridad de la información basándose en riesgos.

3.2 Sujetos y fuentes de información

3.2.1 Sujetos de información

Barrantes Echavarría, denomina las fuentes de información como los hechos o tipos de documentos que contienen datos útiles para satisfacer una demanda de información o conocimiento.

De aquí nace la necesidad de conocer, distinguir y seleccionar las fuentes de información adecuadas para este proyecto. Dichas fuentes pueden ser primarias o secundarias.

3.2.2 Fuentes de información

3.2.2.1 Fuentes primarias

Según Mas Ruiz, Francisco José, (2010) “las fuentes primarias son aquellas generadas por la propia empresa, como consecuencia de su acción cotidiana. Es decir, se obtienen de las diferentes dependencias de la organización, por lo que lo importante es que la empresa cuente con los medios necesarios y una debida organización que permitan tener los datos actualizados”. (Mas Ruiz, Francisco José. Temas de investigación comercial, quinta edición. 2010, p. 104)

Las fuentes primarias contienen información nueva y original, tales como: libros, revistas científicas, periódicos, diarios, documentos oficiales de instituciones públicas, informes técnicos y de investigación de instituciones públicas o privadas y normas técnicas. Toda esta información debe estar disponible al investigador y se obtiene a través del trabajo en el campo mediante la observación, las entrevistas, cuestionarios, encuestas o sondeos realizados por el investigador, recopilando los datos pertinentes para el tratamiento debido de la información a analizar.

La fuente de información primaria para esta investigación es la obtenida por medio de las normas de seguridad de la información, acuerdos de la Superintendencia de Pensiones y actos de supervisión aplicadas a la OPC CCSS a través de instrumentos de evaluación de riesgo de seguridad de la información.

3.2.2.2 Fuentes secundarias

Las fuentes secundarias según Bernal Torres, César Augusto (2006) son aquellas que ofrecen información sobre el tema por investigar, pero que no son la fuente original de los hechos o las situaciones, sino que sólo los referencian. Las principales fuentes secundarias para la obtención de la información son los libros, las revistas, documentos escritos (en general todo medio impreso), los documentales, los noticieros y los medios de información.” (p. 175)

Las fuentes secundarias son documentos que fueron compilados y muestran la información que fue publicada en las fuentes primarias. En general, los objetivos de las fuentes secundarias son proporcionar a los lectores una síntesis de la información que existe en los documentos primarios sobre temas de interés y ayudar a solucionar las necesidades de información.

Como fuentes de información secundarias para esta investigación se cuenta con documentos sobre la normativa institucional vigente, tales como el Reglamento General de Gestión de La Tecnología de Información, documentación sobre mejores prácticas internacionales, las normas internacionales aplicables a las tecnologías de información,

como ejemplo la ISO/IEC 27001, normas internacionales en materia de gestión de riesgos, así como otras fuentes bibliográficas y documentos en línea.

3.3 Técnicas e instrumentos de recolección de la información

Esta fase de recolección de datos e información se logra a través de alguna técnica que tenga como fin obtener la información necesaria para cumplir con los objetivos planteados. Para efectos de este proyecto se utilizará la herramienta de observación.

3.3.1 Recopilación documental

Esta técnica de recolección de información es un instrumento o técnica de investigación social cuya finalidad es obtener datos e información a partir de documentos escritos y no escritos, susceptibles de ser utilizados dentro de los propósitos de una investigación en concreto. Se debe “detectar, obtener y consultar bibliografía y otros materiales que parten de otros conocimientos y/o informaciones recogidas moderadamente de cualquier realidad, de modo que puedan ser útiles para los propósitos del estudio.

Con esta técnica se obtiene gran capacidad para estandarizar datos, lo que permite su tratamiento informático y análisis estadístico; adicionalmente, permite estudios comparativos y una mayor rapidez en la obtención de información.

3.3.2 Observación

La observación es una técnica útil para el proceso de investigación, consiste en observar a los procesos como son ejecutados; con el fin de conocer mejor la dinámica del proceso; de esta forma el investigador puede determinar qué se está haciendo, cómo se está haciendo, quién lo hace, cuándo se lleva a cabo, cuánto tiempo toma, dónde se hace y por qué se hace.

La observación puede realizarse de tres formas:

- Observar a una persona o actividad sin que el observado se dé cuenta y sin interactuar por parte del propio analista.
- Observar una operación sin intervenir para nada, pero estando la persona observada enterada y consciente de la observación.
- Observar y estar en contacto con las personas observadas. La interrogación puede consistir simplemente en preguntar respecto a una actividad específica.

La observación es una técnica valiosa para recopilar datos que implican relaciones. La observación tiende a adquirir mayor sentido al nivel de procesos, donde las tareas se cuantifican más fácilmente. Entre estas tareas encontramos la recopilación, acumulación y transformación de los datos.

3.4 Cuadro de definición de variables

Las variables que se desarrollan en esta investigación dan respuesta a los objetivos propuestos, de esta manera cada variable será el resultado tangible del trabajo a realizar, se describen a continuación:

Cuadro 1: Definición de variables

Objetivo Específico	**Variable**	**Definición Conceptual**	**Definición instrumental**	**Definición Operacional**
Identificar el estado actual de los procesos de seguridad de la información.	Diagnosticar proceso de seguridad de la información actual.	Diagnosticar se refiere a evaluar el estado actual de un proceso o instrumento.	Se revisará el proceso de seguridad de la información aplicado actualmente en la OPC CCSS.	De la revisión se obtendrá el nivel de gestión de seguridad de la organización.
Determinar las áreas que deben de cubrir los aspectos	Identificar controles de seguridad de	El término determinar se refiere a la acción de ubicar, situar o	Se hará una investigación bibliográfica sobre los	Comparar los productos obtenidos en la definición

de la seguridad de la información en una organización.	la información.	instalar en un determinado lugar o espacio los documentos referentes al tema en cuestión.	principales procesos de Seguridad de la Información.	instrumental y generar una lista de procesos de Seguridad de la Información sujetos a riesgos.
Definir usando como referencia las mejores prácticas y normas internacionales, procesos que permitan evaluar el nivel de capacidad de seguridad de la información.	Definir Controles	El término definir se refiere a explicar en un enunciado de manera exacta y clara el significado de una palabra o un concepto; en el contexto de este proyecto se refiere a escoger los controles que sean necesarios para minimizar los riesgos a que están sujetos los procesos de Seguridad de la Información	Investigación bibliográfica de los controles recomendados por las normas o mejores prácticas para medir la capacidad de gestión de Seguridad de la información basada en riesgos.	Por cada riesgo de seguridad de la información, que se evaluará, se debe de asignar una calificación que muestra la capacidad de gestión de Seguridad de la organización.
Desarrollar un modelo para evaluar el nivel de capacidad de seguridad de la información en la OPC CCSS.	Elaborar una metodología	El término elaborar se refiere a tomar la decisión de hacer la situación que se expresa; consiste en construir a partir de elementos, prácticas, normas una metodología que sirva para evaluar la capacidad de gestión de Seguridad de la Información.	Investigación bibliográfica sobre metodologías de evaluación de riesgo que se puedan utilizar para medir la gestión de los procesos en general.	A partir de la teoría de evaluación de riesgos se elaborará una metodología que ayude a medir la capacidad de gestión de seguridad de la información.
Aplicar la metodología	Asignar una calificación	El término asignar se refiere a señalar, fijar	Investigar en los procesos de la OPC	A partir de la metodología

elaborada en algunos de los componentes de seguridad de la información de la OPC CCSS.		o establecer lo que corresponde a algo o alguien para un determinado objetivo.	CCSS según la metodología desarrollada algunos de los procesos.	aplicada, asignar una calificación respecto al nivel de gestión de seguridad de la información.

Fuente: Elaborado por el sustentante. febrero de 2018

CAPÍTULO IV: METODOLOGÍA y RESULTADOS DE LA EVALUACIÓN

4.1 Situación actual del proceso de seguridad de la información

Actualmente en Costa Rica en las 342 entidades públicas, existen limitaciones presupuestarias en el campo de la seguridad de la información y ciberseguridad, que influyen en la falta de personal especializado en la materia, y la poca cultura de los funcionarios públicos, encargados y usuarios que no implementan las medidas de seguridad necesarias para mantener la seguridad de los datos de información.

Aunque existe desde el 2012 el Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT); este con el pasar de los años no ha avanzado como se tenía previsto y no es la institución que define el norte a seguir en seguridad por parte del país.

Adicionalmente, existe el reglamento "***RGGTI"*** de *CONASSIF* y la Ley 8968, de protección de datos, que establecen como se debe proteger la información confidencial que se encuentra en las instituciones y los deberes y derechos que tienen las instituciones y los costarricenses respecto al manejo de la información.

Solo a las instituciones o empresas supervisadas se les solicita contar con un proceso de seguridad de la información. Por cuenta propia algunas instituciones o empresas privadas que desean tener un control sobre su información crean este proceso.

4.2 Controles de seguridad de la información en la OPC CCSS

Buscando cumplir con las reglamentaciones vigentes, la OPC CCSS crea en el año 2013 el proceso de seguridad de la información, el cual forma parte del área de riesgos.

Desde que se creó el proceso de seguridad de la información, ha existido una evolución constante a través de los años, y a partir del año 2015 se realizó una reestructuración en los controles de seguridad, buscando mantener la confidencialidad, integridad y disponibilidad de la información.

La OPC CCSS actualmente mantiene las siguientes políticas de Seguridad de la Información:

- **Clasificación de datos**: Se deben definir lineamientos necesarios para clasificar los datos e información de la Operadora y los fondos administrados, además de establecer las medidas de seguridad requeridas para garantizar la integridad, confidencialidad y disponibilidad de la información y datos de la OPC CCSS.

- **Control de seguridad física y ambiental**: Se deben mantener lineamientos de control para impedir accesos físicos no autorizados, daños e interferencias contra las instalaciones y equipos que procesan la información de la organización. Además, prevenir pérdidas, daños, hurtos de los activos, así como la interrupción de las actividades de la organización.

- **Control de acceso lógico**: Se deben mantener los mecanismos apropiados para identificar, controlar, regular, monitorear, auditar y restringir el ingreso a la red interna de la Operadora, sistemas internos, sistemas EUC´S, sistemas bajo contrato, servidores y aplicaciones.

- **Perfiles de usuarios y sus privilegios**: Se deben mantener procedimientos para definir, asignar, modificar, eliminar, controlar y auditar los perfiles y usuarios.

- **Seguridad de los recursos humanos**: La Operadora se compromete a verificar la veracidad de la documentación e información aportada por el aspirante al puesto, de acuerdo con las leyes, regulaciones y normas éticas relevantes en los procesos de contratación, cambio o desvinculación del colaborador y la información que estos deban acceder.

- **Sanciones por incumplimientos**: Se deben establecer procedimientos para aplicar las respectivas sanciones en caso de incumplimientos por parte del personal contratado o proveedor.

- **Gestión de Activos**: Se identificarán, documentarán e implementarán reglas, restricciones y procedimientos para el uso aceptable de los activos asociados con la información o activos de información tangibles como el equipo.

- **Gestión de medios de almacenamiento**: Se deberán implementar procedimientos y controles para el uso de medios de almacenamiento extraíbles por parte de los colaboradores.
- **Gestión de dispositivos móviles**: Se deben definir los lineamientos y restricciones para utilizar cualquier equipo portátil que pertenece a la Operadora y todo equipo externo que requiera conectarse a la red interna, además los equipos externos que manejen documentos o datos internos o críticos que pertenecen a la Operadora
- **Acuerdos de Confidencialidad**: La OPC CCSS debe crear acuerdos de confidencialidad para los colaboradores y/o terceros bajo contrato.
- **Intercambio de información**: Se debe mantener la seguridad de los medios en tránsito con terceros estableciendo los lineamientos de transporte de medios informáticos o físicos con terceros, con el fin de garantizar la integridad, confidencialidad, disponibilidad y auditabilidad de los datos e información almacenada en esos medios.
- **Eliminación de datos**: La OPC CCSS debe tener procedimientos para la destrucción o eliminación de la información impresa, dispositivos de almacenamiento y activos de información, utilizando sanas prácticas.
- **Gestión de contraseñas**: Se deben implementar procedimientos de control para las contraseñas, que permitan a los usuarios definir contraseñas fuertes y robustas, contemplando longitud, periodicidad y sintaxis. Se deben realizar campañas de uso adecuado de contraseñas y administración de las mismas.
- **Pantalla y escritorio limpio**: Se deben mantener lineamientos y controles para mantener la información crítica, confidencial e interna en cualquiera de sus formas (impresos, magnéticos, electrónicos, tokens, sellos, firmas digitales, documentos de word etc.).
- **Protección en impresoras, salas, oficinas y pizarras**: Se deben implementar lineamientos de protección para el uso adecuado de las impresoras, salas, oficinas y pizarras en la Operadora.
- **Componentes de red y conexiones**: Se deben crear lineamientos para proteger, identificar, controlar, regular, monitorear, auditar y restringir el

acceso a la red interna, y prevenir accesos no autorizados desde el exterior, o en el interior de la red.

- **Seguridad ante código malicioso y/o código móvil**: Se deben crear lineamientos para proteger, identificar, controlar, regular y monitorear posibles ataques de virus informáticos o malware en los dispositivos de almacenamiento, computadoras y dispositivos conectados a la red interna.
- **Uso adecuado de internet y correo electrónico**: Se deben mantener lineamientos para proteger, regular, monitorear, auditar y restringir el uso de los servicios de internet y correo electrónico.
- **Continuidad del Negocio**: Se deben crear lineamientos para asegurar la continuidad y contingencia del negocio y mantener la disponibilidad de los servicios y datos críticos de la Operadora y fondos administrados.
- **Incidentes y eventos de seguridad de la información**: Se deben crear e implementar lineamientos, protocolos y herramientas para registrar, sancionar, dar seguimiento y tratamiento a los eventos e incidentes de seguridad de la información.
- **Monitoreo de Seguridad de la Información**: Se deben realizar monitoreos calendarizados de la seguridad de la información, que puedan identificar o corregir situaciones que atenten contra las políticas, procedimientos e instructivos de seguridad de la información.
- **Mejoramiento continuo**: La OPC CCSS mejora la eficacia de los procesos de seguridad de la información aplicando la política de calidad, los objetivos estratégicos, los resultados de la revisión por la dirección y las herramientas de análisis, medición y mejora, con el fin de contribuir al fortalecimiento continuo del Sistema de Gestión de Calidad.

La periodicidad con la que se realizan los controles respectivos depende de la disposición de los recursos en la institución.

Los controles actuales están basados en las buenas prácticas según la norma ISO/IEC 27001, y se crearon según la experiencia del encargado del proceso y los recursos disponibles. Estos controles no están sustentados en un análisis de riesgos o algún indicador del estado de la seguridad de la información en la OPC CCSS que muestre las áreas más críticas que se deberían de gestionar en primera instancia.

Esta es la documentación actual que presenta la OPC CCSS de los controles existentes de seguridad de la información:

- Política General de Seguridad de la Información, de esta nace el procedimiento.
    - Procedimiento de la Seguridad de la información.
        - **Instructivo de reclutamiento y selección del personal**: Establece las instrucciones para el reclutamiento y selección del personal acorde con una cultura de calidad en el servicio al cliente y de elevada productividad.
        - **Instructivo de trámites administrativos del personal**: Establecer las actividades relacionadas con trámites administrativos correspondientes a Capital Humano.
        - **Gestión de niveles de servicios**: Establecer un procedimiento para crear acuerdos de niveles de servicio.
        - **Instructivo para registro de activos fijos**: Establecer las acciones para la comunicación sobre la adquisición, traslado y acción de baja de los activos fijos, que deben darse al área de Contabilidad para el adecuado registro contable y mantenimiento actualizado del auxiliar correspondiente.
        - **Instructivo para la eliminación de medios de almacenamiento**: Establecer las acciones para asegurar la correcta eliminación de los medios o dispositivos de almacenamiento, los cuales fueron utilizados por el personal de la Operadora de Pensiones. Adicionalmente, establecer el marco de trabajo con el cual se cumpla los lineamientos establecidos en la Política General de Seguridad de la Información y el procedimiento Gestión de Seguridad de la Información.
        - **Instructivo revisión de acceso lógico**: Establecer las acciones para asegurar el cumplimiento del lineamiento de acceso lógico, establecido en Política de Seguridad de la Información.
        - **Manual de perfiles**: El presente manual permite detallar los perfiles de los sistemas y herramientas tecnológicas

administradas y gestionadas por el Área de T.I. de la OPC-CCSS e indica los niveles de acceso para los funcionarios y miembros.

- **Instructivo revisión de perfiles y roles**: Establecer las acciones para garantizar qué Roles y perfiles asignados a los colaboradores en los sistemas de información les permiten acceder únicamente a las opciones a las cuales están autorizados.
- **Instructivo revisión configuración de computadoras**: Establecer las acciones para asegurar el cumplimiento del lineamiento de uso del equipo de cómputo. Este instructivo describe las acciones de control, a realizar para la gestión de la configuración de las máquinas virtuales, de los colaboradores de la Operadora de Pensiones.
- **Instructivo de clasificación de datos**: Establecer y delimitar las actividades necesarias para realizar la clasificación de datos e información de la Operadora de Pensiones.
- **Instructivo asignación, modificación y eliminación de acceso físico a la OPC CCSS**: Establecer las acciones para asegurar el cumplimiento de los lineamientos para asignar los perfiles y tarjetas de acceso al edificio central de la Operadora.
- **Instructivo de control de tarjetas de acceso de la OPC CCSS**: Describir las acciones correspondientes a la gestión, manejo, registro e inventario de las tarjetas utilizadas por la Operadora, en el sistema de control de acceso del edificio de la OPC CCSS.
- I**nstructivo revisión de acceso físico**: Este instructivo describe las acciones de control a realizar para la gestión del acceso físico, con el fin de garantizar el cumplimiento de los lineamientos establecidos por la OPC CCSS.
- **Instructivo revisión de pantalla y escritorio limpio**: Toda información crítica secreta, confidencial e interna en cualquiera de sus formas (impresos, magnéticos, electrónicos, tokens, sellos, firmas digitales, etc.) deben estar resguardadas y

provistas de la seguridad necesaria, por quien la maneja, para evitar el uso indebido por parte del personal no autorizado.

- **Instructivo control de validación de administración de la red de datos y sus componentes críticos**: Los sistemas de comunicaciones e información, deben estar adecuadamente limitados y protegidos para evitar robos de información, de identidad, pérdida, manipulación de datos o la interrupción de los servicios.
- **Reglamento utilización de internet y correo electrónico**: Los colaboradores deben realizar un uso adecuado de los servicios de internet y correo electrónico, que brinda la Operadora mediante el Área de Tecnologías de la Información.
- **Instructivo acción a seguir en caso de detección de malware**: El objetivo de este instructivo es garantizar la disponibilidad, confidencialidad e integridad de la información almacenada en el equipo de cómputo y otros dispositivos de almacenamiento contra posibles ataques de virus informáticos o malware.
- **Manual de la gestión de continuidad del negocio**: La OPC CCSS establece, documenta, implementa y mantiene procesos, procedimientos y controles para asegurar el nivel necesario de la continuidad del negocio.
- **Instructivo eventos de seguridad de la información**: Establece los protocolos para que los colaboradores puedan registrar los incidentes de seguridad y que el responsable de la gestión de incidentes le dé el debido seguimiento.

4.3 Enfoque de la seguridad de la información en una organización

La seguridad de la información debe de encargarse de cubrir sus tres aspectos fundamentales confidencialidad, integridad y disponibilidad.

Sin embargo, actualmente los expertos incluyen una cuarta característica, la auditabilidad, que consiste en dejar un rastro claro y transparente de todos los usuarios que interactúan con la información.

El estándar ISO/IEC 27001 cubre todos los aspectos mencionados y este se complementa con la estrategia de seguridad de TI que plantea COBIT 5.

En una institución la prioridad debe ser cumplir las leyes y reglamentos existentes y atender las recomendaciones de las auditorías gubernamentales. De ahí en adelante plantear un plan de trabajo para atender sus metas de negocio o sus metas de servicio.

De ahí es donde el enfoque debe de realizarse de manera holística en la organización y basarse en la misión y la visión de la empresa, y las leyes que regulen al sector que pertenece la institución.

Dicho lo anterior el enfoque se debe basar en el RGGTI de *CONASSIF*, según los siguientes lineamientos:

- 2.12 Gestionar la Seguridad,

  Definir, operar y supervisar un sistema para la gestión de la seguridad de la información. Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa. (SNP).

- 4.5 Gestionar Servicios de Seguridad,

  Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad. Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.

Las áreas que deben tomar en cuenta las empresas se agrupan en tres aristas:

4.4.1. **SGSI** (Sistema de Gestión de la Seguridad de la Información) que abarca once aspectos fundamentales,

- Política de seguridad
- Organización de la información de seguridad
- Administración de recursos
- Seguridad de los recursos humanos
- Seguridad física y del entorno
- Administración de las comunicaciones y operaciones
- Control de accesos
- Adquisición de sistemas de información, desarrollo y mantenimiento
- Administración de los incidentes de seguridad
- Administración de la continuidad de negocio
- Cumplimiento (legales, de estándares, técnicas y auditorías).

4.4.2 **Valoración de riegos**, los controles deben ser seleccionados e implementados de acuerdo con la valoración del riesgo y los procesos de tratamiento del riesgo.

4.4.3. **Controles**, que son los que permiten garantizar que cada aspecto, que se valoró con un cierto riesgo, está cubierto y puede ser auditado transparentemente.

4.4 Procesos que evalúan la capacidad de seguridad de la información según normas internacionales

Con el fin de determinar los procesos que se utilizarán para evaluar la capacidad según las normas internacionales, se procedió a realizar una comparación de los controles de las normas ISO/IEC 27001 versus los procesos que contempla COBIT 5 relacionados con la seguridad según se muestra en el Cuadro No. 2.

Cuadro No.2: Comparativo ISO/IEC 27001 y COBIT 5

ISO/IEC 27001:2013	COBIT 5
6.1 Organización interna.	APO01. Gestionar el Marco de Gestión de TI
6.1 Organización interna.	APO02. Gestionar la Estrategia
6.1 Organización interna.	APO03 Gestionar la Arquitectura Empresarial
6.1 Organización interna.	APO05 Gestionar el Portafolio
6.1 Organización interna.	APO06 Gestionar el Presupuesto y los Costes
7. Seguridad ligada a los recursos humanos.	APO07 Gestionar los Recursos Humanos
14.2 Seguridad en los procesos de desarrollo y soporte	AP008 Gestionar las relaciones
15. Relaciones con suministradores.	AP009 Gestionar los acuerdos de servicio
15. Relaciones con suministradores.	APO10 Gestionar los Proveedores
12.1 Responsabilidades y procedimientos de operación. 12.7 Consideraciones de las auditorías de los sistemas de información. 18.2 Revisiones de la seguridad de la información.	APO11 Gestionar la Calidad
12.4 Registro de actividad y supervisión. 16. Gestión de incidentes en la seguridad de la información.	APO12 Gestionar el Riesgo
5. Políticas de seguridad.	APO13 Gestionar la Seguridad
	BAI01 Gestión de Programas y Proyectos

14.1 Requisitos de seguridad de los sistemas de información.	BAI02 Gestionar la Definición de Requisitos
12.1 Responsabilidades y procedimientos de operación.	BAI03 Gestionar la Identificación y Construcción de Soluciones
12.1 Responsabilidades y procedimientos de operación. 17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	BAI04 Gestionar la Disponibilidad y la Capacidad
12.1 Responsabilidades y procedimientos de operación. 17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	BAI06 Gestionar los Cambios
12.1 Responsabilidades y procedimientos de operación. 17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	BAI07 Gestionar la Aceptación del Cambio y la Transición
8. Gestión de activos.	BAI09 Gestionar los Activos
12.6 Gestión de la vulnerabilidad técnica. 12.3 Copias de seguridad. 14.2 Seguridad en los procesos de desarrollo y soporte.	BAI10 Gestionar la Configuración
6.1 Organización interna.	EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno
12.4 Registro de actividad y supervisión. 12.6 Gestión de la vulnerabilidad técnica.	EDM02 Asegurar la Entrega de Beneficios
12.4 Registro de actividad y supervisión. 16. Gestión de incidentes en la seguridad de la información.	EDM03 Asegurar la Optimización del Riesgo
12.4 Registro de actividad y supervisión. 12.6 Gestión de la vulnerabilidad técnica.	EDM04 Asegurar la Optimización de Recursos
5.1 Directrices de la Dirección en	EDM05 Asegurar la Transparencia hacia las

seguridad de la información. 6.1 Organización interna.	Partes Interesadas
12.1 Responsabilidades y procedimientos de operación. 12.6 Gestión de la vulnerabilidad técnica. 14.2 Seguridad en los procesos de desarrollo y soporte.	DSS01 Gestionar Operaciones
16.1 Gestión de incidentes de seguridad de la información y mejoras.	DSS02 Gestionar las peticiones y los incidentes del servicio
16.1 Gestión de incidentes de seguridad de la información y mejoras.	DSS03 Gestionar Problemas
17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	DSS04 Gestionar la Continuidad
5. Políticas de seguridad.	DSS05 Gestionar Servicios de Seguridad
6.1 Organización interna. 12. Seguridad en la operativa.	DSS06 Gestionar Controles de Proceso de Negocio
12.4 Registro de actividad y supervisión. 12.6 Gestión de la vulnerabilidad técnica.	MEA01 Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad
12.4 Registro de actividad y supervisión. 12.6 Gestión de la vulnerabilidad técnica.	MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno
12.4 Registro de actividad y supervisión. 12.6 Gestión de la vulnerabilidad técnica. 15. Relaciones con suministradores.	MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos

Fuente: Elaborado por el sustentante, febrero de 2018

La comparación de los controles se llevó a cabo por medio de la lectura de cada uno de los controles de “COBIT 5 para seguridad de la información” y los controles de la ISO/IEC 27001.

Una vez realizada la comparación anterior, se obtuvo un modelo de evaluación de Seguridad de la Información que consta de 34 procesos.

Además, para cada uno de los procesos se realizó un inventario de riesgos asociados y controles mitigadores (*Ver Anexo No.1*).

Para determinar los riesgos y controles mencionados en el párrafo anterior se realizó una investigación basada en el documento denominado *COBIT 5 para seguridad de la información,* en donde se redactaron los posibles riesgos asociados que puede tener una organización según lo indicado por los estándares.

De esta investigación y análisis se escogen en total 1036 controles de evaluación y 259 riesgos asociados según como se muestra en el Cuadro No.3.

Cuadro No.3: Procesos a utilizar en el modelo de evaluación

Procesos	**Cantidad de controles**	**Riesgos asociados**
Gestionar el Marco de Gestión de TI	48	14
Gestionar la Estrategia	31	10
Gestionar la Arquitectura Empresarial	39	8
Gestionar el Portafolio	28	8
Gestionar el Presupuesto y los Costes	31	9
Gestionar los Recursos Humanos	36	9
Gestionar las relaciones	24	5
Gestionar los acuerdos de servicio	20	6
Gestionar los Proveedores	27	8
Gestionar la Calidad	33	6
Gestionar el Riesgo	33	6
Gestionar la Seguridad	19	11
Gestión de Programas y Proyectos	78	13
Gestionar la Definición de Requisitos	17	4
Gestionar la Identificación y Construcción de Soluciones	57	15
Gestionar la Disponibilidad y la Capacidad	25	8
Gestionar los Cambios	18	9
Gestionar la Aceptación del Cambio y la Transición	51	9
Gestionar los Activos	36	5
Gestionar la Configuración	16	6
Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	20	5
Asegurar la Entrega de Beneficios	20	5
Asegurar la Optimización del Riesgo	16	5
Asegurar la Optimización de Recursos	13	4
Asegurar la Transparencia hacia las Partes Interesadas	10	5

Gestionar Operaciones	34	6
Gestionar las peticiones y los incidentes del servicio	24	8
Gestionar Problemas	23	6
Gestionar la Continuidad	42	11
Gestionar Servicios de Seguridad	49	10
Gestionar Controles de Proceso de Negocio	30	6
Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	26	4
Supervisar, Evaluar y Valorar el Sistema de Control Interno	44	11
Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	18	4

Fuente: Elaborado por el sustentante, marzo de 2018

Existe un total de 1036 controles y 259 riesgos asociados a los controles respectivos que se pueden observar en el Anexo No.1.

4.5 Modelo de evaluación de seguridad de la información

Este modelo de evaluación es una herramienta dentro de un contexto definido, que utiliza datos de entrada para analizarlos en un proceso que dará como resultado un producto, que en este caso es el nivel de capacidad de gestión de seguridad de la información.

Como parte de los objetivos de este proyecto se pretende desarrollar un modelo para evaluar la capacidad de gestión de la seguridad de la información basado en un análisis de los riesgos aplicados a los procesos actuales de seguridad de la información de la OPC CCSS.

Para evaluar esta capacidad es necesario crear una metodología de cálculo en donde se procesarán los datos para dar un resultado final.

Estos cálculos se deben de usar en una matriz de cálculo que de manera ordenada mostrará los controles y la respectiva efectividad de cada uno.

4.6 Metodología de cálculo

La metodología de cálculo ayuda a cuantificar los resultados obtenidos por las matrices. Para realizar el cálculo de las capacidades en los controles, se definen los siguientes parámetros:

4.6.1 Impacto

Es la medida, cuantitativa o cualitativa, de la consecuencia de un riesgo donde se tiene seis niveles: impacto insignificante el cual va de 0% a 16.67%, impacto bajo que va desde 16.68% hasta 33.33%, impacto medio que va desde 33.34% hasta 50%, impacto alto que va desde 50.01% hasta 66.67%, impacto muy alto que va desde 66.68% hasta 83.33% e impacto crítico el cual va desde 83.33% hasta 100%.

Cuadro No.4: Nivel de Impacto

Código	Clasificación	Valor
I1	Insignificante	00.00% - 16.67%
I2	Bajo	16.68% - 33.33%
I3	Medio	33.34% - 50.00%
I4	Alto	50.01% - 66.67%
I5	Muy Alto	66.68% - 83.33%
I6	Crítico	83.34% - 100.00%

Fuente: Elaborado por el sustentante, marzo de 2018

El impacto será seleccionado con base a la tabla siguiente; no obstante, los rubros que aparecen en la tabla son ejemplos de impactos que se pueden clasificar dentro de cada categoría, por lo que, si el impacto no se encuentre dentro de la tabla, la organización debe determinar el que mejor corresponda.

Cuadro No.5: Rubros de nivel de Impacto

Insignificante 16.67%	Duplicidad de funciones
	Retrasos en procesos internos
	Inefectividad de las funciones
Bajo 33.33%	Errores de Usuarios (Final y Técnico)
	Llamadas de atención de superiores escritas o verbales
	No atención de los procedimientos establecidos
	Reprocesos de la información no sensible
Medio 50%	Interrupción de los servicios de cara al cliente interno
	Errores en aplicaciones Internas
	Reprocesos de la Información Sensible
	Irregularidades no identificadas
Alto 66.67%	Pérdida de información de menos de un día
	Interrupción de los servicios de cara al cliente externo
	Errores en aplicaciones Externas
	Daños en la Infraestructura Tecnológica (Server, Router, entre otros).
Muy Alto 83.33%	Interrupción de los servicios
	Fraude Interno
	Incumplimiento del Plan estratégico del negocio
	Pérdida de información de 1 o más días
Crítico 100%	Intervención del ente regulador
	Quiebra de la empresa
	Sanciones por procedimientos administrativos
	Sanción o multa a la entidad

Fuente: Elaborado por el sustentante, marzo de 2018

En el cálculo, se debe establecer para cada riesgo identificado el impacto asociado al mismo, se utiliza el límite máximo de cada nivel de impacto y luego se calcula el promedio de los impactos. La fórmula utilizada es la siguiente:

$$IMP = \frac{1}{n}\sum_{i=1}^{n} imp_i$$

Dónde:

IMP = Impacto

n = Cantidad de Riesgos identificados

imp_i = Impacto individual de cada riesgo

(la forma matemática de un promedio simple)

4.6.2 Efectividad del Control

Es la medida cuantitativa que muestra cual es la efectividad de gestión que tiene la organización en los controles de validación

Cuadro No.6: Nivel de efectividad del control

Código	Clasificación	Valor
E1	No definido	00.00% - 15.00%
E2	Inicial	15.01% - 30.00%
E3	Repetible pero Intuitivo	30.01% - 45.00%
E4	Definido	45.01% - 60.00%
E5	Administrado y Medible	60.01% - 75.00%
E6	Optimizado	75.01% - 90.00%

Fuente: Elaborado por el sustentante, marzo de 2018

Cada uno de los niveles de clasificación de la efectividad de los controles significa lo siguiente:

Cuadro No.7: Significado de los niveles de efectividad del control

No definido 15%	La organización carece completamente de cualquier proceso reconocible e incluso desconoce la existencia de un problema a resolver.
Inicial 30%	Los controles asociados al proceso de gestión se encuentran (por lo general) no documentados y en un estado de cambio dinámico, que tienden a ser utilizados de una manera incontrolada y reactiva por los usuarios o por la ocurrencia de un evento.
Repetible pero Intuitivo 45%	El control es ejecutado de forma repetida y posiblemente los resultados obtenidos son consistentes. La disciplina adquirida para ejecutar el control no es muy rigurosa, pero ayuda a garantizar que el control se ejecute de la misma forma en

	momentos de estrés.
Definido 60%	El control se encuentra formalmente documentado y sujeto a mejora a través del tiempo. El que se encuentre formalmente documentado ayuda a garantizar la consistencia de la ejecución del control.
Administrado y Medible 75%	Los controles ya tienen establecidas métricas y la gestión del mismo permite controlar de manera efectiva el proceso, se pueden ajustar y adaptar a proyectos particulares sin tener pérdidas medibles en la calidad o desviaciones en el mismo
Optimizado 90%	Los controles en este nivel se caracterizan por centrarse en la mejora continua del rendimiento a través del incremento e innovación tecnológica mediante cambios y mejoras.

Fuente: Elaborado por el sustentante, marzo de 2018

Al finalizar de incluir la efectividad de todos los procesos de gestión, se suma el resultado obtenido para cada pregunta y el total es la efectividad del control obtenida.

La fórmula utilizada es la siguiente:

$$EC = \sum_{i=1}^{n} \left(prp_i * r_1 \right)$$

Dónde:

$\boldsymbol{EC}$ = Efectividad del control

$\boldsymbol{n}$ = Cantidad de preguntas definidas

$\boldsymbol{prp_i}$ = Peso relativo de la pregunta

$\boldsymbol{r_i}$ = Resultado de la pregunta

4.6.3 Probabilidad de fallo

Es la medida o descripción de la posibilidad de ocurrencia de un evento donde se tiene seis niveles: probabilidad “insignificante” el cual va de 0% a 16.67%, probabilidad “baja” que va desde 16.68% hasta 33.33%, probabilidad “media” que va desde 33.34% hasta 50%, probabilidad “alta” que va desde 50.01% hasta 66.67%, probabilidad “muy alta” que va desde 66.68% hasta 83.33% y probabilidad “siempre” el cual va desde 83.33% hasta 100%.

Cuadro No.8: Niveles de probabilidad de fallo

Código	Clasificación	Valor
P1	Insignificante	00.00% - 16.67%
P2	Baja	16.68% - 33.33%
P3	Media	33.34% - 50.00%
P4	Alta	50.01% - 66.67%
P5	Muy Alta	66.68% - 83.33%
P6	Siempre	83.34% - 100.00%

Fuente: Elaborado por el sustentante, marzo de 2018

La fórmula de cálculo para la probabilidad es la inversa de la efectividad del control e indica la probabilidad de fallo, en que se ve afectado el proceso por sus diferentes actividades incorporando los diferentes niveles de control.

$$PR = 1 - EC$$

Dónde:

PR = Probabilidad

EC = Efectividad del control

4.6.4 Riesgo Inherente del proceso

Riesgo que la organización asumiría sin controles.

El riesgo inherente se calcula de la siguiente manera:

$$Ri = IMP * PR$$

La multiplicación de la tabla de impactos

Dónde:

Ri = Riesgo inherente detectado

PR = Probabilidad

$\boldsymbol{IMP}$ = Impacto del proceso

4.6.5 Exposición al Riesgo del proceso (Riesgo Residual)

Esta es la exposición real que asume la organización después de aplicar los mitigadores, esta se calcula de la siguiente manera:

$$ERP = Ri(1 - IMP)$$

Dónde:

ERP = La exposición al riesgo del proceso.

Ri = Riesgo inherente detectado.

$\boldsymbol{IMP}$ = Impacto del proceso.

Dentro de los niveles de riesgo se encuentran seis categorías, las cuales se definen de la siguiente forma:

Riesgo Insignificante: Se considera esta categoría cuando los parámetros se encuentren entre 0% a 16.67%.

Riesgo Bajo: Se considera esta categoría cuando los parámetros se encuentren entre 16.68% a 33.33%.

Riesgo Medio: Se considera esta categoría cuando los parámetros se encuentren entre 33.34% a 50%.

Riesgo Alto: Se considera esta categoría cuando los parámetros se encuentren entre 50.01% a 66.67%.

Riesgo Muy Alto: Se considera esta categoría cuando los parámetros se encuentren entre 66.68% a 83.33%.

Riesgo Crítico: Se considera esta categoría cuando los parámetros se encuentren entre 83.34% a 100%.

4.6.6 Nivel de gestión de seguridad de la información

Con este cálculo final se puede medir cual es esa capacidad de gestión de seguridad de la información en cada uno de los procesos evaluados y en general realizando un promedio. Este cálculo se realiza de la siguiente forma:

$$\mathbb{C}_{\mathcal{G}} = 100 - ERP$$

Dónde:

$\mathbb{C}_{\mathcal{G}}$= Capacidad de gestión.

100 = Total de la posible capacidad.

ERP = La exposición al riesgo del proceso.

Los niveles de capacidad de gestión cuentan con seis categorías, las cuales se definen de la siguiente forma:

Capacidad de gestión Baja: Se considera esta categoría cuando el resultado se encuentra entre 0% y 16.67%.

Capacidad de gestión Inicial: Se considera esta categoría cuando el resultado se encuentra entre 16.68% y 33.33%.

Capacidad de gestión Media: Se considera esta categoría cuando el resultado se encuentra entre 33.34% y 50%.

Capacidad de gestión En desarrollo: Se considera esta categoría cuando el resultado se encuentra entre 50.01% y 66.67%.

Capacidad de gestión Establecida: Se considera esta categoría cuando el resultado se encuentra entre 66.68% y 83.33%.

Capacidad de gestión Óptima: Se considera esta categoría cuando el resultado se encuentra entre 83.34% y 100%.

4.6.7 Matriz de valorización

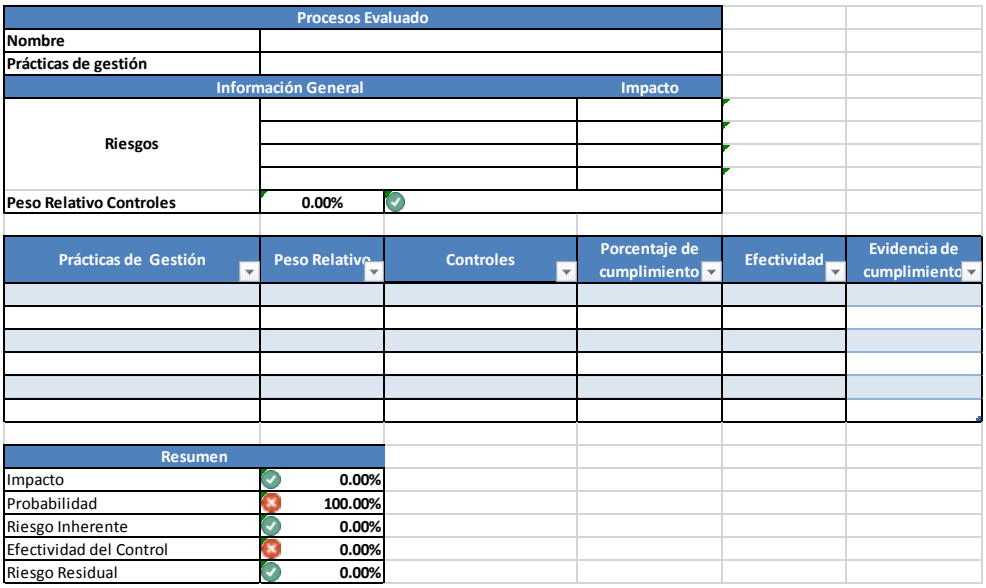
Una Matriz de valorización es una estrategia de evaluación alternativa, generada a través de un listado de un conjunto de criterios específicos y fundamentales que permiten valorar en este caso, la capacidad de gestión de la seguridad de la información.

La creación de esta matriz se conforma de los siguientes pasos:

1. Ingresar los parámetros de impacto, efectividad de control y probabilidad que brinda la metodología de cálculo para que estos puedan ser utilizados por las fórmulas creadas en la metodología.
2. Ubicar los riesgos asociados a cada control para asignarles un respectivo impacto.
3. Ubicar los controles de evaluación en orden según el proceso asignado.
4. Ingresar en la matriz las fórmulas de impacto, probabilidad, riesgo inherente, efectividad de control, riesgo residual y capacidad de gestión para que reciban los datos y se gestionen los resultados finales.

A continuación, se presenta la matriz de valorización creada según los pasos anteriores en donde se pueden visualizar los títulos y las fórmulas que necesitarían el ingreso de información para realizar los cálculos respectivos.

Figura No.11: Matriz de valorización



Procesos Evaluado						
Nombre						
Prácticas de gestión						
Información General			Impacto			
Riesgos						
Peso Relativo Controles	0.00%					

Prácticas de Gestión	Peso Relativo	Controles	Porcentaje de cumplimiento	Efectividad	Evidencia de cumplimiento

Resumen	
Impacto	0.00%
Probabilidad	100.00%
Riesgo Inherente	0.00%
Efectividad del Control	0.00%
Riesgo Residual	0.00%

Para la aplicación de este modelo de evaluación se crearon 34 matrices de valorización para medir los 34 procesos evaluados, una matriz para el ingreso de los parámetros (Impacto, Efectividad de control y Probabilidad) y una matriz final para los resultados en donde se calcula la capacidad de gestión. (Ver Anexo No.1)

4.7 Aplicación del modelo de evaluación de seguridad de la información

Como parte final de este proyecto se realizó la aplicación del modelo de evaluación de la capacidad de gestión de la seguridad de la información en todos los procesos relacionados a seguridad en la OPC CCSS.

La aplicación implicó realizar 1036 controles de evaluación, los cuales en su totalidad debían ser respaldados con evidencia a la vista que validara dicho nivel de gestión por cada proceso.

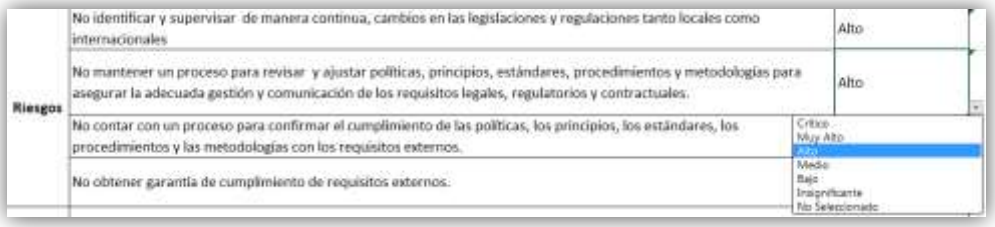
En primera instancia se procede a ingresar los criterios de impacto, efectividad del control y probabilidad como se muestra a continuación en la figura No.12.

Figura No.12: Criterios de riesgo de la matriz de valorización

Impacto		Efectividad del Control		Probabilidad	
Descripción	Peso	Descripción	Peso	Descripción	Peso
Crítico	100.00%	Optimizado	90.00%	Siempre	100.00%
Muy Alto	83.33%	Administrado y Medible	75.00%	Muy Alta	83.33%
Alto	66.67%	Definido	60.00%	Alta	66.67%
Medio	50.00%	Repetible pero Intuitivo	45.00%	Media	50.00%
Bajo	33.33%	Inicial/Ad hoc	30.00%	Baja	33.33%
Insignificante	16.67%	No definido	15.00%	Insignificante	16.67%

Seguidamente, se asignó el nivel de impacto de cada uno de los riesgos asociados por proceso según los criterios de impacto, como se muestra a continuación.

Figura No.13: Asignación del nivel de impacto a los riesgos asociados



Una vez asignado el impacto, se procedió a asignar el peso relativo de cada uno de los controles de evaluación, así como el porcentaje de cumplimiento de cada uno de los controles según la evidencia encontrada o suministrada.

Figura No.14: Peso relativo, cumplimiento y evidencia de cumplimiento.

Peso Relativo	Controles	Porcentaje de cumplimiento	Efectividad	Evindencia de cumplimiento
3.85%	Identificar las partes interesadas (p. ej. dirección, propietarios de procesos o usuarios).	100%	3.85%	5CO01. Código de Gobierno Corporativo Actualmente se identifica las partes interesadas o responsables en los documentos de la Operadora.
3.85%	Involucrar a las partes interesadas y comunicar los objetivos y requisitos empresariales para la supervisión, consolidación e información, utilizando definiciones comunes (p. ej. glosario corporativo, metadatos y taxonomías), líneas de referencia y estudios comparativos (benchmarking).	100%	3.85%	5P01. Comunicación
3.85%	Mantener y alinear de forma continua el enfoque de supervisión y evaluación con el enfoque de la compañía así como las herramientas utilizadas para la obtención de datos y presentación de informes corporativos (p. ej. aplicaciones de inteligencia de negocio).	0%	0.00%	No se cuenta con un procedimiento definido para mantener y alinear de forma continua el enfoque de supervisión y evaluación con el enfoque de la compañía
3.85%	Acordar los objetivos y métricas (p. ej., cumplimiento, rendimiento, valor, riesgo), taxonomía (clasificación y relación entre objetivos y métricas) y la retención de datos (evidencias).	100%	3.85%	7I13. Creación, actualización, custodia y resguardo de expedientes de clientes. Plan_Estrategico_TI_OPC_2015-2017

Después de ingresar los datos y porcentajes correspondientes, se procede a utilizar la metodología de cálculo para obtener el riesgo residual.

Figura No.15: Resultados según la metodología de cálculo

Resumen	
Impacto	**54.17%**
Probabilidad	**43.46%**
Riesgo Inherente	**23.54%**
Efectividad del Control	**56.54%**
Riesgo Residual	**10.23%**

Utilizando el riesgo residual se procede a calcular el nivel de gestión de seguridad de la información del proceso que se presenta en los resultados.

4.8 Resultados

Según la matriz de valorización aplicada (Anexo 1) se reflejan los siguientes resultados por proceso y su respectiva capacidad de gestión de seguridad de la información.

Cuadro No.9: Resultados

Ref. Doc.	Proceso	Capacidad de gestión de Seguridad de la Información
3.1.1	Gestionar el Marco de Gestión de TI	98%
3.1.2	Gestionar la Estrategia	76%
3.1.3	Gestionar la Arquitectura Empresarial	84%
3.1.4	Gestionar el Portafolio	96%
3.1.5	Gestionar el Presupuesto y los Costes	97%
3.1.6	Gestionar los Recursos Humanos	98%
3.1.7	Gestionar las relaciones	94%
3.1.8	Gestionar los acuerdos de servicio	84%
3.1.9	Gestionar los Proveedores	99%
3.1.10	Gestionar la Calidad	99%
3.1.11	Gestionar el Riesgo	91%
3.1.12	Gestionar la Seguridad	91%
3.1.13	Gestión de Programas y Proyectos	86%
3.1.14	Gestionar la Definición de Requisitos	93%
3.1.15	Gestionar la Identificación y Construcción de Soluciones	94%
3.1.16	Gestionar la Disponibilidad y la Capacidad	93%
3.1.17	Gestionar los Cambios	88%
3.1.18	Gestionar la Aceptación del Cambio y la Transición	91%
3.1.19	Gestionar los Activos	98%
3.1.20	Gestionar la Configuración	99%
3.1.21	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	81%

3.1.22	Asegurar la Entrega de Beneficios	88%
3.1.23	Asegurar la Optimización del Riesgo	98%
3.1.24	Asegurar la Optimización de Recursos	93%
3.1.25	Asegurar la Transparencia hacia las Partes Interesadas	68%
3.1.26	Gestionar Operaciones	99%
3.1.27	Gestionar las peticiones y los incidentes del servicio	97%
3.1.28	Gestionar Problemas	98%
3.1.29	Gestionar la Continuidad	99%
3.1.30	Gestionar Servicios de Seguridad	94%
3.1.31	Gestionar Controles de Proceso de Negocio	93%
3.1.32	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	90%
3.1.33	Supervisar, Evaluar y Valorar el Sistema de Control Interno	95%
3.1.34	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	85%

Fuente: Elaborado por el sustentante, marzo de 2018

El nivel de gestión de seguridad de la información según el promedio de los resultados es de **92%**, evidenciando un nivel aceptable para la OPC CCSS.

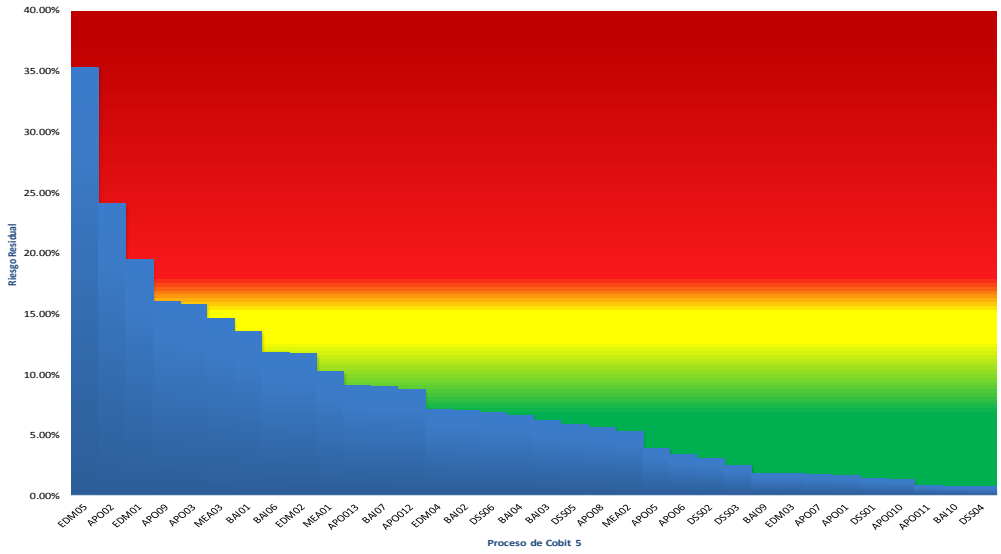
Como se observa en la tabla anterior, 31 de los procesos evaluados se encuentran dentro del rango de riesgo insignificante (0% - 16.67%) y 3 procesos están dentro del rango de riesgo bajo (16.68% - 33.33%).

El Área de TI, tiene 3 procesos que sobrepasan el límite de riesgo aceptado por la Operadora de 16.67%.

- APO02 Generar la estrategia.

- ADM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.
- ADM05 Asegurar la transparencia hacia las partes interesadas.

Gráfico #1: Nivel de Riesgo Asumido por Procesos en la OPC CCSS



Fuente: Elaborado por el sustentante, marzo de 2018

El gráfico muestra a tres procesos que han sobrepasado el umbral de riesgo aceptado por la Operadora de 16,67% según el mapa de calor, dejando un panorama claro de donde se debería trabajar en primera instancia y en donde se deberían concentrar recursos si es que estos procesos son críticos para la organización.

4.9 Conclusiones y recomendaciones

Para realizar este proyecto de investigación aplicada se tuvo que indagar detalladamente toda la información existente en la Operadora de Pensiones, además, fue necesario investigar a detalle la norma “ISO/IEC 27001” y “COBIT 5 para Seguridad de la Información”, y de esta manera se creó una metodología de evaluación robusta,

que logró dar una visibilidad a la organización que no existía y con eso mostrar un panorama preciso de los procesos internos de seguridad de la información.

Siguiendo con el orden respectivo, a continuación se detallarán las conclusiones y recomendaciones relacionadas con cada uno de los objetivos específicos y su desarrollo durante el proyecto.

4.9.1 Identificar el estado actual de los procesos de seguridad de la información

Conclusión: La ciberseguridad y en específico la seguridad de la información en Costa Rica y en la Operadora, tienen un reto importante para los próximos años, donde es necesario madurar los procesos sustantivos y que para la empresa sean relevantes.

Recomendación: Es necesario que la organización esté en constante actualización en materia de seguridad de la información, y realizar estudios de cómo se encuentran otras empresas nacionales e internacionales para que el panorama sea el más adecuado.

4.9.2 Determinar las áreas que deben de cubrir los aspectos de la seguridad de la información en una organización

Conclusión: Las áreas de seguridad que se deben cubrir en Costa Rica deben ir de la mano de lo que dictan las buenas y sanas prácticas de los estándares internacionales, las leyes y reglamentos actuales y la razón de ser de la organización. Esto para no gastar recursos en áreas en donde no se necesita madurar para alcanzar el éxito de la empresa, sin dejar de lado el sistema de gestión de seguridad de la información, la valorización de riesgos y los controles respectivos.

Recomendación: La organización debe tener muy claro cuáles son sus procesos sustantivos y críticos según su misión y visión de negocio para que una vez obtenidos los resultados de la evaluación, la alta gerencia decida el camino de inversión que se va a dar según sus necesidades.

4.9.3 Investigar usando como referencia las mejores prácticas y normas internacionales, procesos que permitan evaluar el nivel de capacidad de seguridad de la información

Conclusión: Existen estándares internacionales de seguridad que tienen muchos procesos de control en común que una vez realizada la comparación se puede aprender que estos procesos tienen una capacidad similar de evaluar la seguridad de la información en una organización y utilizarla para cubrir de manera más robusta dicho proceso de seguridad.

Recomendación: Los estándares de seguridad internacionales tienen suficientes controles para asegurar la información de una empresa, sin embargo, no se deben utilizar controles que no tienen valor agregado para la empresa para no gastar innecesariamente recursos y no poner a la empresa en posibles riesgos financieros.

4.9.4 Desarrollar un modelo para evaluar el nivel de capacidad de seguridad de la información en la OPC CCSS

Conclusiones: La medición de la capacidad debe de realizarse de forma cualitativa, para poder representar esta capacidad según los cálculos realizados y que estos sean claros y precisos para la administración.

Por ser un modelo basado en riesgos, se debe crear el cálculo que brindará el respectivo nivel de gestión de seguridad de la información, transformando así el resultado del nivel de riesgo a un nivel de capacidad.

Con la certificación ISO 9001:2008 implementada en la Operadora, se declara una estructura más organizada, por lo que se hizo realizable la identificación de posibles eventos de riesgo, con sus causas y consecuencias

Recomendación: La matriz de cálculo debe ser realizada de la manera más clara posible, por lo que es necesario tener claro los cálculos que se van a realizar y estudiar el comportamiento de la herramienta.

4.9.5 Aplicar el modelo elaborado en algunos de los componentes de seguridad de la información

Conclusiones: Para poder medir un nivel de capacidad de seguridad de la información se debe contar con un compromiso del personal al cual se le solicita la información, y que la evidencia facilitada de los procesos a evaluar sea objetiva, precisa y clara.

Esta evaluación es realizada para ejecutar un mejoramiento continuo en el control interno, comunicando posibles errores y además fue insumo fundamental para la comisión de tecnologías de información de la OPC CCSS para poder definir el perfil tecnológico solicitado por SUPEN, según la “Minuta de reunión 009 CTI”.

Recomendaciones: Para realizar esta evaluación la organización debe contar con el apoyo de la alta gerencia y todos los colaboradores involucrados en el proceso para que el resultado sea el adecuado.

Se recomienda alinear los planes estratégicos de TI con los objetivos del negocio, de forma que se comuniquen claramente los objetivos y las cuentas asociadas, para que sean comprendidos por todos, y se identifiquen las opciones estratégicas de TI para estructurarlas e integrarlas con los planes de negocio y obtener un enfoque consistente, integrado y alineado con el alcance del gobierno de la empresa y garantizar que las decisiones relativas a Tecnologías de información se hayan adoptado en línea con las estrategias y objetivos de la empresa, garantizando la efectividad y transparencia, en el cumplimiento con los requerimientos regulatorios y legales.

Bibliografía

Pastor, J. (2002). Concepto de Sistemas de Información en la Organización. Editorial UOC, Barcelona, España.

Carlos Muñoz R (1996). Fundamentos para teoría general del derecho, primera edición. Editorial Plaza Valdés, México Distrito Federal, México.

Mas Ruiz (2010), Francisco José. Temas de investigación comercial, quinta edición. Editorial Club Universitario, Alicante, España.

Bernal Torres, César Augusto (2006). Metodología de la información: para administración, economía, humanidades y ciencias sociales, segunda edición. Editorial Pearson Educación de México, México Distrito Federal, México.

COBIT 5. © 2012 ISACA. Todos los derechos reservados.

ISO/IEC 27001:2013. Código de buenas prácticas para la gestión de la seguridad de la información, 2013.

Sistema de Gestión de la Calidad de la OPC CCSS.

Conasiff (2017) Reglamento General de Gestión de La Tecnología de Información

Ley n.º 8968 (2011), Ley de protección de la persona frente al tratamiento de sus datos personales.

Ley 9048(2012), Delitos Informáticos y Conexos.

Tipos de metodología de investigación según Dankhe, Página web: http://www.eumed.net/libros-gratis/2010e/816/CLASIFICACION%20DE%20DANKHE%201986.html

ANEXOS

Anexo 1: Matriz de valorización OPC CCSS

Rubros utilizados

Impacto	
Descripción	Peso
Crítico	100.00%
Muy Alto	83.33%
Alto	66.67%
Medio	50.00%
Bajo	33.33%
Insignificante	16.67%

Efectividad del Control	
Descripción	Peso
Optimizado	90.00%
Administrado y Medible	75.00%
Definido	60.00%
Repetible pero Intuitivo	45.00%
Inicial/Ad hoc	30.00%
No definido	15.00%

Probabilidad	
Descripción	Peso
Siempre	100.00%
Muy Alta	83.33%
Alta	66.67%
Media	50.00%
Baja	33.33%
Insignificante	16.67%

Procesos Evaluado						
Nombre						
Prácticas de gestión						
Información General			**Impacto**			
Riesgos						
Peso Relativo Controles	**0.00%**					

Prácticas de Gestión	Peso Relativo	Controles	Porcentaje de cumplimiento	Efectividad	Evidencia de cumplimiento

Resumen	
Impacto	**0.00%**
Probabilidad	**100.00%**
Riesgo Inherente	**0.00%**
Efectividad del Control	**0.00%**
Riesgo Residual	**0.00%**

Matriz de Valorización

Procesos Evaluado		
Nombre	MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	
Prácticas de gestión	MEA03.01 Identificar requisitos externos de cumplimiento. MEA03.02 Optimizar la respuesta a requisitos externos. MEA03.03 Confirmar el cumplimiento de requisitos externos. MEA03.04 Obtener garantía de cumplimiento de requisitos externos.	
Normas Técnicas Relacionadas		
Información General		**Impacto**
Riesgos	No identificar y supervisar de manera continua, cambios en las legislaciones y regulaciones tanto locales como internacionales	Alto
	No mantener un proceso para revisar y ajustar políticas, principios, estándares, procedimientos y metodologías para asegurar la adecuada gestión y comunicación de los requisitos legales, regulatorios y contractuales.	Alto
	No contar con un proceso para confirmar el cumplimiento de las políticas, los principios, los estándares, los procedimientos y las metodologías con los requisitos externos.	Alto
	No obtener garantía de cumplimiento de requisitos externos.	Medio

Peso Relativo	Controles	Porcentaje de cumplimiento	Efectividad	Evindencia de cumplimiento
5.56%	Asignar la responsabilidad de identificar y supervisar los cambios legales y regulatorios y otros requisitos contractuales externos aplicables a la utilización de recursos de TI y al procesamiento de la información dentro de las operaciones de negocio y de TI.	0%	0.00%	No se cuenta un registro que haga referencia a la tarea de asignar la responsabilidad de identificar y supervisar los cambios legales y regulatorios y otros requisitos contractuales externos
5.56%	Identificar y valorar la totalidad de los posibles requisitos de cumplimiento y su impacto sobre las actividades de TI en ámbitos como los flujos de datos, la privacidad, los controles internos, los informes financieros, la regulación sectorial, la propiedad intelectual y la seguridad e higiene en el trabajo.	20%	1.11%	Actualmente se esta realizando esta actividad, pero no se encuentra formalmente documentada
5.56%	Valorar el impacto de los requisitos legales y regulatorios relacionados con TI sobre los contractos con terceros que afecten a las operaciones de TI, los proveedores de servicio y los socios de negocio.	100%	5.56%	7P06. Gestión de Bienes y Servicios
5.56%	Obtener asesoramiento independiente, si procede, sobre las modificaciones en las legislaciones, regulaciones y estándares aplicables.	100%	5.56%	5R02. Reglamento de Trabajo Comisión de TI
5.56%	Mantener un inventario actualizado de los requisitos legales, regulatorios y contractuales aplicables, su impacto y las acciones necesarias.	0%	0.00%	No se cuenta con un registro que haga referencia a mantener un inventario actualizado de los requisitos legales, regulatorios y contractuales
5.56%	Mantener un registro general consolidado de los requisitos externos de cumplimiento que afecten a la empresa.	0%	0.00%	Falta un registro general consolidado de los requisitos externos de cumplimiento que afecten a la empresa.
5.56%	Revisar y ajustar con regularidad las políticas, los principios, los estándares, los procedimientos y las metodologías para que mantengan su eficacia en asegurar el cumplimiento requerido y la gestión del riesgo empresarial. Contar para ello con expertos internos y externos, según proceda.	100%	5.56%	4P01. Generación y control de los documentos y registros
5.56%	Comunicar los nuevos requisitos y las modificaciones de los existentes al personal que corresponda.	100%	5.56%	4P01. Generación y control de los documentos y registros
5.56%	Evaluar regularmente las políticas, estándares, procedimientos y metodologías de la organización para todas las funciones corporativas con objeto de asegurar el cumplimiento de los requisitos legales y regulatorios aplicables al procesamiento de información.	60%	3.33%	4P01. Generación y control de los documentos y registros. Sin embargo no se hace referencia especificamente que sea aplicable al procesamiento de la información.
5.56%	Gestionar las deficiencias de cumplimiento en las políticas, estándares y procedimientos dentro de plazos razonables.	100%	5.56%	7P07. Gestión de requisitos legales
5.56%	Evaluar periódicamente los procesos y actividades tanto de TI como de negocio para asegurar el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables.	0%	0.00%	Se requiere un procedimiento definido para evaluar periódicamente los procesos y actividades tanto de TI como de negocio para asegurar
5.56%	Revisar regularmente para detectar patrones reiterados de fallos de cumplimiento. Si procede, mejorar tanto las políticas, los estándares, los procedimientos y las metodologías como los procesos y actividades asociados.	0%	0.00%	No se cuenta con un procedimiento para detectar patrones reiterados de fallos de cumplimiento.
5.56%	Obtener confirmación regularmente del cumplimiento de las políticas internas por parte de los propietarios de procesos de TI y de negocio, así como de los directores de las unidades.	100%	5.56%	6I01. Evaluación de desempeño.
5.56%	Realizar revisiones regulares internas y externas (y, si procede, independientes) para evaluar los niveles de cumplimiento.	100%	5.56%	8P02. Auditorias internas de la calidad
5.56%	Si es necesario, obtener declaraciones de los proveedores de servicio TI externos acerca de su nivel de cumplimiento con las leyes y regulaciones aplicables.	0%	0.00%	No se cuenta con un procedimiento para obtener declaraciones de los proveedores de servicio TI externos acerca de su nivel de cumplimiento con las leyes y regulaciones.
5.56%	Si es necesario, obtener declaraciones de los socios de negocio sobre sus niveles de cumplimiento de las leyes y regulaciones en materia de transacciones electrónicas entre compañías.	0%	0.00%	Falta un proceso para obtener declaraciones de los socios de negocio sobre sus niveles de cumplimiento de las leyes y regulaciones.
5.56%	Supervisar e informar de los incidentes de incumplimiento y, si es necesario, investigar la causa raíz.	100%	5.56%	8P04. Control de servicios no conformes 8P02. Auditorias internas de la calidad
5.56%	Consolidar a nivel empresarial los informes sobre requisitos legales, regulatorios y contractuales, involucrando a todas las unidades de negocio.	50%	2.78%	7P07. Gestión de requisitos legales. Sin embargo se requiere un proceso definido para consolidar informes sobre requisitos legales, regulatorios y contractuales a todas las unidades del negocio.

Resumen	
Impacto	62.50%
Probabilidad	48.33%
Riesgo Inherente	30.21%
Efectividad del Control	51.67%
Riesgo Residual	14.60%

Anexo 2: Metodología aplicada OPC CCSS

1. Introducción

Esta aplicación de la metodología se enfocará principalmente en la gestión de la seguridad de la información, y como se debe desarrollar en la Operadora de Pensiones Complementarías de la CCSS. El desarrollo de la investigación utilizará como referencia los estándares ISO 27001 y COBIT 5, aprovechando los diferentes controles que estos proponen, para definir las mejores prácticas que deberían utilizarse para asegurar que la gestión de la seguridad de la información se está realizando de manera satisfactoria en la Operadora de Pensiones Complementarías de la CCSS.

Se evaluará la capacidad de gestión de seguridad de la información que tiene una institución o empresa y observar los resultados reales que está va a facilitar. La aplicación de la metodología se aplicará en la Operadora de Pensiones Complementarias de la CCSS.

1.1 Objetivo general

Evaluar el umbral de riesgo de la seguridad de la información en la Operadora de Pensiones Complementarias de la Caja Costarricense del Seguro Social (OPC CCSS).

2. Valorización del riesgo en los procesos

A continuación, se presentan los riesgos asociados a los procesos de COBIT 5 aplicados a la Operadora. En el estudio, se valorará el total de los 34 procesos que desarrolla COBIT 5, que se muestran en la imagen.

Imagen 1: Procesos de Gobierno de TI Empresarial, COBIT 5

4.103.1 Análisis de riesgo

En este apartado se detallará el análisis de riesgo realizado a los 37 procesos de COBIT 5 aplicados a la OPC CCSS mostrando como resultado final para cada proceso su respectivo impacto, probabilidad, riesgo inherente, efectividad actual de los controles y el riesgo residual.

3.1.1 EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno

Proceso: EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	
Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.	
Practicas de Gestión:	
EDM01.01 Evaluar el sistema de gobierno. *EDM01.02 Orientar el sistema de gobierno.* *EDM01.03 Supervisar el sistema de gobierno.*	
Riesgos Asociados:	
No identificar, ni comprometerse continuamente con las partes interesadas de la empresa	*Medio*

No realizar una estimación actual y futura del diseño del gobierno de TI de la empresa	*Medio*
No informar a los líderes, ni obtener su apoyo, su aceptación y compromiso	*Muy Alto*
No definir la información necesaria para una toma de decisiones informadas	*Muy Alto*
No supervisar la ejecución y la efectividad del gobierno de TI de la empresa	*Alto*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**66.67%**
Probabilidad	**54.00%**
Riesgo Inherente	**36.00%**
Efectividad del Control	**46.00%**
Riesgo Residual	**19.44%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Evaluar el sistema de gobierno***" es **Baja** de **19.44%**, con una probabilidad de ocurrencia **Alta** de **54.00%**, que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **66.67%** y la efectividad de los controles es **Definida** de **46.00%**.

3.1.2 EDM02 Asegurar la Entrega de Beneficios

Proceso: EDM02 Asegurar la Entrega de Beneficios	
Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costes aceptables.	
Practicas de Gestión:	
EDM02.01 Evaluar la optimización de valor. *EDM02.02 Orientar la optimización del valor.* *EDM02.03 Supervisar la optimización del valor.*	
Riesgos Asociados:	
Al no evaluar continuamente las inversiones, servicios y activos del portafolio de TI, no se puede determinar si se alcanzan los objetivos de la empresa y su valor.	*Alto*
No identificar los cambios de dirección que necesita la Operadora para optimizar la creación de valor.	*Medio*
No orientar los principios ni las prácticas de gestión de valor, no dando el valor óptimo de las inversiones TI.	*Medio*
No supervisar los indicadores clave ni sus métricas para determinar el grado en que el negocio está generando el valor y los beneficios previstos de los servicios e inversiones	*Medio*

TI.	
No identificar los problemas significativos ni considerar las acciones correctivas.	*Alto*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**56.67%**
Probabilidad	**45.50%**
Riesgo Inherente	**25.78%**
Efectividad del Control	**54.50%**
Riesgo Residual	**11.73%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Asegurar la Entrega de Beneficios***" es **Insignificante** de **11.73%**, con una probabilidad de ocurrencia **Media** de **45.00%**, que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **56.67%** y la efectividad de los controles es **Definida** de **54.50%**.

3.1.3 EDM03 Asegurar la Optimización del Riesgo

Proceso: EDM03 Asegurar la Optimización del Riesgo	
Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.	
Practicas de Gestión:	
EDM03.01 Evaluar la gestión de riesgos. *EDM03.02 Orientar la gestión de riesgos.* *EDM03.03 Supervisar la gestión de riesgos.*	
Riesgos Asociados:	
No examinar ni evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la Operadora.	*Medio*
No considerar, cuando el apetito de riesgo de la Operadora no es apropiado y el riesgo sobre el valor de la Operadora relacionado con el uso de TI no es identificado ni gestionado.	*Alto*
No contar con prácticas de gestión de riesgos para proporcionar una seguridad razonable para asegurar que el riesgo de TI actual no excede el apetito de riesgo establecido por Junta Directiva.	*Alto*
No supervisar los objetivos ni las métricas clave de los procesos de gestión de riesgo.	*Medio*

No establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución.	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**56.67%**
Probabilidad	**17.81%**
Riesgo Inherente	**10.09%**
Efectividad del Control	**82.19%**
Riesgo Residual	**1.80%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Asegurar la Optimización del Riesgo***" es **Insignificante** de **1.80%**, con una probabilidad de ocurrencia **Baja** de **17.81%**, que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **56.67%** y la efectividad de los controles es **Medible** de **82.19%**.

3.1.4 EDM04 Asegurar la Optimización de Recursos

Proceso: EDM04 Asegurar la Optimización de Recursos	
Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.	
Practicas de Gestión:	
EDM04.01 Evaluar la gestión de recursos. *EDM04.02 Orientar la gestión de recursos.* *EDM04.03 Supervisar la gestión de recursos.*	
Riesgos Asociados:	
No cumplir de manera óptima con las necesidades de la empresa, al no examinar ni evaluar continuamente la necesidad actual y futura de recursos relacionados con TI, ni las opciones para la asignación de recursos y los principios de asignación y gestión.	*Alto*
No adoptar principios de gestión de recursos, que permitan un uso óptimo de los recursos de TI a lo largo de su ciclo de vida económico.	*Medio*
No supervisar los objetivos y métricas clave de los procesos de gestión de recursos de TI.	*Medio*
No identificar, no seguir y no informar los objetivos y métricas para su resolución las desviaciones o los problemas de TI.	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**54.17%**
Probabilidad	**36.16%**
Riesgo Inherente	**19.58%**
Efectividad del Control	**63.84%**
Riesgo Residual	**7.08%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Asegurar la Optimización de Recursos***" es **Insignificante** de **7.08%**, con una probabilidad de ocurrencia **Media** de **36.81%**, que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **54.17%** y la efectividad de los controles es **Medible** de **63.84%**.

3.1.5 EDM05 Asegurar la Transparencia hacia las Partes Interesadas

Proceso: EDM05 Asegurar la Transparencia hacia las Partes Interesadas	
Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de TI de la empresa son transparentes, con aprobación por parte de las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.	
Practicas de Gestión:	
EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas. *EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes.* *EDM05.03 Supervisar la comunicación con las partes interesadas.*	
Riesgos Asociados:	***Impacto***
No cumplir con los requisitos de los diferentes interesados.	*Alto*
No establecer principios de comunicación hacia las partes interesadas.	*Medio*
Comunicación y elaboración de informes poco eficaces.	*Medio*
Falta de mecanismos para asegurar la calidad y completitud de la información en los informes.	*Bajo*
No realizar los informes obligatorios para las partes interesadas.	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**50.00%**
Probabilidad	**84.00%**
Riesgo Inherente	**42.00%**
Efectividad del Control	**16.00%**
Riesgo Residual	**35.28%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Asegurar la Transparencia hacia las Partes Interesadas***" es **Media** de **35.28%**, con una probabilidad de ocurrencia **Siempre** de **84.00%**, que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **50.00%** y la efectividad de los controles es **Inicial** de **16.00%**.

3.1.6 APO01 Gestionar el Marco de Gestión de TI

Proceso: APO01 Gestionar el Marco de Gestión de TI	
Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.	
Practicas de Gestión:	
APO01.01 Definir la estructura organizativa *APO01.02 Establecer roles y responsabilidades* *APO01.03 Mantener los elementos catalizadores del sistema de gestión* *APO01.04 Comunicar los objetivos y la dirección de gestión* *APO01.05 Optimizar la ubicación de la función de TI* *APO01.06 Definir la propiedad de la información (datos) y del sistema* *APO01.07 Gestionar la mejora continua de los procesos* *APO01.08 Mantener el cumplimiento con las políticas y procedimientos*	
Riesgos Asociados:	***Impacto***
Necesidades y prioridades de TI, no reflejadas en el negocio	*Alto*
No establecimiento y comunicación de las responsabilidades del personal de TI	*Alto*
Necesidades del negocio no reflejadas en los objetivos de TI	*Muy Alto*
No rendición de cuentas del área de TI	*Medio*
Catalizadores del sistema de gestión y control de TI no integrados y alineados con la filosofía, estilo operativo y gestión de la empresa	*Medio*
Falta de comprensión y sensibilización de los objetivos y dirección de TI, por parte de los usuarios de la Operadora	*Bajo*

Mal posicionamiento de TI en la estructura organizativa de la Operadora	*Alto*
No definición y mantenimiento de los responsables de la información y los sistemas de información	*Medio*
No clasificación de la información y los sistemas para garantizar su protección	*Medio*
Falta de evaluación, planificación y ejecución de una mejora continua en los procesos de TI conforme los objetivos de la Operadora	*Alto*
No consideración del impacto en los catalizadores de procesos de TI cuando estos se actualizan	*Bajo*
No mantener el cumplimiento y la medición de las políticas de TI	*Alto*
No hacer cumplir las consecuencias del no cumplimiento o desempeño inadecuado	*Medio*
No analizar las tendencias y el rendimiento para considerarlos en la mejora del marco de control	*Bajo*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**54.76%**
Probabilidad	**17.27%**
Riesgo Inherente	**9.46%**
Efectividad del Control	**82.73%**
Riesgo Residual	**1.63%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Asegurar la Transparencia hacia las Partes Interesadas***" es **Insignificante** de **1.63%**, con una probabilidad de ocurrencia **Baja** de **17.27%**, que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **50.00%** y la efectividad de los controles es **Optimizada** de **82.73%**.

3.1.7 APO02 Gestionar la Estrategia

Proceso: APO02 Gestionar la Estrategia	
Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos.	
Practicas de Gestión:	
APO02.01 Comprender la dirección de la empresa. *APO02.02 Evaluar el entorno, capacidades y rendimiento actuales.* *APO02.03 Definir el objetivo de las capacidades de TI.* *APO02.04 Realizar un análisis de diferencias.* *APO02.05 Definir el plan estratégico y la hoja de ruta.* *APO02.06 Comunicar la estrategia y la dirección de TI.*	
Riesgos Asociados:	***Impacto***
No considerar la estrategia, los objetivos futuros y los procesos de negocio de la Operadora.	*Alto*
No tomar en cuenta el entorno externo como los motivadores de la industria, reglamentos relevantes, bases para la competencia.	*Alto*
Falta de evaluación del rendimiento del negocio actual y las capacidades de TI.	*Medio*
No identificación de los problemas que está experimentando la Operadora, y la no generación de recomendaciones.	*Muy Alto*
No consideración aspectos diferenciadores, impactos financieros, y opciones de proveedores de servicios.	*Medio*
Falta de consideración de los procesos de negocio actuales, los problemas presentados, los estándares de referencia, las mejores prácticas, tecnologías emergentes, propuestas de innovación y el entorno de TI, para definir los objetivos de negocio, las capacidades de TI y los servicios necesarios.	*Alto*
No identificación de las diferencias entre el entorno actual y el deseado por la Operadora, y no poder optimizar las inversiones y activos de TI.	*Alto*
Plan estratégico de TI que no contribuya a los objetivos estratégicos de la empresa.	*Medio*
No mitigación de los riesgos de TI por una mala orientación de las estrategias de TI para lograr los objetivos de la Operadora.	*Medio*
Falta de conciencia y comprensión del negocio y los objetivos y dirección de TI por parte del Gobierno Corporativo y colaboradores de la Operadora.	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**60.00%**
Probabilidad	**63.39%**
Riesgo Inherente	**38.03%**
Efectividad del Control	**36.61%**
Riesgo Residual	**24.11%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar la Estrategia***" es **Baja** de **24.11%**, con una probabilidad de ocurrencia **Alta** de **63.39%**, que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **60.00%** y la efectividad de los controles es **Repetible pero intuitivo** de **36.61%**.

3.1.8 APO03 Gestionar la Arquitectura Empresarial

Proceso: APO03 Gestionar la Arquitectura Empresarial	
Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Definir los requisitos para la taxonomía, las normas, las directrices, los procedimientos, las plantillas y las herramientas y proporcionar un vínculo para estos componentes. Mejorar la adecuación, aumentar la agilidad, mejorar la calidad de la información y generar ahorros de costes potenciales mediante iniciativas tales como la reutilización de bloques de componentes para los procesos de construcción.	
Practicas de Gestión:	
APO03.01 Desarrollar la visión de la arquitectura de empresa. *APO03.02 Definir la arquitectura de referencia.* *APO03.03 Seleccionar las oportunidades y las soluciones.* *APO03.04 Definir la implantación de la arquitectura.* *APO03.05 Proveer los servicios de arquitectura empresarial.*	
Riesgos Asociados:	***Impacto***
No contar con una visión de la arquitectura, que permita descripción de alto nivel de las arquitecturas de partida y objetivo, nuevas capacidades, así como preocupaciones de las partes interesadas en su implementación.	*Medio*
No contar con una adecuada definición de la arquitectura donde describa la situación actual y su objetivo.	*Medio*
No contar con procedimiento de racionalización de las desviaciones entre las arquitecturas de referencia	*Medio*
No mantener un registro y procedimiento para asegurar que las iniciativas relacionadas con la arquitectura estén alineadas y que sean parte del cambio general en la empresa.	*Medio*
Falta un plan de implementación y de migración de la arquitectura.	*Medio*
No contar con un procedimiento para asegurar que se proporciona el valor y que se disponen de los recursos necesarios para finalizar los trabajos	*Medio*
No contar con una provisión de los servicios de arquitectura empresarial que incluya guías y supervisión de los proyectos a implementar, maneras de trabajar según contrato, valor aportado y supervisión de cumplimiento.	*Medio*
Falta una aprobación formal del documento al que se hace referencia los procesos de gestión.	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**50.00%**
Probabilidad	**56.15%**
Riesgo Inherente	**28.08%**
Efectividad del Control	**43.85%**
Riesgo Residual	**15.77%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar la Arquitectura Empresarial***" es **Insignificante** de **15.77%**, con una probabilidad de ocurrencia **Alta** de **56.15%**, que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Medio** de **50.00%** y la efectividad de los controles es **Repetible pero intuitivo** de **43.85%**.

3.1.9 APO05 Gestionar el Portafolio

Proceso: APO05 Gestionar el Portafolio	
Ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación. Evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos así como en su valor y riesgo corporativo. Mover los programas seleccionados al portafolio de servicios activos listos para ser ejecutados. Supervisar el rendimiento global del portafolio de servicios y programas, proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas.	
Practicas de Gestión:	
APO05.01 Establecer la mezcla del objetivo de inversión. *APO05.02 Determinar la disponibilidad y las fuentes de fondos.* *APO05.03 Evaluar y seleccionar los programas a financiar.* *APO05.04 Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones.* *APO05.05 Mantener los portafolios.* *APO05.06 Gestionar la consecución de beneficios.*	
Riesgos Asociados:	***Impacto***
No revisar la claridad de las estrategias y servicios corporativos de TI.	*Medio*
No mantener un procedimiento para definir la mezcla de inversión, basada en los costes, la alineación con la estrategia y medidas financieras	*Alto*
No contar con un procedimiento para determinar las fuentes potenciales de fondos,	*Alto*

diferentes opciones de financiación y las implicaciones.	
No contar con un procedimiento para determinar las fuentes potenciales de fondos, diferentes opciones de financiación y las implicaciones.	*Alto*
Falta un procedimiento para evaluar y seleccionar los programas a financiar.	*Medio*
No mantener un método para supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones.	*Alto*
No mantener un registro los portafolios de programas y proyectos de inversión, servicios de TI y activos de TI.	*Alto*
No supervisar los beneficios de proporcionar y mantener servicios y capacidades TI apropiadas	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	***60.42%***
Probabilidad	***25.36%***
Riesgo Inherente	***15.32%***
Efectividad del Control	***74.64%***
Riesgo Residual	***3.88%***

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar el Portafolio***" es **Insignificante** de **3.88%**, con una probabilidad de ocurrencia **Baja** de **25.36%**, que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **60.42%** y la efectividad de los controles es **Administrado y Medible** de **74.64%**.

3.1.10 APO06 Gestionar el Presupuesto y los Costes

Proceso: APO06 Gestionar el Presupuesto y los Costes
Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuesto, coste y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costes a la empresa. Consultar a las partes interesadas para identificar y controlar los costes totales y los beneficios en el contexto de los planes estratégicos y tácticos de TI, e iniciar acciones correctivas cuando sea necesario.
Practicas de Gestión:

APO06.01 Gestionar las finanzas y la contabilidad. *APO06.02 Priorizar la asignación de recursos.* *APO06.03 Crear y mantener presupuestos.* *APO06.04 Modelar y asignar costes.* *APO06.05 Gestionar costes.*	
Riesgos Asociados:	***Impacto***
No contar con un método de contabilización para todos los costes, inversiones y depreciaciones relacionadas con las TI.	*Alto*
"No manejar sistemas empresariales de medición para capturar y asignar los costes reales, y análisis de las desviaciones entre las previsiones y los costes reales	*Alto*
Falta de procesos para la toma de decisiones, así como priorizar la asignación de recursos y definición de las reglas para las inversiones	*Medio*
No contar con un proceso que permita considerar el uso potencial de proveedores, opciones de compra, desarrollo y alquiler.	*Medio*
No contar con la preparación de presupuestos que refleje las prioridades de inversión con base en los programas habilitados por TI y servicios de TI.	*Medio*
No mantener un modelo de costes de TI basado en la definición del servicio, asegurando que la asignación de costes de los servicios es identificable, medible y predecible, que incluya proveedores de servicio.	*Medio*
No contar con una revisión para regular y comparar la idoneidad del modelo de costes/prorrateo en relación con la evolución del negocio y las actividades de TI que le dan soporte.	*Medio*
No contar con un proceso de gestión de costes, con el fin de comprar los costes reales con los presupuestos.	*Alto*
Falta de supervisión y comunicación de los costes en caso de desviaciones, así como la evaluación de su impacto en los procesos y servicios empresariales.	*Alto*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**57.41%**
Probabilidad	**24.19%**
Riesgo Inherente	**13.89%**
Efectividad del Control	**75.81%**
Riesgo Residual	**3.36%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar el Presupuesto y los Costes***" es **Insignificante** de **3.36%**, con una probabilidad de ocurrencia **Baja** de **24.19%**, que en caso de materializarse algún

evento o incidente el impacto para la Operadora sería **Alto** de **57.41%** y la efectividad de los controles es **Optimizada** de **75.81%**.

3.1.11 APO07 Gestionar los Recursos Humanos

Proceso: APO07 Gestionar los Recursos Humanos	
Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.	
Practicas de Gestión:	
APO07.01 Mantener la dotación de personal suficiente y adecuada. *APO07.02 Identificar personal clave de TI.* *APO07.03 Mantener las habilidades y competencias del personal.* *APO07.04 Evaluar el desempeño laboral de los empleados.* *APO07.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio.* *APO07.06 Gestionar el personal contratado.*	
Riesgos Asociados:	***Impacto***
No contar con una evaluación de las necesidades de personal en forma regular o en cambios importantes en la empresa, operativos o en los entornos.	*Medio*
No contar con método para identificar el personal clave de TI, así también el no reducir la dependencia de una sola persona.	*Muy Alto*
No gestionar las habilidades y competencias necesarias del personal.	*Medio*
No verificar regularmente que el personal tenga las competencias necesarias para cumplir con sus funciones	*Alto*
Falta un procedimiento que proporcione a los empleados un aprendizaje permanente y oportunidades para mantener sus conocimientos, habilidades y competencias	*Muy Alto*
No mantener un procedimiento para la evaluación del desempeño laboral de los empleados.	*Medio*
No contemplar un seguimiento de la demanda actual y futura de recursos humanos para el negocio y TI	*Alto*
No mantener un procedimiento para identificar las carencias y proporcionar datos de entrada a los planes de aprovisionamiento	*Medio*
Falta un método que asegure que los consultores y el personal contratado conocen y cumplen las políticas de la organización, así como los requisitos contractuales	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	***61.11%***
Probabilidad	***16.67%***

Riesgo Inherente	***10.19%***
Efectividad del Control	***83.33%***
Riesgo Residual	***1.70%***

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar los Recursos Humanos***" es **Insignificante** de **1.70%**, con una probabilidad de ocurrencia **Insignificante** de **16.67%**, que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **61.11%** y la efectividad de los controles es **Optimizada** de **83.33%**.

3.1.12 APO08 Gestionar las relaciones

Proceso: APO08 Gestionar las relaciones	
Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándolas hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usando términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves.	
Practicas de Gestión:	
APO08.01 Entender las expectativas del negocio. *APO08.02 Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio.* *APO08.03 Gestionar las relaciones con el negocio.* *APO08.04 Coordinar y comunicar.* *APO08.05 Proveer datos de entrada para la mejora continua de los servicios.*	
Riesgos Asociados:	***Impacto***
No conocer o tener claridad del enfoque y expectativas actuales del negocio para TI.	*Alto*
No tener un procedimiento que ayude a identificar oportunidades potenciales para TI en beneficio de toda la empresa.	*Medio*
Falta un método de gestión para la relación de los clientes.	*Medio*
Falta un proceso para coordinar y comunicar el trabajo con las partes interesadas en la entrega de los servicios de TI y las soluciones proporcionadas.	*Medio*
Falta un procedimiento para mejorar y evolucionar continuamente los servicios basados en TI y la entrega del servicio.	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	***53.33%***

Probabilidad	***32.50%***
Riesgo Inherente	***17.33%***
Efectividad del Control	***67.50%***
Riesgo Residual	***5.63%***

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar las relaciones***" es **Insignificante** de **5.63%**, con una probabilidad de ocurrencia **Baja** de **32.50%**, que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **53.33%** y la efectividad de los controles es **Administrable y Medible** de **67.50%**.

3.1.13 APO09 Gestionar los acuerdos de servicio

Proceso: APO09 Gestionar los acuerdos de servicio	
Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la empresa, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento.	
Practicas de Gestión:	
APO06.01 Gestionar las finanzas y la contabilidad. *APO06.02 Priorizar la asignación de recursos.* *APO06.03 Crear y mantener presupuestos.* *APO06.04 Modelar y asignar costes.* *APO06.05 Gestionar costes.*	
Riesgos Asociados:	***Impacto***
Falta de análisis de los requisitos del negocio y como los servicios de TI y los SLA´s, soportan los procesos de negocio.	*Alto*
No definición de los servicios existentes para los colaboradores de la Operadora.	*Medio*
No definir los SLA´s según los servicios existentes internos.	*Alto*
Falta de supervisión de los niveles de servicio y sus mejoras.	*Alto*
No existencia de un calendario de revisión de SLA´s.	*Alto*
No colaboración entre el negocio y TI para la creación de SLA´s	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**61.11%**
Probabilidad	**51.25%**
Riesgo Inherente	**31.32%**
Efectividad del Control	**48.75%**
Riesgo Residual	**16.05%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar los acuerdos de servicio***" es **Insignificante** de **16.05%**, con una probabilidad de ocurrencia **Alta** de **51.25%**, que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **61.11%** y la efectividad de los controles es **Definida** de **48.75%**.

3.1.14 APO10 Gestionar los Proveedores

Proceso: APO10 Gestionar los Proveedores	
Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.	
Practicas de Gestión:	
APO10.01 Identificar y evaluar las relaciones y contratos con proveedores. *APO10.02 Seleccionar proveedores.* *APO10.03 Gestionar contratos y relaciones con proveedores.* *APO10.04 Gestionar el riesgo en el suministro.* *APO10.05 Supervisar el cumplimiento y el rendimiento del proveedor.*	
Riesgos Asociados:	***Impacto***
No evaluación de contratos, proveedores, contratos actuales y alternativos.	*Medio*
No identificación de la relevancia y criticidad de los proveedores y contratos asociados.	*Medio*
Mala selección de proveedores por no utilizar practicas justas, formales y requisitos optimizados.	*Crítico*
No gestionar, mantener y supervisar los contratos y la entrega de servicios.	*Alto*
No asegurar que los nuevos contratos o los cambios son conformes a las normas de la empresa, las leyes y las regulaciones.	*Muy Alto*
No gestionar los conflictos contractuales.	*Alto*
No identificar y no gestionar los riesgos relacionados con la capacidad de los proveedores de proporcionar de manera continua una entrega del servicio segura,	*Alto*

eficaz y eficiente.	
No revisar periódicamente el rendimiento general de los proveedores, el cumplimiento con los requisitos contractuales y el valor de lo pagado y tratar las incidencias identificadas.	*Alto*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**68.75%**
Probabilidad	**13.90%**
Riesgo Inherente	**9.55%**
Efectividad del Control	**86.10%**
Riesgo Residual	**1.33%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar los Proveedores***" es **Insignificante** de **1.33%**, con una probabilidad de ocurrencia **Insignificante** de **13.90%**, que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Muy Alto** de **68.75%** y la efectividad de los controles es **Optimizada** de **86.10%**.

3.1.15 APO11 Gestionar la Calidad

Proceso: APO11 Gestionar la Calidad	
Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.	
Practicas de Gestión:	
APO11.01 Establecer un sistema de gestión de la calidad (SGC). *APO11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.* *APO11.03 Enfocar la gestión de la calidad en los clientes.* *APO11.04 Supervisar y hacer controles y revisiones de calidad.* *APO11.05 Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.* *APO11.06 Mantener una mejora continua*	
Riesgos Asociados:	***Impacto***
No mantener un Sistema de Gestión de Calidad que proporcione una aproximación a la	*Alto*

gestión de la calidad para la información, la tecnología y los procesos de negocio	
Falta un procedimiento que permita identificar y mantener los requisitos, normas, procedimientos y prácticas de los procesos clave para orientar a la organización en el cumplimiento del SGC.	*Alto*
No enfocar la gestión de calidad hacia los clientes.	*Medio*
No contar con un método de supervisión de la calidad de los procesos y servicios, satisfacción del cliente con la calidad, y el valor que proporciona el SGC.	*Medio*
No incorporar la gestión de calidad en la implementación de soluciones y la entrega de servicios.	*Medio*
No mantener un procedimiento que promueva una cultura de mejora continua de la calidad, en la gestión de calidad.	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	***55.56%***
Probabilidad	***12.12%***
Riesgo Inherente	***6.73%***
Efectividad del Control	***87.88%***
Riesgo Residual	***0.82%***

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar los Proveedores***" es **Insignificante** de **0.82%**, con una probabilidad de ocurrencia **Insignificante** de **12.12%**, que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **55.56%** y la efectividad de los controles es **Optimizada** de **87.88%**.

3.1.16 APO12 Gestionar el Riesgo

Proceso: APO12 Gestionar el Riesgo	
Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.	
Practicas de Gestión:	
APO12.01 Recopilar datos. *APO12.02 Analizar el riesgo.* *APO12.03 Mantener un perfil de riesgo.* *APO12.04 Expresar el riesgo.* *APO12.05 Definir un portafolio de acciones para la gestión de riesgos.* *APO12.06 Responder al riesgo.*	
Riesgos Asociados:	***Impacto***
Inefectividad a la hora de catalizar una identificación, análisis y notificación de los riesgos relacionados con TI.	*Medio*
Que la información que soporta las decisiones relacionadas con el riesgo no tome en cuenta al negocio y sus factores de riesgo.	*Alto*
No mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados.	*Alto*
No proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada.	*Medio*
No gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.	*Medio*
No responder de una forma oportuna Y con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.	*Alto*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**58.33%**
Probabilidad	**38.64%**
Riesgo Inherente	**22.54%**
Efectividad del Control	**61.36%**
Riesgo Residual	**8.71%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar el Riesgo***" es **Insignificante** de **8.71%**, con una probabilidad de

ocurrencia **Media** de **38.64%**, que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **58.33%** y la efectividad de los controles es **Administrado y Medible** de **61.36%**.

3.1.17 APO13 Gestionar la Seguridad

Proceso: APO13 Gestionar la Seguridad	
Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.	
Practicas de Gestión:	
APO13.01 Establecer y mantener un SGSI. *APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.* *APO13.03 Supervisar y revisar el SGSI.*	
Riesgos Asociados:	***Impacto***
No contar con un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio.	Muy Alto
Falta de alineación del SGSI a los requerimientos del proceso de negocio y la gestión de seguridad de la empresa.	Alto
No responder de forma efectiva a incidentes o situaciones relacionadas con la seguridad de la información.	Crítico
Falta de gestión de riesgos que atenten contra la seguridad de la información.	Alto
No se cuenta con seguridad de las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados.	Medio
Falta seguridad de que las recomendaciones se implementan como parte integral del desarrollo de soluciones y servicios.	Medio
Aumento de inefectividad en el plan de seguridad de la información (SGSI).	Medio
No comunicar la necesidad y los beneficios de la mejora continua de la seguridad de información.	Medio
Falta de análisis de datos sobre el SGSI.	Medio
Aumento de no conformidades en el SGSI.	Alto
No promover una cultura de seguridad y de mejora continua.	Alto

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**72.73%**
Probabilidad	**35.26%**
Riesgo Inherente	**25.65%**
Efectividad del Control	**64.74%**

Riesgo Residual	**9.04%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar la Seguridad***" es **Insignificante** de **9.04%**, con una probabilidad de ocurrencia **Media** de **35.26%**, que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Muy Alto** de **72.73%** y la efectividad de los controles es **Administrado y Medible** de **64.74%**.

3.1.18 BAI01 Gestión de Programas y Proyectos

Proceso: BAI01 Gestión de Programas y Proyectos	
Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.	
Practicas de Gestión:	
BAI01.01 Mantener un enfoque estándar para la gestión de programas y proyectos. *BAI01.02 Iniciar un programa.* *BAI01.03 Gestionar el compromiso de las partes interesadas.* *BAI01.04 Desarrollar y mantener el plan de programa.* *BAI01.05 Lanzar y ejecutar el programa.* *BAI01.06 Supervisar, controlar e informar de los resultados del programa.* *BAI01.07 Lanzar e iniciar proyectos dentro de un programa.* *BAI01.08 Planificar proyectos.* *BAI01.09 Gestionar la calidad de los programas y proyectos.* *BAI01.10 Gestionar el riesgo de los programas y proyectos.* *BAI01.11 Supervisar y controlar proyectos.* *BAI01.12 Gestionar los recursos y los paquetes de trabajo del proyecto.* *BAI01.13 Cerrar un proyecto o iteración.* *BAI01.14 Cerrar un programa.*	
Riesgos Asociados:	***Impacto***
No mantener un enfoque estándar para la gestión de programas y proyectos que posibilite revisiones y tomas de decisión de gobierno, actividades de gestión de la entrega, que se enfoquen en la consecución de valor y de objetivos para el negocio de una forma consistente.	*Medio*
Falta de planificación, identificación y compromiso de las partes interesadas y la gestión de sus expectativas.	*Alto*
No mantener las bases iniciales del plan del programa y su ciclo de vida económico, asegurando el alineamiento con los objetivos estratégicos y reflejando el estado actual y los conocimientos obtenidos hasta el momento.	*Medio*
Falta de un programa apropiado para adquirir y dirigir los recursos necesarios para lograr las metas y beneficios definidos en el plan del programa.	*Medio*
Falta de supervisión y control del rendimiento del programa (entrega de soluciones) y	*Alto*

de la organización (valor/resultado) versus el plan durante el ciclo de vida económico completo de la inversión.	
Falta de entendimiento entre las partes interesadas por falta de documentación que ayude a confirmar y desarrollar la naturaleza y alcance del proyecto dentro del programa general de inversiones de TI.	*Alto*
Falta de un plan de proyecto formal, aprobado e integrado (que cubra los recursos del negocio y de TI), para guiar la ejecución del proyecto y controlarlo durante toda su vida.	*Medio*
Alcance de los proyectos mal dimensionado por falta de claridad y no tomar en cuenta el aumento de la capacidad del negocio.	*Medio*
Que el plan de procesos y prácticas de gestión de la calidad, no se encuentre alineado al SGC que describe el enfoque de calidad del programa y el proyecto y cómo será implementado.	*Medio*
No eliminar o minimizar los riesgos específicos asociados con los programas y proyectos por falta de planificación, identificación, análisis, respuesta, supervisión y control de las áreas o eventos que tienen el potencial de causar cambios no deseados.	*Alto*
No evaluar el impacto de las desviaciones en el proyecto y el programa general y no comunicar los resultados a las partes interesadas clave.	*Medio*
No gestionar los paquetes de trabajo mediante requerimientos formales de autorización y aceptación por parte del recurso de TI.	*Alto*
Falta de visibilidad cuando se termina un proyecto, con respecto a si se cumplieron o no los resultados y valor planeado.	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**56.41%**
Probabilidad	**49.10%**
Riesgo Inherente	**27.70%**
Efectividad del Control	**50.90%**
Riesgo Residual	**13.60%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestión de Programas y Proyectos***" es **Insignificante** de **13.60%**, con una probabilidad de ocurrencia **Media** de **49.10%,** que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **56.41%** y la efectividad de los controles es **Definida** de **50.90%**.

3.1.19 BAI02 Gestionar la Definición de Requisitos

Proceso: BAI02 Gestionar la Definición de Requisitos	
Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costes y beneficios relacionados, análisis de riesgo y aprobación de los requerimientos y soluciones propuestas.	
Practicas de Gestión:	
BAI02.01 Definir y mantener los requerimientos técnicos y funcionales de negocio. *BAI02.02 Realizar un estudio de viabilidad y proponer soluciones alternativas.* *BAI02.03 Gestionar los riesgos de los requerimientos.* *BAI02.04 Obtener la aprobación de los requerimientos y soluciones.*	
Riesgos Asociados:	***Impacto***
No contar un procedimiento para definir y mantener los requerimientos técnicos y funcionales de negocio.	*Alto*
No mantener un estudio de viabilidad de las potenciales soluciones alternativas, evaluando su viabilidad y seleccionando la opción preferida.	*Medio*
Falta una gestión para identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos.	*Alto*
No contar con una realimentación de las partes interesadas afectadas y, en las fases clave predeterminadas de acuerdo con una aprobación de los requerimientos y soluciones.	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	***58.33%***
Probabilidad	***34.71%***
Riesgo Inherente	***20.25%***
Efectividad del Control	***65.29%***
Riesgo Residual	***7.03%***

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar la Definición de Requisitos***" es **Insignificante** de **7.03%**, con una probabilidad de ocurrencia **Media** de **34.71%,** que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **58.33%** y la efectividad de los controles es **Administrado y Medible** de **65.29%**.

3.1.20 BAI03 Gestionar la Identificación y Construcción de Soluciones

Proceso: BAI03 Gestionar la Identificación y Construcción de Soluciones	
Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.	
Practicas de Gestión:	
BAI03.01 Diseñar soluciones de alto nivel. *BAI03.02 Diseñar los componentes detallados de la solución.* *BAI03.03 Desarrollar los componentes de la solución.* *BAI03.04 Obtener los componentes de la solución.* *BAI03.05 Construir soluciones.* *BAI03.06 Realizar controles de calidad.* *BAI03.07 Preparar pruebas de la solución.* *BAI03.08 Ejecutar pruebas de la solución.* *BAI03.09 Gestionar cambios a los requerimientos.* *BAI03.10 Mantener soluciones.* *BAI03.11 Definir los servicios TI y mantener el catálogo de servicios.*	
Riesgos Asociados:	***Impacto***
Deficiencia al asegurar el alineamiento a estrategia TI con la arquitectura empresarial.	*Medio*
Que los diseños de las soluciones no sean de alto nivel.	*Medio*
No contar con un mecanismo para asegurar que las partes interesadas participen activamente en el diseño y en la aprobación de cada versión.	*Medio*
No incluir ANSs y OLAs internos y externos en el diseñado detallado de soluciones.	*Medio*
No considerar todos los componentes (procesos de negocio y automatización relacionada y controles manuales, aplicaciones soporte de TI, servicios de infraestructura y productos tecnológicos y proveedores/fabricantes) al desarrollar y documentar soluciones.	*Alto*
No contar con métodos de desarrollo, estándares de documentación, requerimientos de calidad (QA) y estándares de aprobación.	*Medio*
No contar con un procedimiento para asegurar que todos los requerimientos legales y contractuales son identificados y cumplidos por el proveedor.	*Alto*
No integrar las soluciones con las actividades de los procesos de negocio.	*Medio*
No implementar controles medidas de seguridad y 'auditabilidad' durante la configuración e integración	*Alto*
Ejecutar un plan de calidad (QA) que no esté alineado con el Sistema de Gestión de Calidad.	*Medio*
No contar con un plan de pruebas y entornos para probar los componentes individualmente y de la solución integrada.	*Medio*
No ejecutar pruebas durante el desarrollo	*Alto*
No incluir en las pruebas de solución a los dueños de los procesos de negocio y usuarios finales en el equipo.	*Medio*
No realizar revisiones periódicas respecto a las necesidades de negocio y	*Medio*

requerimientos operacionales	
No contar con un plan para el mantenimiento de la solución y componentes de la infraestructura.	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**54.44%**
Probabilidad	**33.60%**
Riesgo Inherente	**18.29%**
Efectividad del Control	**66.40%**
Riesgo Residual	**6.15%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar la Identificación y Construcción de Soluciones***" es **Insignificante** de **6.15%**, con una probabilidad de ocurrencia **Media** de **33.60%,** que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **54.44%** y la efectividad de los controles es **Administrado y Medible** de **66.40%**.

3.1.21 BAI04 Gestionar la Disponibilidad y la Capacidad

Proceso: BAI04 Gestionar la Disponibilidad y la Capacidad	
Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados.	
Practicas de Gestión:	
BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia. *BAI04.02 Evaluar el impacto en el negocio.* *BAI04.03 Planificar requisitos de servicio nuevos o modificados.* *BAI04.04 Supervisar y revisar la disponibilidad y la capacidad.* *BAI04.05 Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad.*	
Riesgos Asociados:	***Impacto***
No evaluar la disponibilidad, el rendimiento y la capacidad de los servicios y recursos, con el fin de asegurar que se encuentra disponible una capacidad y un rendimiento	*Muy Alto*

Falta de una línea de referencia en disponibilidad, el rendimiento y la capacidad para comparaciones futuras.	*Medio*
No contar con un procedimiento para identificar adecuadamente los servicios importantes para la empresa, recursos de los procesos y dependencias del negocio.	*Alto*
No asegurar que el impacto de la indisponibilidad de recurso sea acordada y aceptada por el cliente.	*Medio*
No planificar y priorizar las implicaciones en la disponibilidad, el rendimiento y la capacidad de servicios nuevos y modificados.	*Medio*
No contar con un procedimiento para supervisar, medir, analizar, informar y revisar la disponibilidad, el rendimiento y la capacidad.	*Alto*
No revisar informes de análisis de tendencias para identificar cualquier cuestión y variación significativa.	*Medio*
Falta de un procedimiento para investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad.	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**58.33%**
Probabilidad	**33.60%**
Riesgo Inherente	**19.60%**
Efectividad del Control	**66.40%**
Riesgo Residual	**6.59%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar la Disponibilidad y la Capacidad***" es **Insignificante** de **6.59%**, con una probabilidad de ocurrencia **Media** de **33.60%,** que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **58.33%** y la efectividad de los controles es **Administrado y Medible** de **66.40%**.

3.1.22 BAI06 Gestionar los Cambios

Proceso: BAI06 Gestionar los Cambios
Gestione todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y

autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación.	
Practicas de Gestión:	
BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio. *BAI06.02 Gestionar cambios de emergencia.* *BAI06.03 Hacer seguimiento e informar de cambios de estado.* *BAI06.04 Cerrar y documentar los cambios.*	
Riesgos Asociados:	***Impacto***
No evaluar las peticiones de cambio para determinar su impacto en los procesos de negocio y los servicios TI.	*Alto*
Falta de análisis en caso de que, el cambio afectará negativamente al entorno operativo e introduzca un riesgo inaceptable.	*Medio*
No asegurar que los cambios son registrados, priorizados, categorizados, analizados, autorizados, planificados y programados.	*Medio*
No gestionar cuidadosamente los cambios de emergencia para minimizar futuras incidencias.	*Alto*
No lograr garantizar que el cambio está controlado y se realiza de forma segura.	*Alto*
Falta de verificación en los cambios de emergencia son evaluados debidamente y autorizados una vez realizado.	*Alto*
No mantener un sistema de seguimiento e informe que documente los cambios rechazados y comunicación del estado de los cambios.	*Alto*
No asegurar que los cambios aprobados son implementados como estaban previstos.	*Medio*
No mantener un sistema para actualizar de manera consecuente la documentación de la solución y del usuario, así como los procedimientos a los que afecta cuando el cambio haya sido implementado.	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	***59.26%***
Probabilidad	***44.72%***
Riesgo Inherente	***26.50%***
Efectividad del Control	***55.28%***
Riesgo Residual	***11.85%***

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar los Cambios***" es **Insignificante** de **11.85%**, con una probabilidad de ocurrencia **Media** de **44.72%,** que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **59.26%** y la efectividad de los controles es **Definido** de **55.28%**.

3.1.23 BAI07 Gestionar la Aceptación del Cambio y la Transición

Proceso: BAI07 Gestionar la Aceptación del Cambio y la Transición	
Aceptar formalmente y hacer operativas las nuevas soluciones, incluyendo la planificación de la implementación, la conversión de los datos y los sistemas, las pruebas de aceptación, la comunicación, la preparación del lanzamiento, el paso a producción de procesos de negocio o servicios TI nuevos o modificados, el soporte temprano en producción y una revisión post-implementación.	
Practicas de Gestión:	
BAI07.01 Establecer un plan de implementación. *BAI07.02 Planificar la conversión de procesos de negocio, sistemas y datos.* *BAI07.03 Planificar pruebas de aceptación.* *BAI07.04 Establecer un entorno de pruebas.* *BAI07.05 Ejecutar pruebas de aceptación.* *BAI07.06 Pasar a producción y gestionar los lanzamientos.* *BAI07.07 Proporcionar soporte en producción desde el primer momento.* *BAI07.08 Ejecutar una revisión postimplantación.*	
Riesgos Asociados:	***Impacto***
No establecer un plan de gestión de implementación que cubra la conversión de datos y sistemas y criterios relevantes.	*Medio*
No contar con una planificación para la conversión de procesos de negocio, sistemas y datos de los servicios de TI e infraestructuras.	*Medio*
No contar con un plan de pruebas de aceptación basado en estándares corporativos.	*Medio*
Falta definir y establecer un entorno seguro de pruebas.	*Alto*
No probar los cambios independientemente, de acuerdo con el plan de pruebas definido.	*Medio*
No mantener un procedimiento definido de pase a producción y gestión de la solución.	*Medio*
No contar con procedimiento para dar soporte en producción desde el primer momento a los usuarios y a las operaciones de TI durante un periodo de tiempo acordado	*Medio*
No ejecutar una revisión postimplantación para confirmar salidas y resultados	*Alto*
Falta una aprobación formal del documento al que se hace referencia en la gestión de cambios.	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	***53.70%***
Probabilidad	***40.88%***
Riesgo Inherente	***21.96%***

Efectividad del Control	***59.12%***
Riesgo Residual	***8.98%***

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar la Aceptación del Cambio y la Transición***" es **Insignificante** de **8.98%**, con una probabilidad de ocurrencia **Media** de **40.88%,** que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **53.70%** y la efectividad de los controles es **Administrado y Medible** de **59.12%**.

3.1.24 BAI09 Gestionar los Activos

Proceso: BAI09 Gestionar los Activos	
Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para le negocio y que el software instalado cumple con los acuerdos de licencia.	
Practicas de Gestión:	
BAI09.01 Identificar y registrar activos actuales. *BAI09.02 Gestionar activos críticos* *BAI09.03 Gestionar el ciclo de vida de los activos.* *BAI09.04 Optimizar el coste de los activos.* *BAI09.05 Administrar licencias.*	
Riesgos Asociados:	***Impacto***
No mantener un registro actualizado y exacto de todos los activos de TI necesarios para la prestación de servicios	*Muy Alto*
No contar con la identificación de los activos que son críticos en la provisión de capacidad de servicio.	*Muy Alto*
Deficiencia en la gestión del ciclo de vida de los activos, para asegurar que se utilizan eficaz y eficientemente.	*Medio*
Falta un procedimiento para optimizar los costes y mantener el alineamiento con las necesidades del negocio.	*Medio*
No contar con una administración de licencias de software para mantener el número óptimo de licencias para soportar los requerimientos de negocio.	*Alto*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**66.67%**
Probabilidad	**16.67%**
Riesgo Inherente	**11.11%**
Efectividad del Control	**83.33%**
Riesgo Residual	**1.85%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar los Activos***" es **Insignificante** de **1.85%**, con una probabilidad de ocurrencia **Insignificante** de **16.67%,** que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **66.67%** y la efectividad de los controles es **Optimizado** de **83.33%**.

3.1.25 BAI10 Gestionar la Configuración

Proceso: BAI10 Gestionar la Configuración	
Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarios para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración.	
Practicas de Gestión:	
BAI10.01 Establecer y mantener un modelo de configuración. *BAI10.02 Establecer y mantener un repositorio de configuración y una base de referencia.* *BAI10.03 Mantener y controlar los elementos de configuración.* *BAI10.04 Generar informes de estado y configuración.* *BAI10.05 Verificar y revisar la integridad del repositorio de configuración.*	
Riesgos Asociados:	***Impacto***
No contar con un modelo de configuración que incluya la infraestructura, activos y servicios y la forma de registrar los elementos de configuración y sus relaciones.	*Medio*
No contar con un repositorio de configuración	*Alto*
No contar con bases de referencia de configuración.	*Alto*
Falta un procedimiento para mantener actualizado el repositorio de elementos de configuración.	*Alto*
No mantener un procedimiento para definir y elaborar informes de configuración sobre cambios.	*Medio*
Falta un procedimiento para revisar periódicamente el repositorio de configuración y verificar la integridad según el objetivo deseado.	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	***58.33%***
Probabilidad	***11.56%***
Riesgo Inherente	***6.74%***
Efectividad del Control	***88.44%***
Riesgo Residual	***0.78%***

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar la Configuración***" es **Insignificante** de **0.78%**, con una probabilidad de ocurrencia **Insignificante** de **11.56%,** que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **58.33%** y la efectividad de los controles es **Optimizado** de **88.44%**.

3.1.26 DSS01 Gestionar Operaciones

Proceso: DSS01 Gestionar Operaciones	
Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.	
Practicas de Gestión:	
DSS01.01 Ejecutar procedimientos operativos *DSS01.02 Gestionar servicios externalizados de TI* *DSS01.03 Supervisar la infraestructura de TI* *DSS01.04 Gestionar el entorno* *DSS01.05 Gestionar las instalaciones*	
Riesgos Asociados:	***Impacto***
No mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente	*Alto*
No contar con una gestión de los servicios externalizados de TI	*Bajo*
No supervisar las infraestructuras TI y los eventos relacionados	*Alto*
Falta de un registro de información cronológica de las operaciones.	*Alto*
No contar con medidas la protección contra factores ambientales.	*Alto*
No contar con una gestión de las instalaciones que incluya equipos de electricidad y	*Alto*

comunicaciones, en línea con las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo.	

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	***61.11%***
Probabilidad	***14.85%***
Riesgo Inherente	***9.08%***
Efectividad del Control	***85.15%***
Riesgo Residual	***1.35%***

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar Operaciones***" es **Insignificante** de **1.35%**, con una probabilidad de ocurrencia **Insignificante** de **14.85%,** que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **61.11%** y la efectividad de los controles es **Optimizado** de **85.15%**.

3.1.27 DSS02 Gestionar las peticiones y los incidentes del servicio

Proceso: DSS02 Gestionar las peticiones y los incidentes del servicio	
Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.	
Practicas de Gestión:	
DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio. *DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes.* *DSS02.03 Verificar, aprobar y resolver peticiones de servicio.* *DSS02.04 Investigar, diagnosticar y localizar incidentes.* *DSS02.05 Resolver y recuperarse de incidentes.* *DSS02.06 Cerrar peticiones de servicio e incidentes.* *DSS02.07 Seguir el estado y emitir informes.*	
Riesgos Asociados:	***Impacto***
No tener una respuesta oportuna y efectiva a las peticiones de usuario.	*Bajo*
No tener una respuesta oportuna y efectiva a la resolución de todo tipo de incidentes.	*Crítico*
No contar con una clasificación de incidentes y peticiones de servicio.	*Medio*

No asignar prioridad a peticiones de servicio e incidentes según la criticidad del negocio y los acuerdos de servicio.	*Alto*
No identificar, registrar, determinar y asignar posibles incidentes y sus causas, ni asignar recursos de resolución.	*Alto*
No verificar de manera satisfactoria la resolución de incidentes y/o satisfactorio cumplimiento de peticiones, y cierre.	*Alto*
No documentar, solicitar y probar las soluciones identificadas o temporales para restaurar el servicio de TI relacionado.	*Medio*
No proporcionar una mejora continua según los incidentes y tendencias registradas.	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	***60.42%***
Probabilidad	***22.50%***
Riesgo Inherente	***13.59%***
Efectividad del Control	***77.50%***
Riesgo Residual	***3.06%***

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar las peticiones y los incidentes del servicio***" es **Insignificante** de **3.06%**, con una probabilidad de ocurrencia **Baja** de **22.50%,** que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **60.42%** y la efectividad de los controles es **Optimizado** de **77.50%**.

3.1.28 DSS03 Gestionar Problemas

Proceso: DSS03 Gestionar Problemas
Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.
Practicas de Gestión:
DSS03.01 Identificar y clasificar problemas. *DSS03.02 Investigar y diagnosticar problemas.* *DSS03.03 Levantar errores conocidos.* *DSS03.04 Resolver y cerrar problemas.* *DSS03.05 Realizar una gestión de problemas proactiva.*

Riesgos Asociados:	***Impacto***
No contar con un procedimiento para informar de los problemas identificados, incluyendo clasificación, categorización y priorización de problemas.	*Alto*
Contar con un procedimiento para investigar y diagnosticar problemas	*Alto*
El proceso de valorar y analizar las causas raíz, no se lleve a cabo por expertos en las materias relevantes.	*Alto*
Falta un procedimiento para crear registros de errores conocidos y una solución temporal apropiada, e identificar soluciones potenciales.	*Alto*
No contar con procedimiento para identificar e iniciar soluciones sostenibles.	*Medio*
Falta un método que asegure que el personal afectado está al tanto de las acciones tomadas y de los planes desarrollados.	*Alto*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	***63.89%***
Probabilidad	***19.78%***
Riesgo Inherente	***12.64%***
Efectividad del Control	***80.22%***
Riesgo Residual	***2.50%***

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar Problemas***" es **Insignificante** de **2.50%**, con una probabilidad de ocurrencia **Baja** de **22.50%,** que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **63.89%** y la efectividad de los controles es **Optimizado** de **80.22%**.

3.1.29 DSS04 Gestionar la Continuidad

Proceso: DSS04 Gestionar la Continuidad	
Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.	
Practicas de Gestión:	
DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance. *DSS04.02 Mantener una estrategia de continuidad.* *DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.* *DSS04.04 Ejercitar, probar y revisar el plan de continuidad.* *DSS04.05 Revisar, mantener y mejorar el plan de continuidad.* *DSS04.06 Proporcionar formación en el plan de continuidad.* *DSS04.07 Gestionar acuerdos de respaldo.* *DSS04.08 Ejecutar revisiones postreanudación.*	
Riesgos Asociados:	***Impacto***
No definir la política y alcance de la continuidad del negocio afectará el cumplimiento de objetivos, manejo de incidentes y eventos o pérdidas considerables para la empresa.	*Alto*
Falta de alineación de la política y alcance de la continuidad del negocio con los objetivos de negocio y partes interesadas puede afectar la empresa, proveedores o colaboradores.	*Medio*
No evaluar opciones de gestión de la continuidad del negocio afecta la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción.	*Alto*
No desarrollar un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso, perjudica el manejo eficaz y eficiente ante un incidente que afecte las actividades críticas de la empresa.	*Alto*
No probar los planes de continuidad del negocio puede afectar su capacidad para responder de forma efectiva ante situaciones inesperadas, no lograr los resultados esperados, falta de control de las situaciones que se presenten y posibilidad de quedar obsoleto.	*Alto*
No realizar una revisión del plan de la capacidad de continuidad a intervalos regulares, afecta su continua idoneidad, adecuación y efectividad.	*Medio*
Falta de gestión de los cambios en el plan de acuerdo al proceso de control de cambios, provoca el manejo ineficiente de las actualizaciones del plan de continuidad.	*Alto*
No proporcionar sesiones formativas regulares a todas las partes implicadas, internas y externas, afecta la ejecución de procedimientos y roles en caso de disrupción.	*Medio*
Falta de gestión de acuerdos de respaldo.	*Medio*
No mantener la disponibilidad de la información crítica del negocio.	*Alto*
No evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios, afecta la mejora continua del plan y aprendizaje de las situaciones orridas.	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**59.09%**
Probabilidad	**10.83%**
Riesgo Inherente	**6.40%**
Efectividad del Control	**89.17%**
Riesgo Residual	**0.69%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar la Continuidad***" es **Insignificante** de **0.69%**, con una probabilidad de ocurrencia **Insignificante** de **10.83%,** que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **59.09%** y la efectividad de los controles es **Optimizado** de **89.17%**.

3.1.30 DSS05 Gestionar Servicios de Seguridad

Proceso: DSS05 Gestionar Servicios de Seguridad	
Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.	
Practicas de Gestión:	
DSS05.01 Proteger contra software malicioso (malware). *DSS05.02 Gestionar la seguridad de la red y las conexiones.* *DSS05.03 Gestionar la seguridad de los puestos de usuario final.* *DSS05.04 Gestionar la identidad del usuario y el acceso lógico.* *DSS05.05 Gestionar el acceso físico a los activos de TI.* *DSS05.06 Gestionar documentos sensibles y dispositivos de salida.* *DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.*	
Riesgos Asociados:	***Impacto***
No mantener medidas preventivas, de detección y correctivas en la empresa para proteger los sistemas de información y tecnología del software malicioso	*Muy Alto*
No utilizar medidas de seguridad y procedimientos de gestión para proteger la información de la empresa.	*Alto*
No mantener los puestos de usuario final asegurados a un nivel igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.	*Alto*

No asegurar el derecho de acceso a los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio.	*Alto*
No gestionar los propios derechos de acceso con los procesos de negocio.	*Alto*
No contar con procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio.	*Alto*
No contar con un procedimiento de registro y autorización de acceso a locales, edificios y áreas.	*Medio*
No contar con procedimientos de gestión para resguardar activos de TI sensibles que ponga en riesgo la información interna del negocio.	*Crítico*
No contar con prácticas de gestión de documentos sensibles, prácticas de contabilidad y activos fuera de las instalaciones de la empresa.	*Muy Alto*
No contar con herramientas de detección de instrucciones, supervisión de infraestructura para detectar accesos y métodos integrados con la supervisión y gestión de eventos.	*Muy Alto*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	***73.33%***
Probabilidad	***28.27%***
Riesgo Inherente	***20.73%***
Efectividad del Control	***71.73%***
Riesgo Residual	***5.86%***

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar Servicios de Seguridad***" es **Insignificante** de **5.86%**, con una probabilidad de ocurrencia **Baja** de **28.27%,** que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Muy Alto** de **73.33%** y la efectividad de los controles es **Optimizado** de **71.73%**.

3.1.31 DSS06 Gestionar Controles de Proceso de Negocio

Proceso: DSS06 Gestionar Controles de Proceso de Negocio
Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Identificar los requisitos de control de la

información y gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos.	
Practicas de Gestión:	
DSS06.01 Alinear las actividades de control embebidas en los procesos de negocio con los objetivos corporativos. *DSS06.02 Controlar el procesamiento de la información.* *DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.* *DSS06.04 Gestionar errores y excepciones.* *DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades de información.* *DSS06.06 Asegurar los activos de información.*	
Riesgos Asociados:	***Impacto***
No alinear las actividades de control dentro de los procesos de negocio con los objetivos corporativos.	*Alto*
No contar con un proceso de ejecución de las actividades de proceso de negocio y controles relacionados para asegurar que el procesamiento de la información es válido.	*Alto*
No contar con un procedimiento de gestión de los roles de negocio, responsabilidades, niveles de autoridad y segregación de tareas necesarias para apoyar los objetivos del proceso de negocio.	*Alto*
Falta de gestión para las excepciones y errores de los procesos de negocio y facilitar su corrección	*Alto*
No asegurar la trazabilidad de los eventos y responsabilidades de información.	*Medio*
No mantener un procedimiento para asegurar los activos de información.	*Alto*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	***63.89%***
Probabilidad	***32.67%***
Riesgo Inherente	***20.87%***
Efectividad del Control	***67.33%***
Riesgo Residual	***6.82%***

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Gestionar Controles de Proceso de Negocio***" es **Insignificante** de **5.86%**, con una probabilidad de ocurrencia **Baja** de **32.67%,** que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **63.89%** y la efectividad de los controles es **Administrado y Medible** de **67.33%**.

3.1.32 MEA01 Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad

Proceso: MEA01 Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	
Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.	
Practicas de Gestión:	
MEA01.01 Establecer un enfoque de la supervisión. *MEA01.02 Establecer los objetivos de cumplimiento y rendimiento.* *MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento.* *MEA01.04 Analizar e informar sobre el rendimiento.* *MEA01.05 Asegurar la implantación de medidas correctivas.*	
Riesgos Asociados:	***Impacto***
No involucrar a las partes interesadas en el establecimiento y mantenimiento de un enfoque de supervisión	*Alto*
No establecer objetivos de cumplimiento y rendimiento.	*Medio*
Falta un proceso para recopilar y procesar datos oportunos y precisos de acuerdo con los enfoques del negocio.	*Medio*
No mantener un proceso para revisar e informar de forma periódica sobre el desempeño respecto de los objetivos establecidos.	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	**54.17%**
Probabilidad	**43.46%**
Riesgo Inherente	**23.54%**
Efectividad del Control	**56.54%**
Riesgo Residual	**10.23%**

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad***" es **Insignificante** de **10.23%**, con una probabilidad de ocurrencia **Media** de **43.46%,** que en caso de materializarse algún evento o incidente el impacto para la Operadora sería **Alto** de **54.17%** y la efectividad de los controles es **Definido** de **56.54%**.

3.1.34 MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.

Proceso: MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	
Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general.	
Practicas de Gestión:	
MEA03.01 Identificar requisitos externos de cumplimiento. *MEA03.02 Optimizar la respuesta a requisitos externos.* *MEA03.03 Confirmar el cumplimiento de requisitos externos.* *MEA03.04 Obtener garantía de cumplimiento de requisitos externos.*	
Riesgos Asociados:	***Impacto***
No identificar y supervisar de manera continua, cambios en las legislaciones y regulaciones tanto locales como internacionales	*Alto*
No mantener un proceso para revisar y ajustar políticas, principios, estándares, procedimientos y metodologías para asegurar la adecuada gestión y comunicación de los requisitos legales, regulatorios y contractuales.	*Alto*
No contar con un proceso para confirmar el cumplimiento de las políticas, los principios, los estándares, los procedimientos y las metodologías con los requisitos externos.	*Alto*
No obtener garantía de cumplimiento de requisitos externos.	*Medio*

Una vez ejecutada la valoración de riesgos al proceso, el resultado fue el siguiente:

Resumen	
Impacto	***62.50%***
Probabilidad	***48.33%***
Riesgo Inherente	***30.21%***
Efectividad del Control	***51.67%***
Riesgo Residual	***14.60%***

Como se muestra en el cuadro de anterior, la exposición de riesgo que presenta el proceso "***Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos***" es **Insignificante** de **14.60%**, con una probabilidad de ocurrencia **Media** de **48.33%,** que en caso de materializarse algún evento o incidente el impacto para la

Operadora sería **Alto** de **62.50%** y la efectividad de los controles es **Definido** de **51.67%**.

4. Resultados

Ref. Doc.	Proceso	Ref. COBIT 5	Nivel de Riesgo	Porcentaje de Riesgo
3.1.1	Gestionar el Marco de Gestión de TI	APO01	Insignificante	1.63%
3.1.2	Gestionar la Estrategia	APO02	Bajo	24.11%
3.1.3	Gestionar la Arquitectura Empresarial	APO03	Insignificante	15.77%
3.1.4	Gestionar el Portafolio	APO05	Insignificante	3.88%
3.1.5	Gestionar el Presupuesto y los Costes	APO06	Insignificante	3.36%
3.1.6	Gestionar los Recursos Humanos	APO07	Insignificante	1.70%
3.1.7	Gestionar las relaciones	APO08	Insignificante	5.63%
3.1.8	Gestionar los acuerdos de servicio	APO09	Insignificante	16.05%
3.1.9	Gestionar los Proveedores	APO010	Insignificante	1.33%
3.1.10	Gestionar la Calidad	APO011	Insignificante	0.82%
3.1.11	Gestionar el Riesgo	APO012	Insignificante	8.71%
3.1.12	Gestionar la Seguridad	APO013	Insignificante	9.04%
3.1.13	Gestión de Programas y Proyectos	BAI01	Insignificante	13.60%
3.1.14	Gestionar la Definición de Requisitos	BAI02	Insignificante	7.03%
3.1.15	Gestionar la Identificación y Construcción de Soluciones	BAI03	Insignificante	6.15%
3.1.16	Gestionar la Disponibilidad y la Capacidad	BAI04	Insignificante	6.59%
3.1.17	Gestionar los Cambios	BAI06	Insignificante	11.85%
3.1.18	Gestionar la Aceptación del Cambio y la Transición	BAI07	Insignificante	8.98%
3.1.19	Gestionar los Activos	BAI09	Insignificante	1.85%
3.1.20	Gestionar la Configuración	BAI10	Insignificante	0.78%
3.1.21	Asegurar el establecimiento y mantenimiento del	EDM01	Bajo	19.44%

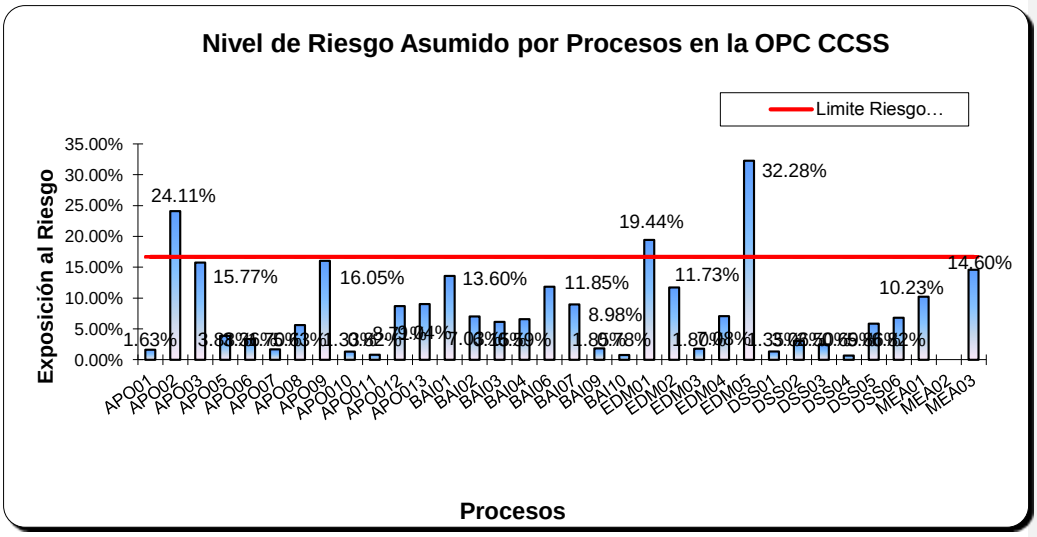
	marco de referencia de gobierno			
3.1.22	Asegurar la Entrega de Beneficios	EDM02	Insignificante	11.73%
3.1.23	Asegurar la Optimización del Riesgo	EDM03	Insignificante	1.80%
3.1.24	Asegurar la Optimización de Recursos	EDM04	Insignificante	7.08%
3.1.25	Asegurar la Transparencia hacia las Partes Interesadas	EDM05	Bajo	32.28%
3.1.26	Gestionar Operaciones	DSS01	Insignificante	1.35%
3.1.27	Gestionar las peticiones y los incidentes del servicio	DSS02	Insignificante	3.06%
3.1.28	Gestionar Problemas	DSS03	Insignificante	2.50%
3.1.29	Gestionar la Continuidad	DSS04	Insignificante	0.69%
3.1.30	Gestionar Servicios de Seguridad	DSS05	Insignificante	5.86%
3.1.31		DSS06	Insignificante	
3.1.32	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	MEA01	Insignificante	10.23%
3.1.33		MEA02	Insignificante	
3.1.34	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	MEA03	Insignificante	14.60%

Como se observa en la tabla anterior, 31 de los procesos evaluados se encuentran dentro del rango de riesgo **insignificante** (0% - 16.67%) y 3 procesos están dentro del rango de riesgo **bajo** (16.68% - 33.33%).

El Área de TI, tiene 3 procesos que sobrepasan el límite de riesgo aceptado por la Operadora de 16.67%.

- APO02 Generar la estrategia.
- ADM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.
- ADM05 Asegurar la transparencia hacia las partes interesadas.

En los siguientes gráficos se destaca el riesgo asumido por cada proceso evaluado, según el límite de 16.67%


Nivel de Riesgo Asumido por Procesos en la OPC CCSS
Limite Riesgo…
Exposición al Riesgo
35.00%
30.00%
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
24.11%
15.77%
16.05%
13.60%
11.85%
8.98%
19.44%
11.73%
32.28%
10.23%
14.60%
1.63%
APO01
APO02
APO03
APO05
APO06
APO07
APO08
APO09
APO010
APO011
APO012
APO013
BAI01
BAI02
BAI03
BAI04
BAI06
BAI07
BAI09
BAI10
EDM01
EDM02
EDM03
EDM04
EDM05
DSS01
DSS02
DSS03
DSS04
DSS05
DSS06
MEA01
MEA02
MEA03
Procesos

Anexo 3: Minuta de reunión 009 CTI

OPC CCSS
Operadora de Pensiones Complementarias

Minuta de reunión 009 CTI

1. Datos de la reunión

Fecha: 19/3/2018

Lugar: Operadora de Pensiones CCSS.

Objetivo/s: Comisión de TI.

Reunión convocada por: Guillermo Trejos, encargado de seguridad de la información.

2. Participantes (Nombre y Cargo)

Héctor Maggi, gerente general.
Graciela Mora, directora financiera.
Alejandro Castillo, jefe de riesgos.
Luis Vargas, jefe de TI.
Guillermo Trejos, encargado de seguridad de la información.

Invitados:

Marvin Navarro, auxiliar de seguridad de la información.
Christopher Benítez, especialista de infraestructura.

3. Temas tratados

1. **AR-59-2018 INFORME FINAL DEL SEVRI TI**

Este tema es presentado por el señor Trejos, de acuerdo con lo indicado en el artículo 18 de la Ley de Control Interno, se hace entrega del informe final de valoración de riesgos operativo de TI con corte al 2018.

Valorización del Riesgos de Tecnologías de Información basada en COBIT 5

Objetivo

OPC CCSS
Operadora de Pensiones Complementarias

Determinar el riesgo de Tecnologías de la Información de la OPC CCSS, para definir el perfil tecnológico solicitado por SUPEN.

Procesos año 1

Ref. COBIT 5	Proceso	Nivel de Riesgo	Porcentaje de Riesgo
APO01	Gestionar el Marco de Gestión de TI	Insignificante	1.63%
APO02	Gestionar la Estrategia	Bajo	24.11%
APO09	Gestionar los acuerdos de servicio	Insignificante	16.05%
APO010	Gestionar los Proveedores	Insignificante	1.33%
BAI01	Gestión de Programas y Proyectos	Insignificante	13.60%
EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	Bajo	19.44%
EDM02	Asegurar la Entrega de Beneficios	Insignificante	11.73%
EDM03	Asegurar la Optimización del Riesgo	Insignificante	1.80%
EDM04	Asegurar la Optimización de Recursos	Insignificante	7.08%
EDM05	Asegurar la Transparencia hacia las Partes Interesadas	Bajo	32.28%
DSS02	Gestionar las peticiones y los incidentes del servicio	Insignificante	3.06%

Procesos año 2

Ref. COBIT 5	Proceso	Nivel de Riesgo	Porcentaje de Riesgo
APO012	Gestionar el Riesgo	Insignificante	8.71%

OPCCCSS
Operadora de Pensiones Complementarias

APO013	Gestionar la Seguridad	Insignificante	9.04%
BAI06	Gestionar los Cambios	Insignificante	11.85%
DSS04	Gestionar la Continuidad	Insignificante	0.69%
DSS05	Gestionar Servicios de Seguridad	Insignificante	5.86%
DSS06	Gestionar Controles de Proceso de Negocio	Insignificante	6.82%
MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno	Insignificante	5.22%

Procesos año 3

Ref. COBIT 5	Proceso	Nivel de Riesgo	Porcentaje de Riesgo
APO06	Gestionar el Presupuesto y los Costes	Insignificante	3.36%
BAI03	Gestionar la Identificación y Construcción de Soluciones	Insignificante	6.15%
BAI04	Gestionar la Disponibilidad y la Capacidad	Insignificante	6.59%
BAI09	Gestionar los Activos	Insignificante	1.85%
BAI10	Gestionar la Configuración	Insignificante	0.78%
DSS01	Gestionar Operaciones	Insignificante	1.35%
DSS03	Gestionar Problemas	Insignificante	2.50%

Proceso año 4

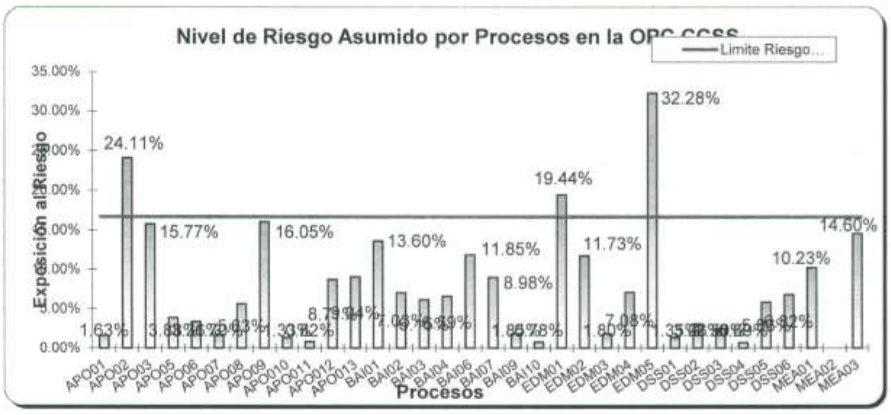
OPCCCSS
Operadora de Pensiones Complementarias

Ref. COBIT 5	Proceso	Nivel de Riesgo	Porcentaje de Riesgo
APO03	Gestionar la Arquitectura Empresarial	Insignificante	15.77%
APO05	Gestionar el Portafolio	Insignificante	3.88%
APO07	Gestionar los Recursos Humanos	Insignificante	1.70%
APO08	Gestionar las relaciones	Insignificante	5.63%
BAI02	Gestionar la Definición de Requisitos	Insignificante	7.03%
BAI07	Gestionar la Aceptación del Cambio y la Transición	Insignificante	8.98%

Proceso año 5

Ref. COBIT 5	Proceso	Nivel de Riesgo	Porcentaje de Riesgo
APO011	Gestionar la Calidad	Insignificante	0.82%
MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	Insignificante	10.23%
MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	Insignificante	14.60%

Límite de riesgo aceptado



- *APO02 Generar la estrategia. (año 1)*
- *ADM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno. (año 2)*
- *ADM05 Asegurar la transparencia hacia las partes interesadas. (año 3)*

Los miembros de la Comisión de T. I. emiten sus observaciones y comentarios sobre el oficio AR-59-2018 Informe final del SEVRI TI presentado por el señor Guillermo Trejos, encargado de seguridad de la información del Área de T. I. y se toma el siguiente acuerdo:

Acuerdo 1°
Visto y analizado el Oficio AR-59-2018 del 19 de marzo de 2018 remitido por el Área de Riesgos, el cual contiene el Informe final del SEVRI T. I. corte 2018, esta Comisión aprueba dicho informe y solicita a la Administración tomar las acciones preventivas pertinentes para atender los niveles de riesgo de los procesos que se posicionaron en estado de alerta; también se solicita remitir el informe a la Junta Directiva para su aprobación final.
Acuerdo firme.

El señor Castillo propone que la periodicidad del SEVRI de TI sea anualmente si la comisión está de acuerdo.

El señor Maggi consulta en cual documento está declarado todo lo relacionado con el SEVRI de TI.

El señor Castillo responde que está declarado en el 8M01.

El señor Maggi indica que, en este caso, se tendría que solicitar al Comité de Riesgos el análisis del cambio de periodicidad ya que este documento es aprobado primeramente por este Comité y posteriormente por la Junta Directiva.

El resto de los miembros concuerdan y se toma el siguiente acuerdo:

Acuerdo 2°
Esta comisión solicita al Comité de Riesgos valorar la posibilidad de cambiar la periodicidad declarada en el documento 8M01 Marco orientador, para la elaboración del SERVRI de TI, de semestral a anual; debido a la extensa elaboración que requiere este proceso y que, el cambio marginal que pueden arrojar los resultados es mínimo, sin añadir valor agregado a la gestión.
Acuerdo firme.

2. METODOLOGÍA CASADA DE METAS (PERFIL TECNOLÓGICO)

El señor Vargas expone el análisis realizado a la Operadora mediante la metodología Cascada de Metas.

Metodología
CASCADA DE METAS
MARZO 2018

La cascada de metas de COBIT 5 es el mecanismo para traducir las necesidades de las partes interesadas en metas corporativas y metas relacionadas con las TI, las cuales a su vez pueden relacionarse con procesos específicos de COBIT 5.
Esta metodología define objetivos genéricos de TI y del Negocio y los asocia con los procesos de COBIT 5, específicamente con aquellos que tienen una importante relación (Procesos Primarios) y con los que tienen una relación fuerte pero menos importante (Procesos Secundarios).

4. Compromisos asumidos

Descripción	Responsable	Fecha de conclusión

5. Temas pendientes

No hay temas pendientes.

OPC CCSS
Operadora de Pensiones Complementarias

6. Firma de los Asistentes

Nombre	Firma
Héctor Maggi, gerente general.	
Graciela Mora, directora financiera.	
~~Sugey Gómez, directora comercial~~	1
~~Renato Alvarado, presidente.~~	2
Alejandro Castillo, jefe de riesgos.	
Luis Vargas, jefe de TI.	
Guillermo Trejos, encargado de seguridad de la información.	