PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO DE SISTEMAS Y COMPUTACIÓN

"Desarrollo de guía metodológica empleando COBIT 5, para evaluar la seguridad del Cloud Computing que ofrecen los proveedores de este servicio, en la ciudad de Quito"

AUTOR:
JOHNNY ARIAS

DIRECTOR: Mtr. ALBERTO PAZMIÑO

QUITO, 2017

Tabla de contenido

1. Capítulo: Cloud Computing

Este capítulo trata temas que facilitan la comprensión y proveen una idea al entorno de Cloud Computing, siendo conceptos que deben tenerse claros en el momento de llevar a cabo un análisis de seguridad de este modelo de negocio. Además de explicar y detallar las diferentes formas de implementación, aplicación y normalización del modelo para de esta forma realizar un correcto proceso de análisis al adentrarse en el mundo de la computación en la nube.

1.1 Introducción al Cloud Computing

Conocido en español como Computación en la nube, o internacionalmente referido como “Cloud Computing” hace relación a un modelo de servicios y negocios.

El definir la nube, el Internet, es complejo debido a que no se puede saber con certeza todo lo que este medio de comunicación abarca, por el mismo hecho además de la manera histórica en la que se dio el surgimiento del modelo “Cloud Computing” lograr una definición del mismo es igual de dificultoso.

Pero actualmente este modelo es una tendencia fuerte en el mundo de negocios, por ello es fundamental llegar a un acuerdo en que consiste “Cloud Computing”, para ello se toma de referencia la definición dada por el instituto de estándares y tecnología de los Estados Unidos.

Podemos entender al “Cloud Computing” como un modelo para permitir ubicuidad, conveniencia, acceso a red bajo demanda a un conjunto de recursos computacionales configurables y compartidos que puede ser rápidamente aprovisionado y puesto en lanzamiento con un mínimo esfuerzo administrativo o interacción con el proveedor de servicios (NIST, 2011)

Con esto se puede entender que los modelos Cloud Computing recaen en compartir a una red recursos de cómputo y servicios, es un modelo de negocios basado en Internet. Diferenciándose de los modelos clásicos donde se cuentan con dispositivos personales y servidores locales en los que se tienen las aplicaciones y servicios que se procesarán localmente.

1.2 Cloud Computing: su Evolución

1.2.1 Introducción

Al referirnos a la evolución de “Cloud Computing” se deben tomar en cuenta ciertos aspectos iniciales, para entender de mejor forma el relativamente rápido crecimiento de este modelo de negocio.

Para iniciar se toma de base un análisis realizado por Srinivasan[1] como aporte a la comparativa de la evolución de tecnologías mundialmente adoptadas.

Tecnología	Tiempo para llegar a 50 millones de usuarios
Teléfono	75 años
Radio	38 años
Televisión	13 años
Computadoras Personales	16 años
Internet	4 años
Buscador Google	3 meses
YouTube	11 meses
Facebook	2 años 10 meses
Twitter	3 años

Tabla 1: Resumen del crecimiento tecnología, tomado de S. Srinivasan, Cloud Computing Basics, 2014

Se puede ver que las tecnologías como teléfono, radio, televisión y computadoras personales tomaron bastante tiempo en ser mundialmente empleadas, gran parte de esto se debía al tiempo en que dichos equipos y la tecnología en general avanzaba permitiendo la construcción de este tipo de dispositivos.

Pero al llegar a hacer un análisis de Youtube, Facebook, Twitter y Google (el motor de búsqueda) se ve un contraste enorme en el tiempo que estas tecnologías llegaron a tener al menos 50 millones de usuarios.

Según Srinivasan, esto se debe a que para el momento de implementación de estas tecnologías web toda la infraestructura tecnología ya se había construido lo que facilitó inmensamente su consumo.

[1] (Srinivasan, 2014)

“Es importante darse cuenta que el crecimiento de ciertas tecnologías depende de la disponibilidad de una apropiada infraestructura. Todas las tecnologías modernas se benefician de la disponibilidad de varias tecnologías habilitadoras.” (Srinivasan, 2014)

El mejoramiento que han sufrido las tecnologías habilitadoras, como Internet, ha beneficiado de gran forma a los modelos de “Cloud Computing”. Esto se da debido a que, en la actualidad, el Internet es un aspecto globalizado que ha dado un incremento significativo en el entorno de las comunicaciones.

Como pensamiento inicial se puede definir que la computación en la nube, empezó de mano de Amazon, que alrededor de 10 años atrás empezó a lanzar el modelo de Infraestructura como servicio.

Otras grandes empresas se unieron al mercado de Cloud Computing, media década atrás cuando incursionaron en sus propias formas de este modelo como Windows con Azure y Microsoft Office 365, o Google con Google Apps. El que grandes compañías se hayan unido a este tipo de modelo de negocio ha generado que varios modelos exitosos a nivel mundial puedan haberse iniciado, algunos casos son Netflix, Dropbox y Flickr que emplean los servicios de Proveedores de Cloud Computing, para generar su propio negocio a partir de ellos.

Un aspecto fundamental que se debe tener en cuenta al momento de analizar la evolución de la computación en la nube es:

Al analizar la evolución del “Cloud Computing” se abarcan distintos contenidos que se encuentran involucrados en su proceso de crecimiento y maduración. Se hará un análisis breve puesto a que es un tema introductorio que se enfoca en dar una idea inicial del estado del arte de este modelo de negocio, además de ser un punto inicial para relacionar conceptos base de este trabajo.

1.2.2 Evolución a lo largo de los años

"La Idea básica de Cloud Computing es tomar ventaja del concepto de economía en escala para que los servicios que pueda proveer el departamento de TI se den con una infraestructura descentralizada." (Srinivasan, 2014)

El principal argumento que procuró el cambio en la forma de administrar la infraestructura propia, dentro de respectivos departamentos de TI, se da por el gran avance de la intercomunicación provista con el auge del Internet y el constante incremento de las velocidades de conexión, esto sumado a la flexibilidad de las demandas de cómputo que tienen las empresas, causado por la globalización. Provee el estímulo necesario para incursionar en investigar e implementar nuevos modelos de negocio que se sean óptimos para estas nuevas condiciones del mercado.

Para relacionar este aspecto se toma en cuenta el análisis realizado por Maximilliano Destefani Neto y de IBM, en su sección: "Thoughts on Cloud: A Brief History of Cloud"[2]. En este documento se detallan los principales hitos del "Cloud Computing", algo que se debe tomar en cuenta es que: "La frase Cloud Computing (Computación en la nube) es empleada para abarcar todo tipo de servicios computacionales en línea"[3].

Durante la década de los 50's no existía indicio del término computación en la nube, simplemente no existía la nube como tal, el aspecto tecnológico que nace es el de centralización de recursos y compartición de tiempos.

A finales de los 60's, precisamente en 1969 es creada ARPANET, el primer prototipo que conectó 4 computadoras ubicadas en distintos puntos geográficos, el inicio del Internet.

En la década de los 70's se crea el modelo cliente servidor, modelo que define clientes que tienen acceso a datos y aplicaciones desde un nodo central, servidor, a través de una red.

[2] (IBM, Staff Writer, 2015)
[3] (Srinivasan, 2014)

Desde ese punto se avanza hasta mediados de los 90's donde la tecnología y el concepto de Internet llega a globalizarse, permitiendo la aparición de la "nube" en diagramas de redes.

Ilustración 1: Aparición de la nube, en diagramas de red, Tomado de Thoughts On Cloud, Cloud through the ages: 1950s to present day, IBM

De esta manera al finalizar los 90's grandes empresas de tecnología se lanzan al entorno de la nube, Salesforce.com lanza el primer mercado digital de aplicaciones; Google lanza su buscador; Netflix inicia sus servicios como proveedor de películas DVDs.

En el nuevo milenio existe un gran progreso en el desarrollo de las páginas web, puesto que se da el inicio a la Web 2.0, contenido generado por usuarios y el uso de interfaces dinámicas.

Además, en 2004 sale a la luz Facebook, la red social más conocida en el mundo.

En 2006 Amazon, lanza Amazon Web Services, un modelo que permite el almacenamiento y renta de servicios de cómputo. El primer concepto de SaaS (Software como un Servicio). Además, en este mismo año el término "Cloud" es mundialmente empleado.

Para 2007 Netflix pasa de ser un vendedor de DVDs en línea, a brindar servicios de streaming[4].

Durante todo este periodo se tenía conocida a la "nube" como algo público puesto que relativamente todos tienen acceso a ello, es por esto que, en 2008 por temas de brindar mayor seguridad y confiabilidad a clientes, las empresas generan el modelo "nube privada".

[4] Distribución digital de multimedia a través de una red de computadoras. (Wikipedia, 2016)

El año en que nacen las aplicaciones basadas en servidores (Browser-Based Cloud[5]) es 2009 lo que revoluciona el mercado de las aplicaciones de productividad el principal aportante de esto es Google, con Google Apps. Liberando al usuario de emplear la capacidad de procesamiento de su máquina personal para realizar las tareas y empleando capacidad de procesamiento brindada por Google.

Durante el periodo de 2009 a 2010 salen al mercado los conceptos de Open-Source Cloud, proyectos como EUCALYPTUS[6] (en 2014 HP adquirió Eucalyptus Systems, Inc) y OpenStack[7] hacen posible realizar "Cloud Computing" privado empleando herramientas Open- Source[8].

Para 2011 se crea el concepto de Hybrid Cloud, o Nube híbrida que relaciona conceptos principales de la nube privada como la pública. En este mismo año nace la iniciativa de Microsoft "To the Cloud" una serie de comerciales para incentivar el uso de servicios Cloud Computing, Apple lanza iCloud una plataforma de almacenamiento en línea.

En 2012 Google lanza su propia forma de almacenamiento en línea conocida como Google Drive.

En 2013 IBM se une al mercado de proveedores de Cloud Computing, al adquirir SoftLayer, una solución de nube privada con gran velocidad.

Como se puede observar el proceso evolutivo de la computación en la nube ha tenido lapsos acelerados y lapsos de duda, en los que ha tenido ciertos estancos en su progreso. El gran crecimiento se debe en gran parte a la fuerza con la que Internet logró globalizarse, pero el estancamiento principal se sufrió el modelo de "Cloud Computing" se dio antes de nacer el concepto de "nube privada" debido a la falta de seguridad que los clientes percibían.

[5] (IBM, Staff Writer, 2015)
[6] (Hewlett Packard Enterprise Development LP, 2016)
[7] (The openStack Project, 2016)
[8] Se refiere a que el código fuente puede ser inspeccionado por cualquier persona. (opensource.com, s.f.)

Otro factor que en la actualidad hace difícil el determinar el nivel de crecimiento, evolución y estado actual del “Cloud Computing” es su cercanía con Internet, esta relación intrínseca dificulta mucho el poder determinar que es un servicio “Cloud Computing” y que es Internet como tal.

A lo largo de la investigación se podrán dar cuenta que esta dificultad de poder definir como algo exacto a los servicios de computación en la nube ha afectado toda la evolución y comprensión de este modelo de negocio.

1.3 Características

El modelo de negocio Cloud Computing, en base a lo establecido por el NIST (National Institute of Standards and Tecnology) en 2011 en el documento: “The NIST Definition of Cloud Computing”[9], cuenta con 5 características esenciales que lo diferencian y definen, son las siguientes:

1.3.1 Servicio en Demanda (On demand Self Services):

Lo fundamental de este aspecto es que el usuario, cliente o consumidor esté en la capacidad de emplear los recursos del proveedor del servicio, sin la necesidad de interacción humana, toda la interacción o la gran mayoría de la misma se da empleando una plataforma web de autoservicio.

Dentro de esta categoría recaen los servicios de correo electrónico, proveedores de servicios de red, aplicaciones web como servicios de tv on-demand como Directvplay o Netflix.

1.3.2 Amplio acceso a la red (Broad network Access):

Lo principal es que los recursos del modelo Cloud Computing estén disponibles y se pueda acceder a ellos a través de toda la red, permitiendo el acceso desde un cliente heterogéneo (teléfonos móviles, computadoras, tablets).

[9] (NIST, 2011)

1.3.3 Combinar Recursos (Resource pooling):

Este aspecto se refiere a que los recursos y servicios del proveedor se combinan empleando un modelo multi propietario (multi-tenant[10]) empleando recursos dinámicos ya sean físico y virtuales, que se ajusten dependiendo la demanda de los clientes, además de esto el aspecto de la infraestructura tecnológica es invisible para el usuario, ya que su localización y componentes están ocultos para el mismo y él no tiene control alguno sobre ellos dando un alto nivel de abstracción.

1.3.4 Elasticidad rápida (Rapid elasticity):

La alta y rápida elasticidad se refiere a la forma de manejar los recursos, los cuales son habilitados por el proveedor del servicio además deben ajustarse adecuadamente al consumo del cliente, ya sea habilitándolos o liberándolos a medida que el usuario los requiera y el momento que sean necesarios, en algunos casos de forma automática basándose en parámetros o funciones. Esto asegura que la aplicación trabaje en capacidades óptimas brindando solo el servicio que es en realidad necesario para el cliente y optimizando el control de los recursos tecnológicos y de cómputo.

1.3.5 Servicio Medido (Measured service):

Un sistema que este enfocado en el modelo “Cloud Computing” debe contar con sistemas de control y optimización de recursos, el uso de los recursos debe ser monitoreado, medido y reportado de manera transparente en base a su nivel de utilización de esta forma se asegura el concepto de pagar por lo utilizado.

En base a la información provista por el NIST estas son las características esenciales, pero la alianza por la seguridad de la nube (Cloud Security Alliance) propone una característica más:

1.3.6 Tenencia múltiple (Multi tenacity[11]):

Este aspecto está totalmente enfocado a emplear medidas de seguridad a lo largo del modelo de negocio, es decir utilizar: niveles de servicio, políticas de segmentación,

[10] Multi-tenant: hace referencia a que solamente una instancia de la aplicación se ejecuta en el servidor, pero cada cliente tiene una instancia propia de dicha aplicación. (Krebs, Momm, & Kounev, 2012)
[11] (ISACA)

aislamiento, gobernabilidad y modelos de cobranza y facturación acorde a los diferentes grupos de facturación.

1.4 Modelos de Servicios

Los modelos de servicios hacen referencia a la forma en la que estos se hacen disponibles al cliente, estos modelos son interdependientes[12] y a su vez tienen una alta sinergia entre ellos existen 3 modelos fundamentales: Infraestructura como un servicio (IaaS), Plataforma como un servicio (PaaS) y Software como un servicio (SaaS).

1.4.1 Infraestructura como un Servicio (IaaS)

Lo fundamental de este modelo de servicio es que el proveedor brinda acceso a componentes de infraestructura al cliente. Estos componentes pueden incluir almacenamiento, firewalls, redes, máquinas virtuales, procesamiento entre otros recursos de cómputo.

"Infraestructura como un servicio (IaaS) es una forma de Cloud Computing que provee recursos de computación virtualizados a través del Internet" (Rouse, Infrastructure as a Service (IaaS), 2015)

Con toda esta infraestructura provista por el proveedor el cliente tiene la capacidad de emplear los recursos necesarios para que funcione el software (aplicaciones o sistemas operativos) que requiera.

Simplificando el concepto, IaaS es un modelo en el que el proveedor alberga el hardware (servidores, redes, almacenamiento), software y otros componentes que conformen la infraestructura tecnológica que permita al usuario realizar todo lo que necesita sin tener que administrar, control, monitorear y configurar él mismo esta infraestructura. Todo el manejo de la infraestructura queda delegado al proveedor del servicio.

El principal proveedor de IaaS es Amazon con su rama Amazon Web Services[13]

[12] (Gorelik, 2013)
[13] (Amazon Web Services, Inc, 2016)

1.4.2 Plataforma como un servicio (PaaS)

Este modelo brinda al cliente una plataforma que ha sido previamente construida. La cual es distribuida al cliente mediante el Internet. Lo fundamental es que todos los recursos que necesite la aplicación que se entregó como servicio son manejados, controlados y ajustados al consumo requerido por el proveedor, en la infraestructura propia del proveedor. Haciendo que el cliente no deba instalar hardware o software dedicados a que la aplicación funcione.

Este modelo se relaciona directamente con la infraestructura como un servicio, para ser exacto pasa a ser una extensión de la infraestructura como servicio adicionando la entrega de un entorno para que el cliente use la plataforma y sus aplicaciones con la capacidad de cómputo brindada por el proveedor.

El PaaS está principalmente enfocado a proveer API's para funciones de desarrollo un ejemplo es Google AppEngine y Google Cloud Platform[14]

1.4.3 Software como un servicio (SaaS)

Este modelo utiliza una premisa simple, remover la necesidad de instalar y correr las aplicaciones en los equipos propios. Estas aplicaciones están almacenadas y corren dentro de la infraestructura del proveedor que cuenta una interface a la nube.

El cliente para acceder a estos servicios utiliza un navegador de Internet o algún software que actúa como interface cliente.

La facilidad de esto es que el cliente no tiene que emplear recursos de cómputo o almacenamiento contando con todas las características del programa.

Ejemplo de SaaS[15] son servicios de e-mail, CRM's y plataformas sociales.

1.5 Modelos de Implementación Cloud Computing

En lo que respecta a la implementación de estos modelos de negocio, hay tres clasificaciones fundamentales.

[14] (Google, 2016)
[15] (Gorelik, 2013)

1.5.1 Nube Pública

"La nube pública es el modelo en que la infraestructura tecnológica es propia de una organización y esta se encarga de vender los servicios de Cloud Computing al público en general" (Linthicum, 2009)

Para extender un poco el concepto y hacerlo más familiar el servicio de Cloud Computing empleando una nube pública es el modelo básico y se enfoca en la infraestructura estándar de los modelos Cloud Computing, es decir emplear recursos computacionales a través de Internet que se encuentran hospedados externamente a la organización, lo principal es el concepto **externo** ya que hace referencia a que los recursos no pertenecen a la organización que se beneficia del servicio de la nube.

Los principales beneficios de una nube pública son los siguientes:

Alta escalabilidad: esto hace referencia a que el modelo es muy adaptable a las distintas capacidades de uso que se dé, ya sea para procesamiento o almacenamiento.

Instalación fácil y relativamente de bajo costo: El costo es reducido y fácil debido a que no existe una cantidad elevada de instalación ya que no se debe implementar un centro de cómputo con todos los recursos tecnológicos, sino que se realiza un pago moderado a medida del nivel de consumo de los recursos prestados por el proveedor. La instalación generalmente es sencilla ya que solo depende de alguna aplicación que funciona de interface a los recursos tecnológicos, como es un navegador web.

Uso adecuado de recursos: el plus principal del modelo es el solo emplear la cantidad necesaria del recurso tecnológico, en caso de que este recurso fuese propio si no se ocupara el 100% de la infraestructura se estaría desperdiciando el equipamiento y a su vez perdiendo gran parte de la inversión tecnológica.

Este no es el caso del modelo de nube pública debido a que varios clientes acceden al recurso y este aspecto minimiza en gran parte el desperdicio y no uso de la tecnología disponible.

1.5.2 Nube Privada (Private Cloud)

Este concepto de nube privada nace debido a que gran parte de las organizaciones no se aferran y se mantienen alejadas de emplear la nube pública, principalmente por la "falta de seguridad" que este modelo supone, en un principio, la supuesta "carencia de seguridad" de la nube publica se fundamenta en que el proveedor del servicio al administrar los recursos cuenta con la posibilidad de acceder a la información del cliente. Debido a este recelo de las entidades a asumir el modelo de la nube pública se genera una adaptación y modificaciones al concepto estándar de Cloud Computing, para, en base a un cambio fundamental, crear la nube privada.

> "La nube privada tiene una infraestructura propia o arrendada por una organización y su operación está totalmente enfocada en ser empleada por esa organización" (Linthicum, 2009)

Como se entiende en la definición, la principal diferencia es que la infraestructura tecnológica que brinda el proveedor, que en algunos casos pasa a ser propia del cliente, está totalmente enfocada a servir solo a un cliente, que es el "dueño" de estos recursos.

A pesar de este cambio los beneficios de la nube privada siguen siendo los mismos, de escalabilidad, instalación fácil y relativamente de bajo costo. El principal cambio que se da es el contar con un auto-servicio, es decir la infraestructura propia, que de cierta forma brinda mayor seguridad debido al estar enfocada totalmente al uso dedicado a una sola organización, pero a su vez puede conllevar desperdicio y mal uso de recursos si no se administran de forma adecuada.

Este tipo de modelos se direcciona y maneja de mejor manera en organizaciones con necesidades de cómputo con baja probabilidad de ser predecibles y con modelos de negocio dinámicos, ya que el contar con mayor control del ambiente y la infraestructura tecnológica brinda más libertar para modificar y direccionar la ocupación de los recursos.

1.5.3 Nube Híbrida

Este modelo utiliza la unión de la nube privada con la nube pública, generando un punto de intersección entre ambos modelos de implementación, permitiendo contar con la facilidad de intercambiar la carga de trabajo entre las dos infraestructuras tecnológicas a medida que sea necesario el optimizar el uso de los recursos o el minimizar costos.

"La nube Híbrida es una infraestructura, compuesta de dos o más nubes (interna, de comunidad, o pública) que las mantiene como entidades únicas pero que están ligadas mediante estándares y tecnológicas propietarias lo que permite contar con datos y aplicaciones portables" (Linthicum, 2009)

La utilidad principal de este tipo de implementación del modelo es para empresas con alto valor dinámico en su manejo de datos y procesamiento de información, además de contar con alta carga de trabajo. Un ejemplo son entidades que cuenten con sistemas transaccionales, entidades financieras que en finales de mes o feriados se ven sobrecargados con transacciones, en este tipo de casos el uso de una nube hibrida es la solución ya que se puede realizar una redistribución de procesamiento para optimizar los recursos y mantener el sistema funcional.

A pesar de generar gran escalabilidad este modelo es más complicado de implementar y conlleva sus retos técnicos debido a que para un correcto uso de la interconexión de las nubes se debe contar con estándares en todo tipo de datos y aplicaciones que estarán en el intercambio de ambientes, además de contar con compatibilidad de las redes como tal y una conexión entre ellas estable.

1.5.4 Otros tipos

Existen varios tipos de adaptaciones de nubes que manejan conceptos similares a los de las nubes hibridas o privadas, como los modelos On-Premise.

Pero otro modelo que es más empleado y se distingue de mejor manera es el modelo de Nube comunitaria o nube en comunidad.

Nube en comunidad (nube comunitaria):

"La nube comunitaria se caracteriza por que la infraestructura esta compartida entre varias organizaciones que se apoyan entre sí, generando una comunidad, con fines de uso y necesidades en común"[16]

[16] (Linthicum, 2009)

El principal uso de estas nubes es el de generar un modelo de Cloud Computing que facilite la comunicación y la compartición de recursos, haciendo que los objetivos generados en las alianzas estratégicas se completen.

Algunos ejemplos de este tipo de nubes comunitarias son Boinc[17], que es una red comunitaria que emplea conceptos de Cloud Computing, entre recursos tecnológicos de universidades (como Berkeley o la Universidad de California), de centros de investigación y de voluntarios. Empleando estos recursos tecnológicos se forma una comunicación mediante el Internet generando una nube comunitaria, que está enfocada a prestar estos recursos para realizar tareas de procesamiento requeridas para proyectos de investigación. Otro ejemplo muy similar es Folding@home[18] que es una red que emplea el concepto de nube comunitaria para, empleando los recursos tecnológicos, enfocar la capacidad de procesamiento dada por la red a encontrar curas para distintas enfermedades como cáncer, Alzheimer y Parkinson.

2. Capítulo: COBIT®[19] 5

En este capítulo se describe y se realiza una introducción y explicación de en qué consiste el marco de referencia COBIT 5, desarrollado por ISACA[20], además de la motivación para emplearlo como base de análisis para este trabajo de disertación.

2.1 Introducción a COBIT5

Un aspecto fundamental que se resalta durante todo el marco de referencia COBIT5 es:" La información es un recurso clave para todas las organizaciones"[21]

COBIT5 hace resaltar la importancia de la información de la organización teniendo en cuenta su ciclo de vida desde su creación hasta el momento en que ésta es destruida. Y resalta a la tecnología, los avances de tecnologías, como un ente clave en el manejo de la información, haciéndose una parte integral que se relaciona conjuntamente con la vida personal, social y empresarial.

[17] (University of California, Barkeley, 2016)
[18] (Stanfod university, 2013)
[19] Control Objectives for Information and related Technology es decir Objetivos de Control para Información y Tecnologías relacionadas (COBIT)
[20] Information Systems Audit and Control Association, es decir Asociación de Auditoría y Control de Sistemas de Información (ISACA)
[21] (COBIT 5 Task Force (2009-2011), 2012)

Recalca lo importante del resguardo de la información y el control de la misma en todo el ciclo de vida recaen en los siguientes puntos, según ISACA son aspectos que conciernen principalmente a las organizaciones y ejecutivos:

- Mantener alta calidad de información que apoye las decisiones de negocio
- Generar valor al negocio desde las inversiones habilitadoras en TI, por ejemplo: lograr objetivos estratégicos o innovar empleando TI
- Lograr excelencia operacional a través de una aplicación tecnológica, confiable y eficiente.
- Mantener riesgos asociados a TI en niveles aceptables
- Optimizar el costo de servicios y tecnología TI
- Cumplir con leyes (siempre aumentando), regulaciones, políticas y acuerdos contractuales.

En resumen, COBIT 5: "provee de un marco de referencia comprensivo que asiste a empresas a lograr todos sus objetivos de gobierno y administración empresarial de TI."[22]

Un tema que siempre se resalta a lo largo de este marco de referencia es el de gobernabilidad ("Governance") debido a que el entorno empresarial ha reconocido la importancia y necesidad de adoptar TI como una parte fundamental del negocio. Más que nada hacer un acercamiento hacia gobierno y administración para una colaboración con TI.

2.2 Principios de COBIT5

Este marco de referencia se basa en 5 principios claves enfocados tanto en la administración de TI de la empresa, así como en la gobernabilidad.

2.2.1 Principio 1: Satisfacer las necesidades de las partes interesadas

"Empresas existen para crear valor para los stakeholders (partes interesadas) mediante el mantenimiento del balance entre la realización de beneficios y la optimización de riesgos además del uso de recursos" (COBIT 5 Task Force (2009-2011), 2012)

COBIT 5 logra apoyar en este aspecto, enfocando varios habilitadores y procesos que mediante el apoyo de las tecnologías TI permiten generar valor al negocio.

[22] (COBIT 5 Task Force (2009-2011), 2012)

Un punto fundamental que se aclara es que no se puede generalizar a las empresas ni sus objetivos, cada organización tiene objetivos y metas diferentes es por ello que este marco de referencia emplea el concepto cascada de metas. Un mecanismo que permite estandarizar los objetivos empresariales generando un enfoque a metas específicas y metas relacionadas con las TI.

2.2.1.1 Cascada de metas

Como se resaltó anteriormente cada organización tiene un enfoque distinto, objetivos diferentes. Por ello cada organización opera de forma específica en base a como está afectada por factores ya sean internos (organización, cultura, etc.) y externos (mercado, geopolítica, etc.) por ello se requiere un sistema de gestión y gobierno personalizado.

El mecanismo de cascada de metas se emplea de forma que las necesidades, objetivos y metas de las partes interesadas, al ser “personales” para cada organización se estandaricen en específicos, metas de la organización, metas habilitadoras y metas relacionadas a TI.

La transición permite tener metas específicas en todos los niveles y áreas de la organización apoyando cada una de las metas y requerimientos de las partes interesadas, alineándose efectivamente la empresa con TI para generar soluciones y servicios que cumplan las necesidades de la organización.

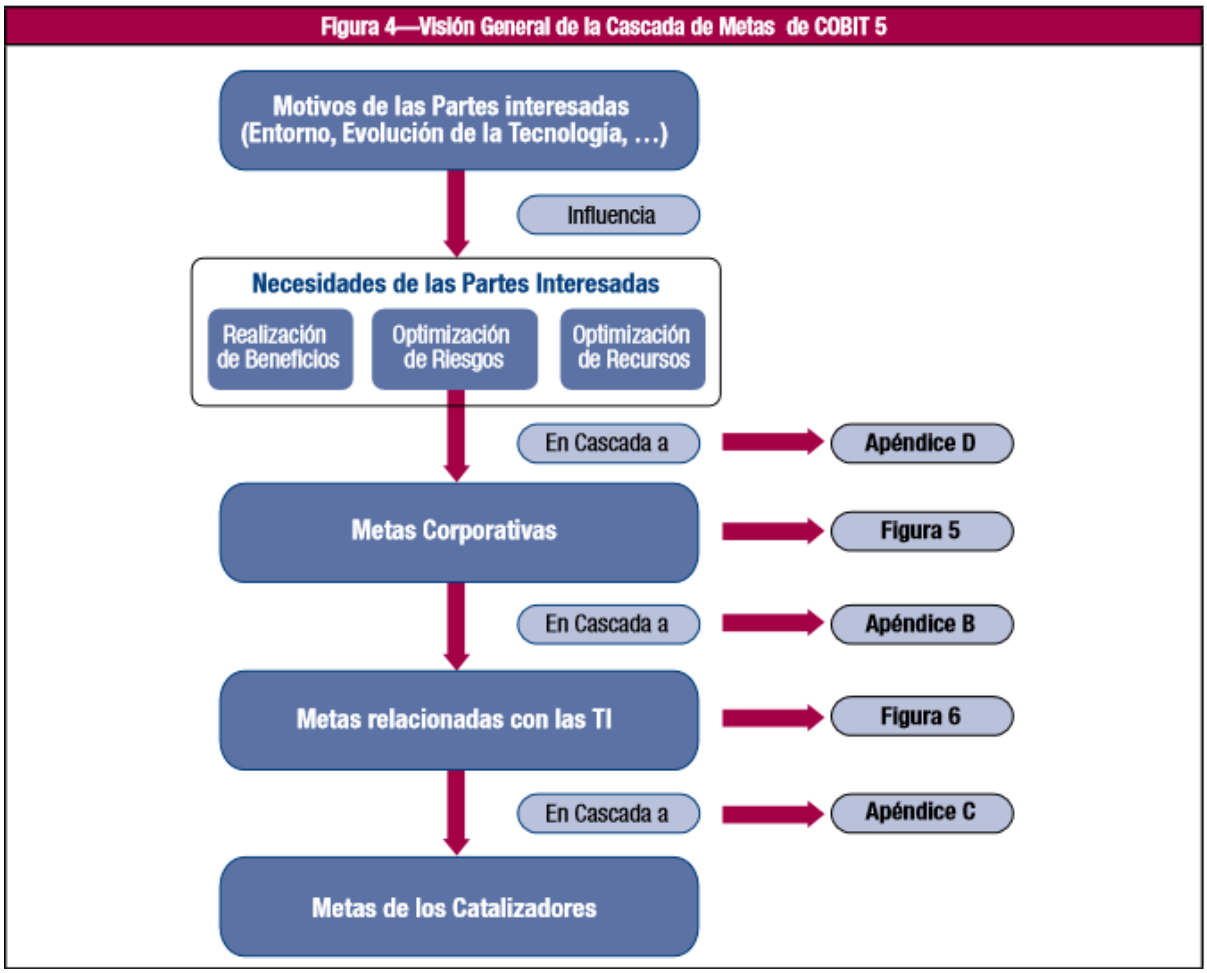

Ilustración 2: COBIT 5 vista de resumen de cascada de metas, tomado de libro COBIT 5 (COBIT 5 Task Force (2009-2011), 2012)

2.2.2 Principio 2: Cubrir la empresa extremo a extremo

Un punto fundamental de COBIT 5 es que integra el gobierno de la empresa con la administración de TI.

"cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no está enfocado solo en las funciones de TI, pero trata a la información y tecnologías relacionadas como recursos que necesitan un trato similar a todos los demás recursos empresariales" (COBIT 5 Task Force (2009-2011), 2012)

Este principio hace recaer la importancia de la gobernabilidad de TI y la administración de los catalizadores para poder hacerlo un factor que abarque toda la

organización, inclusivo para todos y con relevancia en todos los aspectos de gobierno y de administración de la información.

COBIT 5 logar emplear los catalizadores de tal forma que facilita a cada grupo de interés definir requisitos extensos para la información y su respectivo ciclo de vida, permitiendo conectar al modelo de negocio con una información adecuada.

2.2.2.1 Enfoque de Gobierno

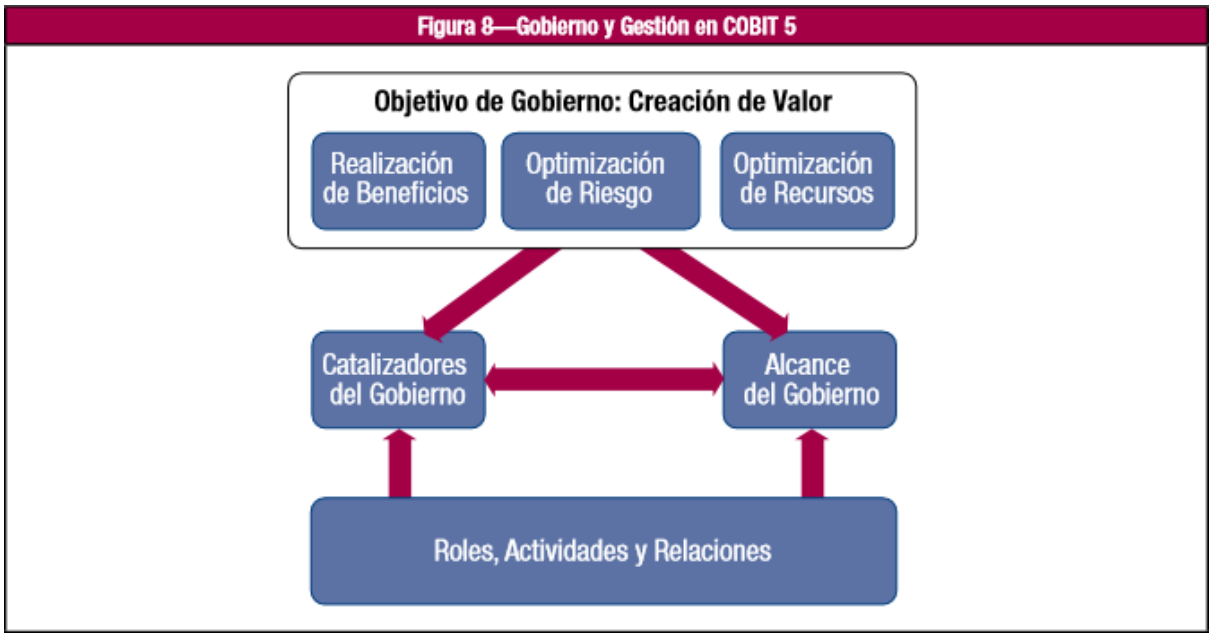

Ilustración 3: Gobierno y Gestión en COBIT 5, tomado de libro COBIT 5 (COBIT 5 Task Force (2009-2011), 2012)

El objetivo de gobierno es el de generar valor, que está enfocado a la organización y puede hacerse de distintas formas ya sea optimizando recursos, riesgos o mediante la realización de beneficios. Pero para lograr llegar a estos objetivos se debe emplear los catalizadores del gobierno y tener claro el alcance del gobierno.

Según COBIT 5, los catalizadores de gobierno son recursos organizacionales, ya sean marcos de referencia, estructuras, principios, procesos y prácticas, las cuales direccionan las acciones para encaminarlas hacia alcanzar los objetivos[23]

COBIT 5 recalca que el gobierno se aplica a toda empresa, organización o entidad y por lo tanto es posible definir diferentes vistas de la empresa a la que este es aplicado.

[23] (COBIT 5 Task Force (2009-2011), 2012)

"Es esencial definir bien este alcance del sistema de gobierno" (COBIT 5 Task Force (2009-2011), 2012)

Por ultimo tenemos los roles, actividades y relaciones, estos elementos definen los involucrados en el gobierno, sus responsabilidades y su forma de interacción. El siguiente grafico provisto por COBIT 5 da una explicación más amplia de este punto.

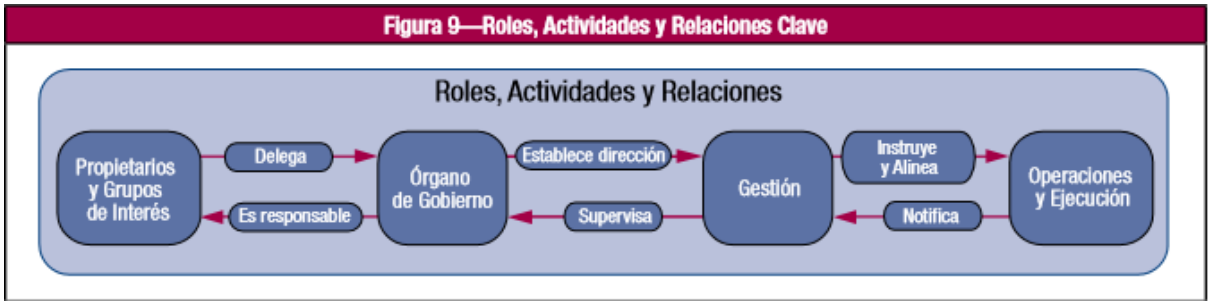

Ilustración 4: Roles, Actividades y Relaciones Clave, tomado del libro COBIT 5 (COBIT 5 Task Force (2009-2011), 2012)

Con este grafico se aclara los roles (propietarios, órgano de gobierno, gestión, operaciones y ejecución) que intervienen en el gobierno además de las actividades y su interrelación.

2.2.3 Principio 3: Aplicar un Marco de Referencia Único Integrado

La realidad es que existe un gran número de estándares o buenas prácticas que son aplicables en áreas de TI, cada uno con su guía y actividades a cumplirse. COBIT 5 se alinea con otros marcos de referencia y estándares de alto nivel, permitiendo y formando un marco general que sirve para manejar y gobernar el TI de la empresa.

El aspecto a resaltar es que COBIT abarca perfectamente todos los temas referentes a cobertura de la empresa, gestión y al gobierno. Esto lo hace por ser la integración de varias guías existentes de ISACA (COBIT4.1, Val IT 2.0, Risk IT, BMIS). Además, se alinea a otros estándares y marcos referenciales como son ITIL, TOGAF y normas ISO.

En el caso de este proyecto que se enfocará en el uso de COBIT 5 para la evaluación de seguridad de modelos "Cloud Computing" se observará la interacción del marco base con la guía profesional "COBIT 5 para seguridad de la información" en conjunto con las normas ISO 27000[24] que se enfocan en estándares de seguridad de la información.

[24] (ISO, 2016)

2.2.4 Principio 4: Permitir un enfoque holístico

"la administración de TI y gobernabilidad requieren un acercamiento holístico para ser eficientes y efectivos" (COBIT 5 Task Force (2009-2011), 2012)

COBIT 5 cuenta con "catalizadores" que permiten tomar en consideración las interacciones de componentes además de apoyar en la implementación de sistemas de administración y gobernabilidad del TI empresarial.

2.2.4.1 Catalizadores de COBIT 5

"Los catalizadores se definen como cualquier cosa que pueda ayudar a cumplir los objetivos de la empresa"[25]

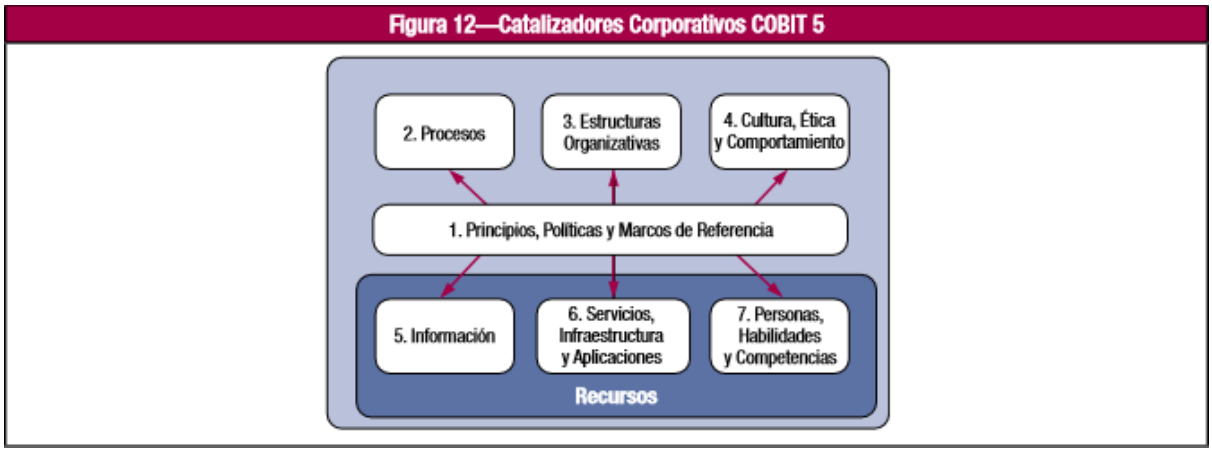

Ilustración 5: Catalizadores Corporativos COBIT 5, Tomado del libro COBIT 5 (COBIT 5 Task Force (2009-2011), 2012)

Según COBIT 5 existen 7 categorías de catalizadores:

Principios, políticas y marcos de referencia: se definen como el medio empleado para traducir comportamientos deseados en guías prácticas enfocadas para la gestión del día a día.

Procesos: se refieren al conjunto de actividades y prácticas que permiten cumplir objetivos y a su vez producir resultados que estén soportados en las metas relacionadas con TI.

Estructuras Organizativas: Entidades de toma de decisiones clave en una organización.

[25] (COBIT 5 Task Force (2009-2011), 2012)

Cultura, ética y comportamiento: son partes intrínsecas de los individuos y de la empresa que suelen ser subestimadas como factores de éxito en actividades de gobierno y gestión.

Información: se encuentra enmarcada en toda la organización, incluye todo su ciclo de vida, "la información es necesaria para mantener la organización funcionando y bien gobernada"[26] en especial al nivel operativo. Es un recurso clave de la organización.

Servicios, infraestructura y aplicaciones: Son todas las aplicaciones y tecnología que provee a la organización de servicios y procesamiento de información.

Personas, habilidades y competencias: abarca a todas las personas y sus cualidades necesarias para completar de forma satisfactoria toda actividad, correcta toma de decisiones y respectivas acciones correctivas.

Debido a la gran importancia de los catalizadores en COBIT 5 se cuenta con un desarrollo posterior del tema, que trata más a fondo las dimensiones y detallas de los mismos.

[26] (COBIT 5 Task Force (2009-2011), 2012)

2.2.4.2 Dimensiones de los Catalizadores de COBIT 5

Los catalizadores contienen varias “dimensiones” en común, las cuales brindan las siguientes características: “Proporciona una manera común, simple y estructurada de tratar con los catalizadores, permite a una entidad manejar sus complejas interacciones y facilita resultados exitosos de los catalizadores”[27]

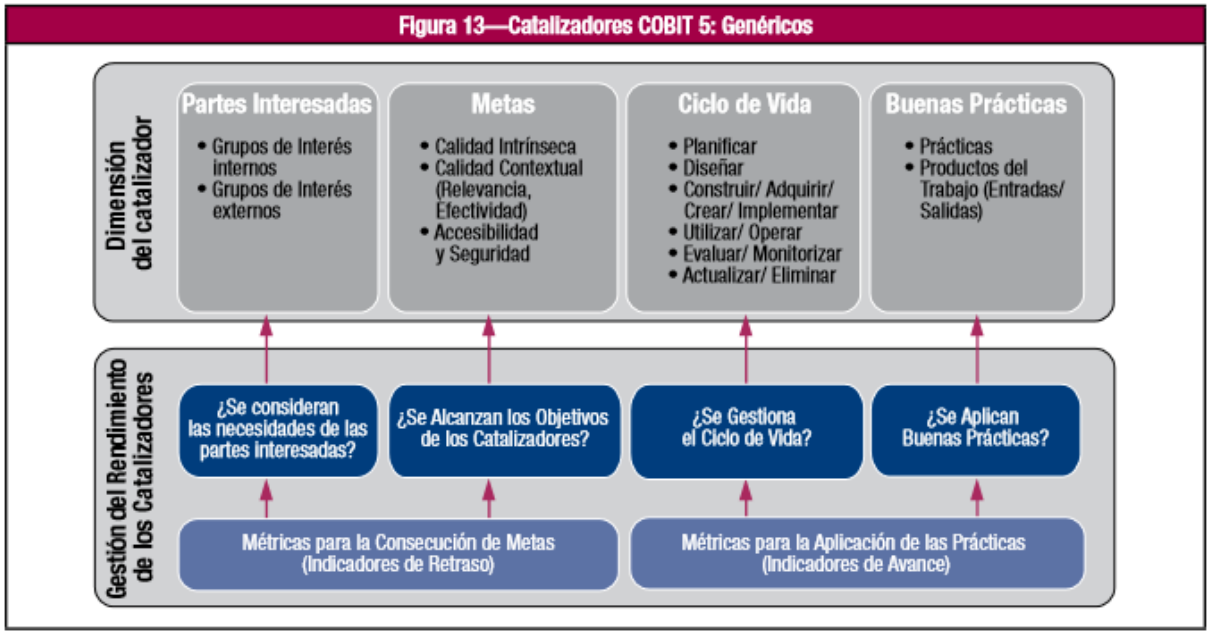

Ilustración 6: Catalizadores COBIT5: Genéricos, tomado del libro de COBIT 5 (COBIT 5 Task Force (2009-2011), 2012)

Como se observa en la ilustración existen 4 dimensiones de catalizadores cada una de ellas se relaciona a un aspecto de rendimiento, responden preguntas que a lo largo del proceso permitirán obtener indicadores, los que se enfocan en dar una visión del retraso o avance en las metas.

Al referirnos a los indicadores de “retraso” o mejor expresado de desfase, son indicadores orientados a salidas, nos estamos refiriendo a las métricas o el resultado actual que tiene el catalizador con respecto al valor necesario para que la meta sea alcanzada. Son indicadores de fácil medición, pero de difícil mejora. Las dimensiones que afectan este indicador son las siguientes:

Partes Interesadas: hace referencia a las partes que cumplen un rol o tienen un interés en dicho catalizador, estos grupos pueden ser internos o externos a la organización

[27] (COBIT 5 Task Force (2009-2011), 2012)

y cada uno puede tener sus propias necesidades e intereses, en ciertos casos pueden estos intereses se pueden contraponer.

Metas: Todo catalizador tiene metas, los catalizadores generan valor al ir cumpliendo cada una de las metas propuestas. Según COBIT 5, las metas se pueden definir de la siguiente manera: Resultados esperados del catalizador y aplicación u operación del catalizador en sí mismo.

Además de esto las metas según COBIT 5, pueden dividirse en:

Calidad intrínseca: Medida en la que el catalizador trabaja de manera precisa, objetiva para lograr resultados precisos y de confianza.

Calidad contextual: Medida en la que el catalizador y sus resultados son aptos para el propósito dentro del contexto operacional.

Accesibilidad y seguridad: Medida en que los catalizadores y sus resultados son accesibles y seguros.

Por otra parte, al referirnos a los indicadores de "avance" se toma en cuenta el funcionamiento del catalizador como tal. Y las dimensiones que afectan esta métrica son las siguientes.

Ciclo de vida: Este aspecto del catalizador se aplica desde su comienzo y operación hasta su posterior eliminación ya sea información, proceso o política. El ciclo de vida que se representa en COBIT 5 corresponde a una interpretación del Ciclo de Deming[28] este ciclo está dado de la siguiente manera: Planificar, Diseñar, Construir (adquirir, crear, implementar), Utilizar (operar), Evaluar (monitorizar), Actualizar.

Buenas Prácticas: Cada catalizador puede definir buenas prácticas, las cuales proveen ejemplos y sugerencias sobre la manera de implementar de una mejor forma el catalizador, sus entradas y salidas, soportan la obtención de los objetivos del mismo.

2.2.5 Principio 5: Separar el Gobierno de la Gestión

Para poder trabajar con COBIT 5 hay que tomar en cuenta la distinción entre Gobierno y Gestión de Tecnología. Puesto a que cada una engloba distintas actividades, estructuras organizativas y propósitos.

[28] Ciclo de Deming está dado por: Plan, Do, Check, Act (PDCA)

Gobierno: “El gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas”[29]

Gestión: “La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales”[30]

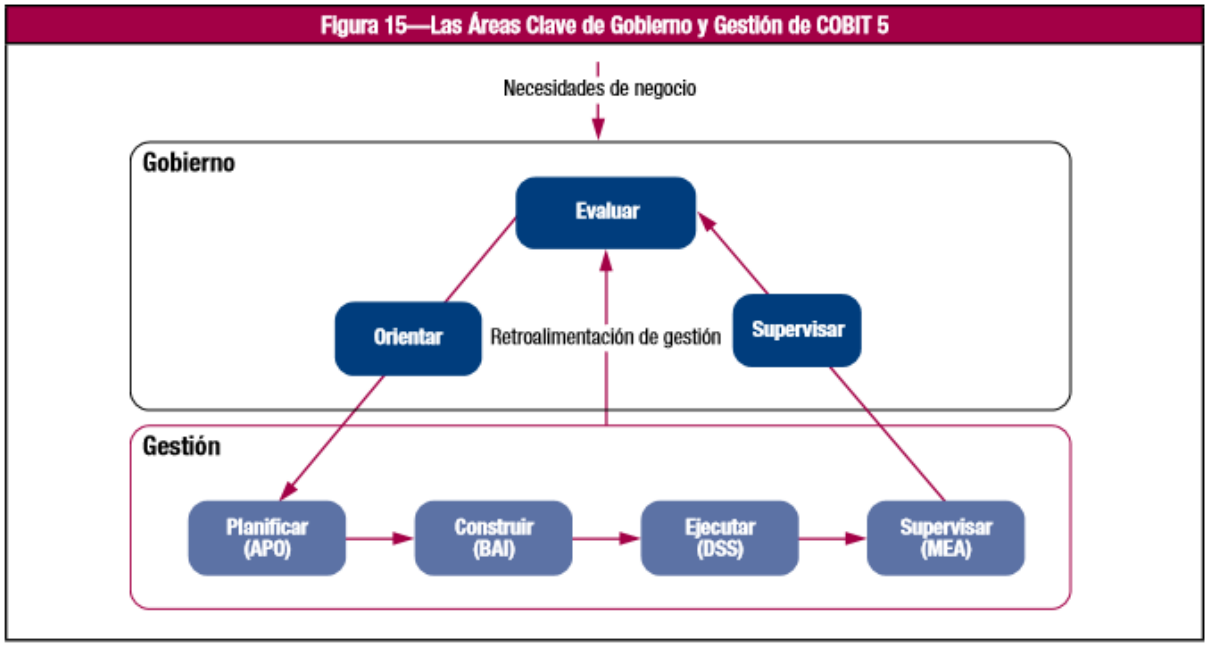

Ilustración 7: Las Áreas Clave de Gobierno y Gestión de COBIT 5, tomado del libro de COBIT 5 (COBIT 5 Task Force (2009-2011), 2012)

2.2.5.1 Dominios de COBIT5

Como se observa anteriormente COBIT divide las actividades que realiza el gobierno y la gestión, en la ilustración anterior se encuentran descritos los dominios de COBIT 5. Los dominios son contenedores y conjuntos afines de procesos que se enfocan en apoyar aspectos puntuales de la organización.

[29] (COBIT 5 Task Force (2009-2011), 2012)
[30] (COBIT 5 Task Force (2009-2011), 2012)

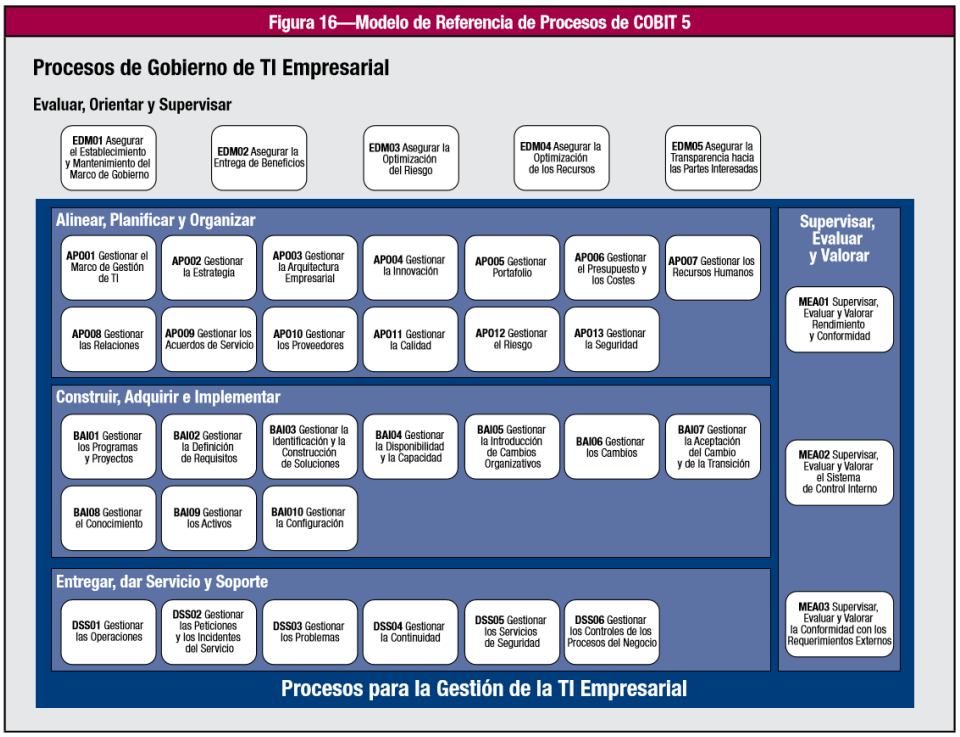

Ilustración 8: Modelo de referencia de procesos de COBIT 5, Tomado de libro COBIT 5 (COBIT 5 Task Force (2009-2011), 2012)

COBIT 5 cuenta con 5 dominios, uno de ellos direccionado al Gobierno de TI, concentrado en las tareas de: “Evaluar, Orientar y Supervisar”. Y los 4 restantes designados a la Gestión, que se preocupan: “Alinear, Planificar y Organizar”, “Construir, Adquirir e Implementar”, “Entregar, dar Servicio y Soporte”, “Supervisar, evaluar y Valorar”.

Dentro de cada uno de estos dominios existen un total de 37 procesos, cada uno con sus respectivas actividades enfocadas en apoyar aspectos puntuales de la organización.

Para este trabajo de disertación se tratarán principalmente los siguientes procesos[31] abarcados en COBIT 5:

APO12: Gestionar el Riesgo

APO13: Gestionar la Seguridad

DSS03: Gestionar los Problemas

DSS05: Gestionar los Servicios de Seguridad

[31] (COBIT 5 Task Force (2009-2011), 2012)

2.3 COBIT 5 relacionado a la Seguridad

COBIT 5 toma en cuenta el aspecto de la seguridad, relacionándola principalmente con la seguridad de la información, para entender profundamente este tema COBIT 5 cuenta con una Guía Profesional para Seguridad de la Información[32], la cual será material base para este trabajo de disertación además de dar los fundamentos de la guía metodológica que se desarrollará.

Como preámbulo y punto de partida COBIT 5 hace énfasis en crear un Sistema de Administración de Seguridad de la Información (ISMS), este sistema debe estar correlacionado con los procesos APO13: Gestionar la Seguridad, DSS04: Gestionar la continuidad y DSS05: Gestionar los servicios de seguridad. Estos procesos pasarán a ser la guía que permite definir y monitorear el sistema de seguridad.

Las motivaciones principales que llevaron al desarrollo de COBIT 5 para seguridad de la información son:

- La necesidad de la seguridad de la información dentro de un contexto empresarial, es decir, cubriendo toda la organización de extremo a extremo además de incluir la responsabilidad de IT en estas funciones.
- La relación cercana entre la información y los objetivos empresariales.
- Proteger la información con respecto a divulgación no autorizada, modificaciones involuntarias e intrusos.

"…el hecho es que la seguridad de la información es esencial para las operaciones empresariales del día a día, violaciones en la seguridad de la información pueden conllevar impactos dentro de la organización como ejemplo: daños financieros u operacionales." (ISACA, 2012)

Además de este ejemplo COBIT 5 trata de prevenir el mal uso de la información o alteraciones de la misma, para proteger a la organización de riesgos legales o perjuicios de la reputación de la empresa, para no poner en peligro relaciones con clientes y empleados.

[32] (COBIT 5 for Information Security, 2012)

3. Capítulo: Seguridad de la Información

El manejo de la información, ya sea personal o empresarial) siempre ha sido un punto base para las empresas, la información es un recurso fundamental para el éxito de una organización y con el proceso en la tecnología y en técnicas con las cuales acceder a la información relacionarla y encontrar patrones que permitan enfocar dichos datos para generar valor a la empresa han provocado que cada momento está sea más valiosa.

Esta característica de evolución en su grado de importancia también es la que hace que el resguardo y seguridad con la que se maneja haya crecido y se convierte en un aspecto fundamental para los gobiernos de empresas.

3.1 Importancia de la información

Algo que se debe entender es el grado de importancia de la información: la información es intrínsecamente fundamental. Puesto a que son datos confiables, específicos, organizados y más que nada cuentan con un propósito.

Y debido a esto hay que recalcar que la información es un recurso vital para todos, en especial para organizaciones. Al contar con toda la información necesaria las empresas pueden tomar decisiones fundamentadas, reorganizar estrategias de negocio, modificar y crear productos o servicios direccionados para sus clientes. Por este aspecto es fundamental para la empresa contar con información que cumpla con los requerimientos de seguridad objeto en este trabajo.

Pero hay una contraparte para que la información sea útil no solo se debe contar con ella, el grado de importancia de esta recae altamente en las acciones y decisiones que se puedan hacer en base de la misma.

Para entender mejor este punto se puede ejemplificar lo siguiente: si se cuenta con información que evidencia la baja satisfacción de clientes. Esta información solo es útil si dentro de ella se evidencian formas en las que podemos mejorar el nivel de satisfacción. Pero esta información no tendría valor alguno y perdería toda importancia si después de entender el problema la organización o empresa no hacen nada para cambiarlo o resolverlo.

Para sintetizar la idea la importancia de la información recae en dos aspectos:

- La confiabilidad de la información como tal y las acciones que se puedan hacer en base a la misma.

- “La información es valiosa porque puede afectar comportamientos, decisiones y desenlaces.” (WebFinance, 2016)

3.2 ¿Qué es seguridad de la información?

Al ver que la información es fundamental para las organizaciones, algo que debe estar ligado totalmente es su seguridad.

La seguridad suele hacer referencia a la ausencia de riesgo y en generar confianza.

En base a esto se entiende que el principal propósito es disminuir riesgos y generar confianza, al aplicarlo a la información tenemos lo siguiente.

“El término seguridad de la información significa proteger la información y sistemas de información de accesos no autorizados, uso, divulgación, modificación o destrucción para proporcionar: integridad, confidencialidad y disponibilidad” (Legal Information Institute (LII) Cornell university Law School, 2016)

Esta definición que se presentó previamente es empleada de forma similar por organismos como CNSS, ISACA e ISO. Lo que genera la base y puntos clave sé que consideraran en la generación de la guía metodológica objeto de la presente disertación.

Para esto se debe comprender de mejor manera los siguientes conceptos y para ello se usan las definiciones dadas por NIST[33]:

Integridad: Protegerse contra la modificación o destrucción inadecuada, asegurar la no repudiación de la información y la autenticidad. También se la entiende como la propiedad que tienen los datos sensibles a no ser modificados o eliminados de una manera no autorizada y no detectada.

Confidencialidad: Preservar las restricciones autorizadas en el acceso y divulgación de información, incluyendo medios para proteger la información del propietario. También

[33] National Institute of Standards and Technology, es decir Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST)

se la entiende como la propiedad de que la información sensible no sea revelada a personas, entidades o procesos no autorizados.

Disponibilidad: Garantizar el acceso oportuno y fiable a la información uso. También se la puede entender como la propiedad de ser accesible y utilizable a petición de una entidad autorizada.

Con esto se entiende que características debe fomentar y mantener la seguridad de la información, pero para profundizar un poco, se debe comprender que es como tal por ello podemos empezar ratificando que la seguridad de información es una práctica, un conjunto de estrategias para administrar políticas, herramientas y procesos de manera que se logre prevenir, documentar y detectar cualquier amenaza dirigida a información digital o física.

Para lograrlo las estrategias suelen apoyarse principalmente en procesos de negocio, los cuales están construidos alrededor de la triada CIA[34], es decir, Confidencialidad, Integridad y Disponibilidad. Todas las políticas y normas deben direccionarse a precautelar y asegurar tanto datos como información y sus respectivos medios de comunicación y almacenamiento.

Para entender de mejor manera el impacto y la importancia actual de la Seguridad de la Información se realizará un análisis, basado en la encuesta “The global State of Information Security Survey 2016”[35] realizado por la consultora (PwC) PrincewaterhouseCoopers LLP. El objetivo de este informe es dar un contexto de los incidentes de seguridad que se han suscitado en 2015.

Como un punto de inicio se toma en cuenta estadísticas que se relacionan a los riesgos e incidentes de seguridad.

[34] La triada CIA, hace referencia a las siglas en inglés Confidentiality, Integrity and Availability.
[35] (pwc, PrincewaterhouseCoopers LLP, 2016)

Ilustración 9: Estadísticas relacionadas a Incidentes de Seguridad, Tomado de: Resultados de la Encuesta Global de Seguridad de la Información 2016, Pág 3.

Al contar con estos datos se puede ver que el número de ataques en 2015 han incrementado, pero también hay que entender que estos incidentes han sido detectados lo que significa cierta mejora en este aspecto de seguridad, por otra parte, los incidentes relacionados a robar información “confidencial” incluyendo patentes y propiedad intelectual han aumentado en más de la mitad lo que debe generar mucha preocupación para las organizaciones y ser un foco de atención en este aspecto.

Por otra parte, una estadística que da mucha información y a su vez brinda altos niveles de preocupación en cuanto formas de tratar los recursos humanos de la empresa es la siguiente.

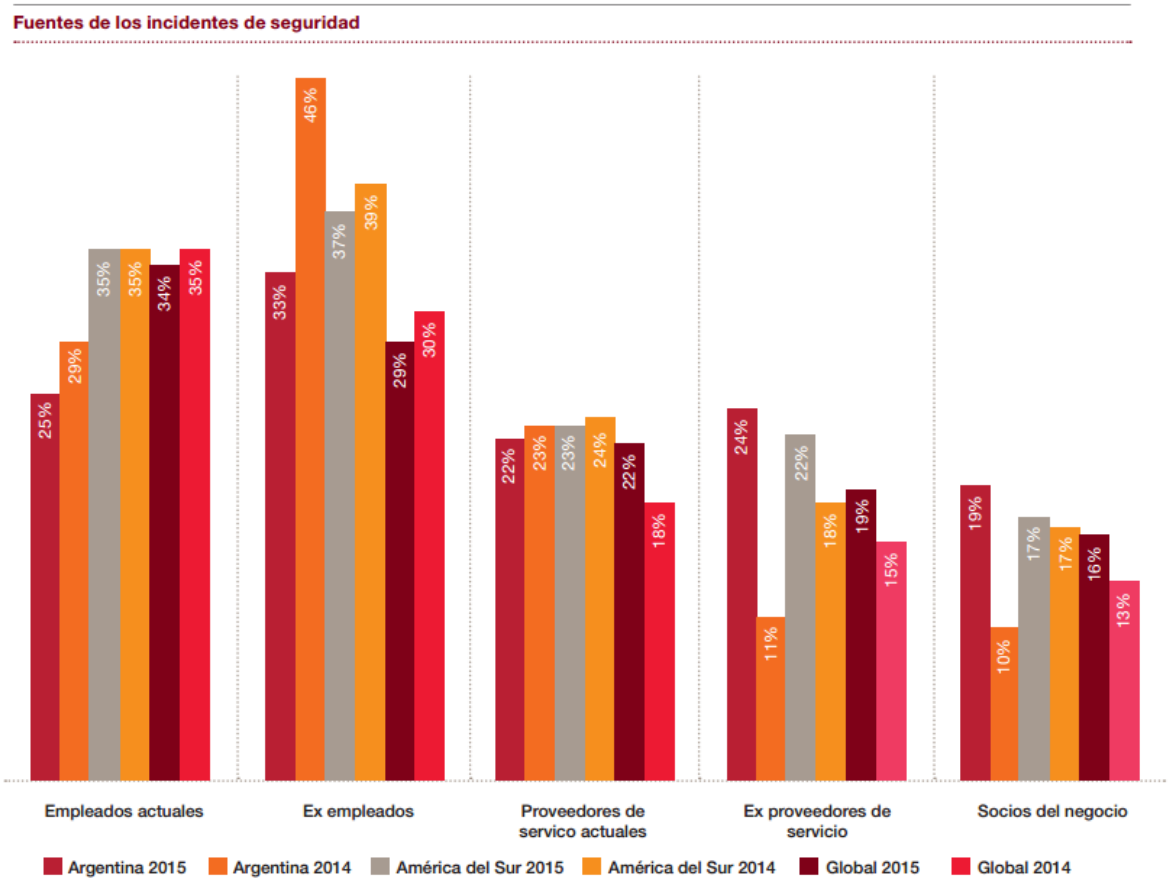

Ilustración 10: Fuentes de Incidentes de Seguridad, Tomado de: Resultados de la Encuesta Global de Seguridad de la Información, 2016, Pág 17.

Es preocupante debido a que las dos principales fuentes de incidentes de seguridad están relacionadas a recursos humanos, el punto fundamental que se debe cuidar, capacitar y concientizar en cuanto a la seguridad de la información son los empleados (actuales y anteriores) además de proponer acuerdos o políticas que aseguren la información con consultores, contratistas, socios y proveedores.

Como se puede observar en el gráfico anterior las principales fuentes que generan inseguridad para la información son personas relacionadas directamente con la empresa, personas que están involucradas en manejar, comunicar e incluso modificar esta información, tener este aspecto en cuenta debe ser fundamental para poder mejorar las normas de seguridad de la información en cualquier organización.

El entorno de la ciberseguridad[36] y su importancia para las empresas también ha tenido un crecimiento considerable, generando que las empresas incursionen en nuevas formas para protegerse de incidentes de seguridad.

Ilustración 11: Involucramiento de ejecutivos y directorio en ciberseguridad, Tomado de: Resultados de la Encuesta Global de Seguridad de la Información, 2016, pág 10

Las empresas en 2015, al menos la mitad de ellas, han incursionado en incluir a un CISO[37] como encargado de la seguridad empresarial, además de ello cuentan con planes de capacitación y entrenamiento y modelos de conducta para todo el personal para concientizar estrategias de seguridad de la información.

Además de esto 69%[38] ha optado por incorporar servicios de seguridad basados en Cloud Computing, esto permite contar con los siguientes beneficios.

[36] La protección resultante de todas las medidas para negar el acceso no autorizado y la explotación de sistemas informáticos amigables. Definición tomada de: The free Dictionary by Farlex
[37] CISO (Chief Information Security Officer) o Director de Seguridad de la Información
[38] (The Global State of Information Security Survey 2016, 2016, pág. 5)

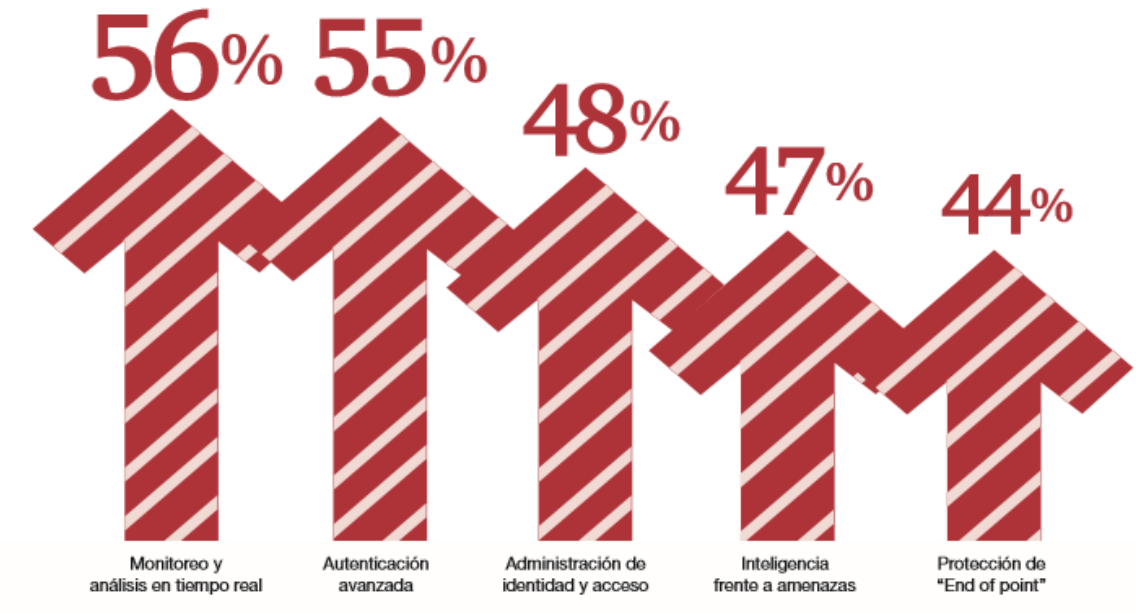

Ilustración 12: Servicios de seguridad basados en la nube, Tomado de: Resultados de la Encuesta Global de Seguridad de la Información 2016, pág 5

El principal beneficio al que recaen las empresas al incluir estos servicios es al de contar con un monitoreo de tiempo real de tráficos de red, tecnologías de bloqueo de ataques o intrusión en la red, consiguiendo con esto tener tiempos de respuesta menores para tratar con incidentes de seguridad. Además de contar con medidas más avanzadas para la autenticación y manejos de identidad en los sistemas empresariales contar con mejores medidas.

Guido Sacchi, CIO de Global Paymentes, recalca la importancia de emplear servicios de seguridad basados en la nube debido a que facilitan en seguimiento de alertas y brindan mejor información de las amenazas, filtrando dicha información y eventos, para su mejor consideración por personal de seguridad y descartando falsos positivos.

Este tipo de testimonios y la gran tendencia de emplear Cloud Computing por empresas ha generado el gran crecimiento en la adopción de servicios de seguridad basada en la nube.

Finalmente, como aspecto principal para este trabajo de disertación está el punto de adopción de marcos de referencia enfocados a la ciberseguridad. En 2015 un 91% de las empresas ha adoptado este tipo de marcos. Al contar con un número tan elevado se puede ver que la conciencia empresarial esta direccionada en buen camino para

resguardar su información. Como principales beneficios de la adopción de estos marcos de referencia se citan los siguientes.

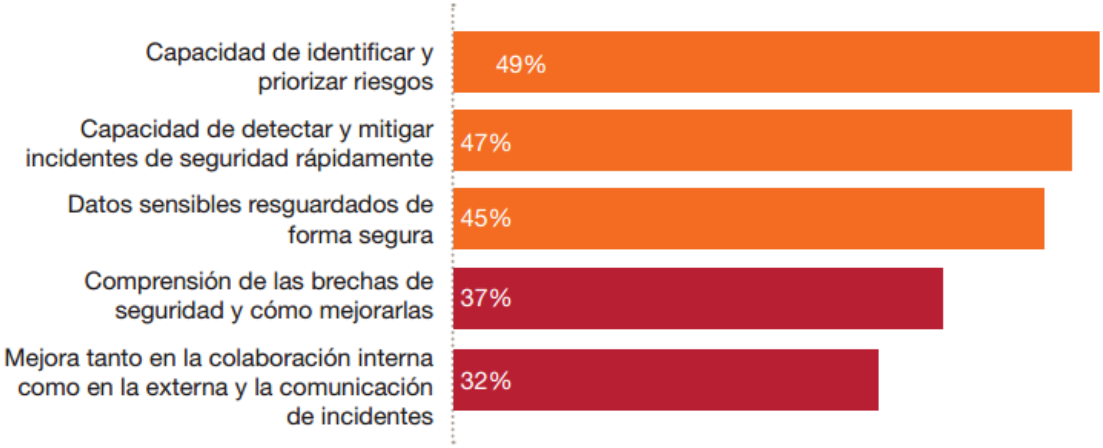

Ilustración 13: beneficios de marcos de referencia de seguridad, Tomado de: Resultados de la Encuesta Global de Seguridad de la Información,2016 pág 4

El principal beneficio que se tiene es poder identificar los riesgos de seguridad y priorizar entre ellos para mitigarlos. Otros aspectos que a mi parecer son de suma importancia son: el mejorar la comunicación interna y externa y contar con un mejor entendimiento en las brechas de seguridad. Estos beneficios desde nuestra perspectiva son los que más deben aprovecharse, son puntos que toda empresa debe tratar de explotar, debido a que la principal fuente de riesgo es el personal de la organización, si al implementar estos marcos de referencia generamos una mayor conciencia y mejor comunicación respecto a los principales riesgos con los que cuenta la empresa en seguridad de información, se puede mejorar inmensamente.

Dentro de los marcos de referencia más utilizados para resguardo de la ciberseguridad están las guías de la ISO 27001 y los estándares del NIST (US National Institute of Standars and Technology o Instituto nacional de estándares y tecnología de los Estados Unidos).

3.3 Contraste entre COBIT 5 y ISO/IEC 27001

Para el desarrollo de la guía metodológica de este trabajo se utilizará de base COBIT 5, que es un marco de referencial enfocado al gobierno y gestión de TI, que cuenta con una guía profesional que trata seguridad de la información. Por otra parte hay que tener en cuenta que una de las principales guías empleadas mundialmente es la ISO 27001. Es por ello que se realizará un mapeo de ambas para dar a entender sus bases, sus principales estrategias y más que nada sus entornos de aplicación.

Un punto que se debe entender es que COBIT 5 es un marco de Gobierno de TI, una guía de buenas prácticas que se enfoca en como llevar a cabo una correcta Gestión de la tecnología, mientras que la ISO 27001 es una normativa estándar de seguridad, al ser un estándar está en un nivel más alto que las guías de buenas prácticas, pero puede "aterrizarse" para estar implementada a la par y de forma más específica en el entorno abarcado por COBIT 5.

Al referirse a ISO 27001 como una guía macro se hace énfasis en que estas guías de buenas prácticas se enfocan o recaen en estándares de seguridad de la información, englobando todo el espectro que esta rama trata. Mientras que COBIT 5 hace referencia a un espectro menor o mejor dicho se enfoca en el gobierno, por ello en este marco se tratan Estándares de Gobierno de Seguridad de la Información.

Debido a esta distinción se puede ver que COBIT 5 y el estándar de ISO 27001 no son excluyentes, y más bien pueden implementarse en conjunto e incluso apoyarse uno con otro, para entender de mejor manera este aspecto se realizará un análisis de pros y contras de ambos marcos de referencia, lo cual sustentará la decisión final de apoyarse en ambas guías, principalmente en COBIT debido al enfoque que tiene este trabajo de disertación.

3.3.1 Pros y Contras de COBIT para seguridad de la información

El primer punto que se debe destacar es que COBIT como tal no fue diseñada con el único propósito de tratar la seguridad de la información, sino que es una guía y herramienta para gobierno y gestión de las tecnologías de la información. Claro que se debe recalcar que cuenta con procesos y guías técnicas que hacen referencia a este tema.

COBIT 5 cuenta con 37 procesos, de los cuales 3 (APO13 Administrar la Seguridad, DSS04 Administrar la Continuidad y DSS05 Administrar servicios de Seguridad)[39] están enfocados y son los conductores de lograr la Seguridad de la Información. Esto no quiere decir que se puedan emplear otros procesos de COBIT 5 como soporte ni que solo estos procesos impliquen “Seguridad”.

La principal ventaja de COBIT 5 para tratar la seguridad de la información es que el marco de referencia logra hacer una integración de esta rama dentro del marco de gobierno de TI generando un mayor rango de cobertura. Incluso si se emplea COBIT 5 solo para contar con guías de seguridad de información, este marco intrínsecamente provee aspectos del marco base, lo que genera un beneficio a la empresa si se desea realizar una aplicación por ciclos o partes del mismo.

COBIT 5 para la seguridad de información, al ser un marco general de buenas prácticas, recae en la forma de implementar dicha seguridad, es decir en “como” hacer las cosas, ciertos aspectos no son detallados en cuanto a que medidas deben tomarse para mejorar la seguridad, algo que se ha corregido de cierta forma con la adición de guías profesionales y técnicas para dar una mejor visión de la implementación de COBIT 5.

3.3.2 Pros y contras de ISO 27001 para seguridad de la Información

Lo fundamental de la ISO 27001 es que es una guía cuyo único propósito es la seguridad de la información y como tratar con estos problemas.

La ISO 27000 es aplicable cuando se requieren estándares de administración de sistemas de seguridad de la información, ISMS (Information Security Management System), y empezó como el estándar ISO 17799:2005.

El principal beneficio de la ISO 27001 es que define prácticas y métodos para la implementación de la seguridad de la información detallando los controles necesarios para ese efecto. Se enfoca en aspectos de comunicación e intercambios de datos confiables.

Como se puede ver lo fundamental de la norma ISO 27001 es que proporciona mayores detalles de qué hacer y controles a implementar. Esta es la principal diferencia y

[39] (ISACA, 2012, pág. 13)

ventaja competitiva que tiene respecto a las guías de COBIT 5 que se enfocan en qué sin dar mayores detalles de cómo.

3.3.3 Análisis de COBIT 5 en comparación con ISO 27001

El siguiente cuadro, se basa en el trabajo realizado por Varun Arora, en su informe "Comparing Different information security standards", para la universidad Carnegie Mellon de Qatar. El objetivo del cuadro es general puntos de comparación y contraste entre COBIT 5 e ISO 27001, para analizar su respectivo enfoque, paradigma, alcance.

	COBIT 5	**ISO 27001**
ENFOQUE	Orientación al negocio y Gobierno de TI.	Implementación de control de seguridad y enfocado en gestionar riesgos
PARADIGMA	Planificar los procesos de TI	Sistemas de administración de seguridad de la Información
ALCANCE	Solución integral, un marco completo para Gobierno de TI de la organización además de incluir planificación de seguridad.	Guía independiente para la seguridad

Tabla 2: Cuadro de diferencias de COBIT 5 e ISO 27001.

En este cuadro se aclaran los principales aspectos que diferencian un marco del otro. Al ver esto se observa que son enfoques distintos para el mismo tema y su posible aplicación paralela es viable. A pesar de la diferencia de enfoques, ambos marcos se preocupan de los mismos problemas, COBIT 5 pone un amplio enfoque en el gobierno de TI mientras que ISO se enfoca específicamente en la seguridad, pero el siguiente mapeo de procesos de ambas guías tiene como objetivo enfatizar de mejor manera los puntos de semejanza.

La siguiente información tiene como base el documento "234-Mapeando fortalezas de COBIT 5 Seguridad con ISO/IEC 27001:2013"[40] en el cual se detalla completamente un

[40] (Tello Meryk, 2014)

mapeo de procesos de ambos marcos de referencia, pero para este trabajo solo se tomarán en cuenta los procesos de COBIT 5 que si se relacionen con los requerimientos de ISO/IEC 27001:2013.

Se menciona la versión 2013 debido a que es la versión más actual que a la fecha está disponible para Ecuador, basándose en la disponibilidad del catálogo INEC, distribuidor oficial de ISO para este país.

	COBIT 5	**ISO/IEC 27001:2013**
EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia del Gobierno	5.1 Liderazgo y compromiso 5.2 Política 5.3 Roles, responsabilidades y autoridades organizacionales 6.2 Objetivos de seguridad de la información y la planeación para su logro 7.4 Comunicación A.5 Política de Seguridad de Información
EDM02	Asegurar la entrega de beneficios	4.1 Entendiendo a la organización y su contexto 4.2 Entender las necesidades y expectativas de las partes interesadas 6.1.1 General 9.3 Revisión Gerencial 10 Mejoramiento
EDM03	Asegurar la optimización de riesgo	5.2 Política 6.1 Acciones para abordar los riesgos y las oportunidades 7.5 Información documentada 8.1 Plan operacional y de control 8.3 Tratamiento al riesgo de seguridad de información 9.1 Monitoreo, medición, análisis y evaluación 9.3 Revisión gerencial
EDM04	Asegurar la optimización de recursos	4.4 Sistema de Administración de la seguridad de información 7.1 Recursos 7.2 Competencia 7.3 Concientización
EDM05	Asegurar la trasparencia respecto a las partes interesadas	A.12 Operaciones de Seguridad

Tabla 3: Mapeo de relación de procesos de Gobierno de COBIT 5 con ISO/IEC 27001:2013

En la tabla anterior se puede observar de forma clara que todos los procesos de monitorio, dirección y evaluación, destinados para el Gobierno de TI de COBIT 5 tienen alguna relación con los requerimientos mencionados en ISO/IEC 27001:2013. Esto hace ver la importancia y la vialidad de utilizar ambos marcos de referencia. Además de recalcar que a pesar de la diferencia en sus enfoques son muy similares en los aspectos que abarcan.

Para continuar con este análisis se tienen las siguientes tablas que muestran los procesos de COBIT 5 que forman parte de la gestión de TI y la relación que tienen con los requerimientos de ISO/IEC 27001:2013.

	COBIT 5	**ISO/IEC 27001:2013**
APO01	Gestionar el marco de referencia de la gestión de TI	5 Liderazgo A.5 Política de seguridad de la información A.6 Organización de seguridad de la información
APO02	Gestionar la estrategia	4 Contexto de la organización 5.2 Política 6 Planeación
APO07	Gestionar los recursos humanos	7.2 Competencia 7.3 Concientización A.7 Seguridad de Recursos Humanos
APO08	Gestionar las relaciones	A.6.1 Organización interna
APO10	Gestionar los proveedores	A.15 Relación con proveedores
APO11	Gestionar la calidad	4.1 Entendiendo la organización y su contexto 4.2 Entender las necesidades y expectativas de las partes interesadas 6.1.1 General 9.3 Revisión gerencial 10 Mejoramiento
APO12	Gestionar el riesgo	5.2 Política 6.1 Acciones para abordar los riesgos y las oportunidades 7.5 Información documentada 8.1 Plan operacional y de control 8.3 Tratamiento al riesgo de seguridad de información 9.1 Monitoreo, medición, análisis y evaluación 9.3 Revisión gerencial
APO13	Gestionar la seguridad	Aplica todo requerimiento del estándar ISO/IEC 27001:2013

Tabla 4: Mapeo de relación de procesos de Gestión (alineación, planificación y organización) de COBIT 5 con ISO/IEC 27001:2013

En esta tabla se ratifica la importancia del proceso: APO13: Gestionar la seguridad, puesto que este proceso se relaciona en su totalidad con los objetivos del marco de referencia de la ISO. Además de este proceso se debe tomar en cuenta que se mencionan los proceso que involucran gestión de riesgo y personas relacionadas con la organización, tanto internas como externas, esto es importante debido a las estadísticas[41] previamente mostradas ya que son la principal fuente de incidentes de seguridad para las empresas.

[41] Hace referencia a la Ilustración 10 del documento.

	COBIT 5	ISO/IEC 27001:2013
BAI02	Gestionar la definición de requerimientos	A.18 Cumplimiento
BAI03	Gestionar la identificación y construcción de soluciones	A.14 Adquisición, desarrollo y mantenimiento de sistemas
BAI04	Gestionar la disponibilidad y capacidad	A.12.1.3 Administración de capacidad
BAI06	Gestionar cambios	A.12.1.2 Administración de cambios
BAI07	Gestionar la aceptación y transición de cambios	A.12.1.4 Separación de los ambientes de desarrollo, prueba y operaciones
BAI08	Gestionar el conocimiento	7.5 Información documentada
BAI09	Gestionar los activos	A.8 Administración de activos

Tabla 5: Mapeo de relación de procesos de Gestión (Construcción, Adquisición e Implementación) de COBIT 5 con ISO/IEC 27001:2013

Estos procesos tienen su par en la ISO/IEC 27001:2013, y todos hacen referencia hacia formas seguras de manejar recursos de la empresa y maneras adecuadas de manipular y cambiar estos mismos.

	COBIT 5	ISO/IEC 27001:2013
DSS01	Gestionar operaciones	6.1 Acciones para abordar los riesgos y oportunidades 8 Operaciones A.11 Seguridad física y ambiental A.12.3 Respaldos A.12.4 Monitoreo y registro A.15 Relación con proveedores
DSS02	Gestionar peticiones e incidentes de servicios	A.16 Administración de incidentes de seguridad de la información
DSS04	Gestionar continuidad	4.1 Entendiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 7.5 Información documentada 10 Mejoramiento
DSS05	Gestionar servicios de seguridad	Aplica todo requerimiento del estándar ISO/IEC 27001:2013
DSS06	Gestionar controles de procesos de negocio	6.1.2 Evaluación de riesgo de seguridad de la información 9 Evaluación del rendimiento A.8.2 Clasificación de la información A.9.4 Control de acceso a los sistemas y aplicaciones

Tabla 6: Mapeo de relación de procesos de Gestión (Entrega, Servicio y Soporte) de COBIT 5 con ISO/IEC 27001:2013

Dentro de este dominio de procesos, el fundamental y que se relaciona con todo lo mencionado en la norma ISO/IEC 27001:2013 es DSS05 Gestionar servicios de seguridad, como se ve este proceso se enfoca netamente a tratar este problema, otro al que debe prestarse mucha atención es el DSS06 debido a que este trata los controles de procesos del negocio, por ello se debe cuidar mucho y enfatizar técnicas que mejoren la seguridad de los mismos.

Por ultimo tenemos los procesos de gestión englobados en monitoreo, evaluación y valoración. Algo importante es que por el aspecto intrínseco de los mismos estos son fundamentales y se deben tomar en cuenta siempre que se trate de seguridad de la información.

	COBIT 5	**ISO/IEC 27001:2013**
MEA01	Monitorear, evaluar y valorar el rendimiento y la conformidad	4.1 Entendiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 9 Evaluación del rendimiento
MEA02	Monitorear, evaluar y valorar el sistema de control interno	4.1 Entendiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 9 Evaluación del rendimiento A.18.2 Revisiones de seguridad de la información
MEA03	Monitorear, evaluar y valorar la conformidad con los requerimientos externos	4.1 Entendiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 9 Evaluación del rendimiento A.18.1 Cumplimiento con requerimientos legales y contractuales

Tabla 7: Mapeo de relación de procesos de Gestión (Monitorear, evaluar y valorar) de COBIT 5 con ISO/IEC 27001:2013

Después de un análisis más profundo se tiene que tanto COBIT 5 como ISO/IEC 27001:2013 tratan de generar confidencialidad, integridad y disponibilidad para la información, para ello cuentan con varias semejanzas que los encaminan a cumplir la seguridad de información de la organización.

- Entendimiento de la organización, necesidades y expectativas
- Responsabilidad de la Alta Gerencia y resto de roles
- Planificación
- Medir, evaluar y tratar el riesgo

- Documentación (resultados)
- Mejoramiento continuo

Es cierto que cuentan con todos estos puntos de similitud y que tratan de solucionar el mismo problema, su aplicación puede darse en conjunto, no se excluyen en implementación y la aplicación de ambos provee un amplio margen de protección y brinda seguridad de información. A pesar de tener pequeños aspectos diferenciantes en su aplicación.

Para este trabajo de disertación se tomará como guía base a COBIT 5 para la seguridad de información y si es necesario algún apoyo externo se procederá a tomar información de la ISO/IEC 27001:2013 debido a su gran similitud.

4. Capítulo: Desarrollo de Guía Metodológica

En este capítulo se detallan aspectos de análisis respecto al contenido del marco guía COBIT 5 que fueron empleados para desarrollar la guía metodológica de evaluación de seguridad. Además de contenido adicional para comprender como los temas analizados influyen en el nivel de Seguridad de Información de la organización.

La guía Metodológica de Evaluación se encuentra como anexo a esta disertación por ello se recomienda revisarla en conjunto con este Capítulo para tener una visión complementaria que brinda conceptos e ideas claves empleadas en la implementación de seguridad de Información en una organización.

4.1 Justificación

El desarrollo de esta disertación se fundamenta en realizar una guía de evaluación que pueda ser aplicada principalmente por proveedores de servicio de Cloud Computing, en la ciudad de Quito, aunque hay que recalcar que los temas que se tratan en la guía no están cerrados a solo aplicarse en dicho entorno, debido a que los aspectos de seguridad, y seguridad de la información, son aplicables en una mayor escala esto hace posible que las buenas prácticas y conceptos que se describen y son tomados como elementos de evaluación en esta guía sean adaptables a otros entornos, además debido a que la guía toma como pauta el trabajo realizado por ISACA en su marco de referencia de COBIT 5, intrínsecamente hace aplicable esta guía a otros entornos laborales.

4.2 Motivación

En la actualidad el modelo de “Cloud Computing” está en un punto de mayor adopción y crecimiento como modelo de servicios, esto ocurre a pesar de que a lo largo de su proceso de maduración han existido grandes dudas, principalmente provocadas por preocupaciones respecto a la seguridad de información que este modelo brinda, ya que se maneja directamente información de clientes. Este aspecto es fundamental en que tome la decisión de estudiar más a profundo formas en las que se pueda brindar un servicio seguro, cumpliendo con los tres aspectos básicos de seguridad de información (Confidencialidad, Integridad y disponibilidad).

De la misma manera la elección de emplear a COBIT 5 como marco base, se da puesto a que es uno de los Framework más empleados a nivel mundial, lo que genera mayor familiarización con los conceptos que se tratarán en la guía de este trabajo de

disertación. Además, provee una guía de alto nivel acoplable a estándares u otras buenas practicas facilitando de gran manera el realizar una guía complementaría, como es el caso de esta disertación, que pueda ser implementada sin mayor dificultad a las distintas realidades empresariales.

Para concluir cabe recalcar que lo fundamental de este trabajo es realizar una guía de evaluación inicial, basada en los principios de COBIT 5 para lograr evaluar la seguridad de los proveedores de servicios “Cloud Computing”.

4.3 Introducción

La Guía Metodológica se basa en la información provista en “COBIT 5 for Information Security” y se enfocará en realizar las evaluaciones de seguridad basándose solo en temas tratados dentro de este manual, principalmente se tomará en cuenta el manejo e implementación adecuada de los catalizadores y los siguientes procesos:

- APO13 Administración de Seguridad
- DSS04 Administración de Continuidad
- DSS05 Administración de Servicios de Seguridad

Estos procesos son los más relacionados a Seguridad de la Información y deben ser los primeros en cumplir una correcta ejecución, ya que si una organización los administra e implementa adecuadamente contará con un sistema de seguridad inicial adecuado.

Para entender plenamente el propósito de la guía hay que tener una definición que facilite comprender el concepto de Seguridad de la Información, para ello se tendrá la siguiente definición de ISACA:

“Asegurar qué dentro de la empresa, la información esté protegida contra la divulgación a usuarios no autorizados (Confiabilidad), la modificación inadecuada (Integridad) y al no acceso cuando es necesario (Disponibilidad)”[42]

Dentro de COBIT5 existen muchos aspectos que analizar al momento de implementarlo como guía de buenas prácticas enfocado a seguridad de información, se debe considerar factores de entorno, contexto actual de seguridad de información de la organización y requerimientos de seguridad de información. Estos temas están enfocados en la implementación inicial de una organización con cultura de seguridad de información.

[42] (ISACA, 2012)

Al ser está disertación una guía de evaluación no se tratarán dichos aspectos, sino que se analizarán temas relacionados con la evaluación del contexto actual de la organización respecto a la seguridad de información. Evaluando en base a catalizadores y procesos de COBIT 5.

4.4 Catalizadores de COBIT 5 y su relación con la Seguridad de Información

La importancia de los Catalizadores en COBIT 5 se da debido a que son factores cuya implementación repercute directamente en los resultados empresariales, si se administran y ejecutan de forma adecuada causarán una influencia importante en el trabajo de la organización. De la misma forma si se manejan técnicas de seguridad en su implementación esto generará una cultura de seguridad en toda la organización.

4.4.1 Principios, Políticas y Marcos de Referencia

Los principios, políticas y Marcos de Referencia son encargados de transmitir el comportamiento deseado a los miembros de la organización, por lo que son mecanismos de comunicación para transmitir direcciones e instrucciones dadas por los cuerpos de gobierno y administración.

Para un correcto manejo de este catalizador COBIT 5 resalta la necesidad de contar con un Framework de políticas. El mismo que debe definir los siguientes puntos:

- Quienes aprueban las políticas de la organización.
- Las consecuencias de fallar el cumplimiento de una política.
- Formas de manejar excepciones a las políticas.
- Medios por los que se revisará y medirá el cumplimiento de las políticas.

La responsabilidad de mantener y desarrollar este marco de políticas está a cargo del Presidente del Comité Directivo de Seguridad de la Información. Un modelo jerárquico en el que interactúan las políticas que deben conformar este marco es el siguiente, basado en el marco de políticas de COBIT 5.

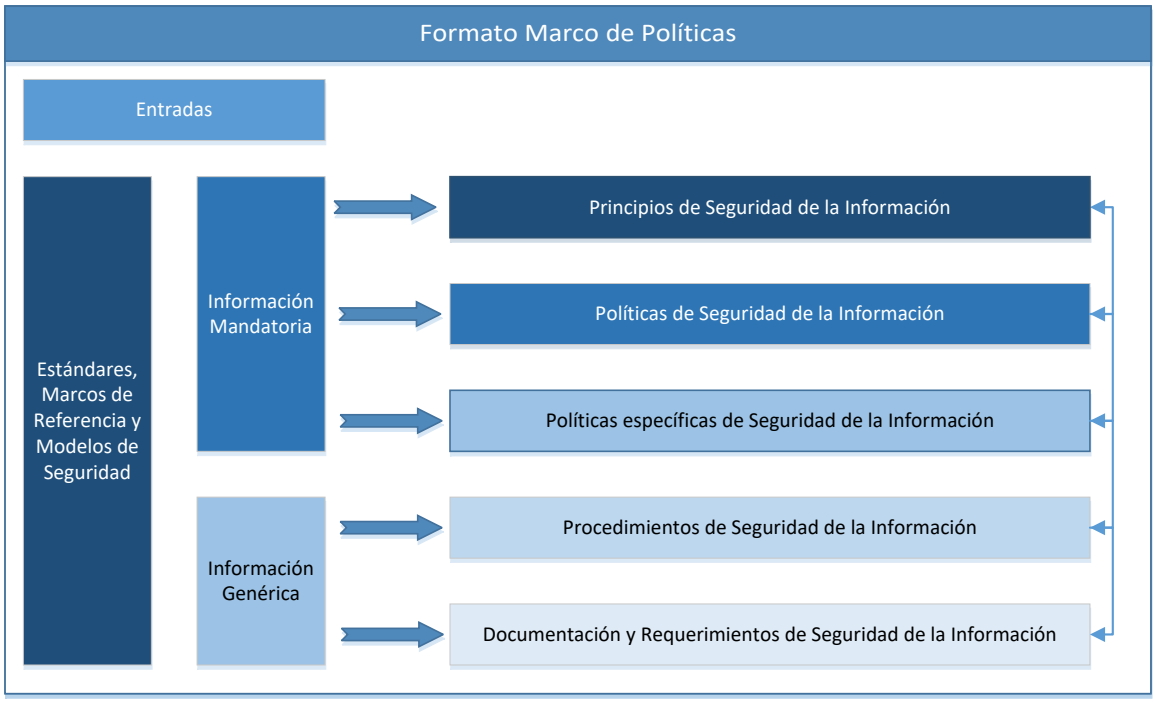

Ilustración 14: Marco de Políticas, basado en el Marco de Políticas de COBIT 5.

Con el manejo de este marco se puede generar una estructura avanzada y bien definida para enmarcar todas las políticas de Seguridad de la Organización, en la Guía Metodológica de Evaluación se encuentra información respecto a los principios que se sugiere emplear, así como políticas básicas con las que debe contar la organización para manejar un buen nivel de seguridad respecto a este catalizador.

En cuanto a las políticas de Seguridad de la Información se debe tomar en cuenta que son guías respecto a cómo poner en práctica los principios de seguridad de información de la organización.

Además, se debe tener en cuenta que las políticas de seguridad de Información deben estructurarse por 3 grupos diferentes de la organización.

- La Política de Seguridad de Información debe realizarla el Comité de Seguridad de Información y debe estar dirigido por las Partes Interesadas.
- Las Políticas específicas de Seguridad de información deben estar dirigidas por la Función (área) de Seguridad de Información
- Otras Políticas que se relacionan con la seguridad deben estar dirigidas por sus respectivas áreas.

Estas políticas se aplican para asegurar e influenciar el desarrollo y cumplimiento de los requisitos de seguridad.

Debido a que la Política de Seguridad de Información puede ir desde un documento descriptivo de una hoja hasta un manual detallado, la realización de la evaluación se fundamentó en analizar el alcance del documento, puesto que tomando en cuenta estos factores se puede determinar un nivel preliminar adecuado para este documento.

Por otra parte, la evaluación de las Políticas Específicas de Seguridad de Información, tanto las pertenecientes a la función de seguridad de Información como las pertenecientes a otras áreas de la organización, son evaluadas en base a características primarias que deben cumplir, además se mencionan las políticas básicas con las que debe contar toda organización que desee administrar una adecuada seguridad de información.

Las políticas específicas mencionadas en COBIT 5 y tratadas en la Guía de Evaluación son las siguientes, las primeras 4 a cargo de la función de Seguridad de Información y las demás pertenecientes a otras áreas de la organización:

- Política de Control de Acceso
- Política de Seguridad de Información del Personal
- Política Física y ambiental de Seguridad de Información
- Política de respuesta a Incidentes de Seguridad
- Política de Continuidad del Negocio y Recuperación de Desastres
- Política de Administración de Activos
- Política de Comportamiento
- Políticas de Mantenimiento, Desarrollo y Adquisición de sistemas de Información
- Política de Administración de Proveedores
- Política de Administración de Operaciones y Comunicación
- Política de Cumplimiento de Normas
- Política de Administración de Riesgos

Cabe recalcar que estas políticas son base y sugerencias por parte de COBIT 5 para contar con un nivel adecuado de Seguridad de la Información.

4.4.2 Procesos

Este catalizador se enfoca en la forma adecuada de gestionar los 37 procesos definidos en COBIT 5.

Los procesos se definen como un conjunto de actividades o prácticas direccionadas por las políticas empresariales que tienen entradas (varias fuentes) y salidas (productos y servicios).

Todos los procesos deben implementarse de forma que cumplan los siguientes metas:

- Intrínsecas: Es decir que cumpla con las reglas externas e internas, que sea un proceso de calidad y este alineado a buenas prácticas.
- Contextuales: el proceso debe adaptarse a la situación actual de la organización y ser relevante y fácil de implementar.
- Seguridad y Acceso: el proceso debe mantener confidencialidad y disponibilidad.

Es verdad que todo proceso de COBIT 5 debe gestionarse en entornos seguros, pero según el manual de “COBIT 5 Para seguridad de Información” existen 3 procesos que se relacionan de forma directa y son la base para una organización con cultura de seguridad de información.

- APO13: Gestionar la Seguridad
- DSS04: Gestionar la Continuidad
- DSS05: Gestionar servicios de Seguridad

Debido a que estos tres procesos son la base para una adecuada administración de la seguridad de información, son los procesos que se evalúan en la guía metodológica.

Información detallada (descripción, propósito, etc.) de estos procesos se encuentra en la guía metodológica que se encuentra anexada a esta disertación.

4.4.3 Estructuras Organizacionales

En este catalizador se describen posiciones que tienen alta relevancia en su interacción con seguridad de información, además de ser entes clave en toma de decisiones.

A continuación, se tiene una descripción del puesto y responsabilidad que debe cumplir aquel rol.

Posición	Responsabilidad
CISO (Director de seguridad de la Información)	Responsabilidad sobre todo el programa de seguridad de la información de la organización.
ISSC (Comité Director de Seguridad de Información)	Asegurar mediante monitoreo y revisión la aplicación efectiva de seguridad de información a lo largo de la organización.
ISM (Administrador de Seguridad de la Información)	Responsabilidad sobre toda la administración de seguridad.
ERM Committee (Comité de Gestión de Riesgos de Negocio)	Responsable de la toma de decisión respecto a activos, finanzas, riesgos y optimización para generar mayor valor de la empresa para las partes interesadas.
Dueños de Negocio / Custodios de Información	Enlace entre la función de seguridad de información y el negocio.

Tabla 8: Posiciones referentes a Seguridad de Información, Tomado de COBIT 5 Seguridad de Información.

Estos roles son fundamentales para que la organización cuente con un entorno enfocado en seguridad de información y serán las posiciones evaluadas en la guía metodológica.

Pero cabe recalcar que existen otros roles importantes que dependiendo de la realidad empresarial pueden estar o no implementados en la organización, es por esto que se muestra una matriz de ventajas y desventajas a continuación para abarcar un poco puestos de la organización que no se evaluaron en la guía metodológica. Estas posiciones son tomadas del manual de COBIT5 Seguridad de la Información.

Posición	Ventajas	Desventajas
Director Ejecutivo (CEO)	Riesgos de Información se elevan al nivel más alto de la organización.	Los riesgos deben ser presentados en contextos que sean entendibles para un CEO. Debido al nivel de responsabilidades del CEO puede ser posible que el nivel de abstracción en el análisis de riesgos sea muy alto.
Director de Información (CIO)	Problemas y soluciones de seguridad de información se pueden alinear a las iniciativas de IT	Pueden existir conflictos de interés. El rendimiento puede manejarse enfocado a TI y no enfocado a Seguridad de Información, es decir falta de enfoque.

Director Financiero (CFO)	Los problemas de seguridad de la Información pueden ser atendidos y entender su impacto desde un punto de vista financiero	Riesgos de información pueden fallar en ser atendidos por otras prioridades financieras. Puede darse conflictos de interés.
Director de Riesgos (CRO)	Riesgos de Información son elevados a una posición que puede observar también riesgos financieros, operacionales, estratégicos y cumplimiento de metas.	Es un rol ausente en la mayoría de empresas. En empresas en las que la posición es ausente se delegan las actividades al CEO o la mesa directiva.
Director de Tecnología (CTO)	Seguridad de la Información puede aliarse e incluirse con los mapas tecnológicos y futuras tecnologías.	Riesgos de información pueden fallar en ser atendidos por otras prioridades de iniciativas tecnológicas.
Director de Operaciones (COO)	Problemas y Soluciones de seguridad de Información pueden atenderse tomando en cuenta su impacto en operaciones del negocio.	Riesgos de información pueden fallar en ser atendidos por otras prioridades de iniciativas operacionales.
Consejo de Directores	Los riesgos de información son relevantes en los niveles altos de la organización.	Los riesgos de información deben ser presentados en un formato adecuado para los miembros de la mesa directiva.

Tabla 9: Desglose de Posiciones, Ventajas y Desventajas que pueden emplearse en una estructura organizativa con cultura de seguridad de Información, basado en COBIT 5 Seguridad de Información.

4.4.4 Cultura, Ética y Comportamiento

El aspecto de cultura es fundamental para un exitoso entorno de seguridad de información en cualquier organización, no solo debe ajustarse y darse a conocer el estado de la seguridad de información a miembros internos de la organización, sino que para lograr una cultura adecuada se debe informar incluso a personas externas (consultores, proveedores, etc.).

Otro aspecto importante es que las partes interesadas deben definir los comportamientos deseados e implementarlos para alinearlos con las normas y reglas de la organización. Para generar un entorno ético organizacional adecuándolo a la cultura de seguridad de información.

La Guía Metodológica se enfoca en evaluar una serie de comportamientos que deben darse en la organización para enfocarla a conseguir una cultura de seguridad de la información, pero en este capítulo se describen estos comportamientos para tener un mejor entendimiento, con el fin de facilitar su evaluación si no se conoce de forma adecuada que comprende cada comportamiento así, como facilitar la implementación de los mismos al contar con una descripción más extensa de ellos.

Comportamientos Deseados:

Para un mejor entendimiento de los comportamientos deseados en la organización, se realiza una descripción tomando en cuenta los siguientes aspectos: Ética organizacional e individual además de formas en las que el liderazgo puede afectar ese comportamiento.

Descripción de Comportamientos Deseados		
Comportamiento	**Categoría**	**Descripción**
La Seguridad de la Información es practicada diariamente en toda operación.	Explicación	La seguridad de información debe ser parte de las funciones diarias.
	Nivel Organizacional	El comportamiento indica que la seguridad de información es aceptada como parte del negocio de forma imperativa y como factor de metas organizacionales.
	Nivel Individual	Los individuos se preocupan acerca del bienestar de la organización y aplican técnicas de seguridad de información en todas sus operaciones.
Se Respeta la importancia de los Principios y Políticas de Seguridad de Información	Explicación	Se reconoce la importancia de los principios y políticas de seguridad de la información.
	Nivel Organizacional	Se promocionan los principios y políticas por parte de personal de administración, además de probar, revisar y comunicar políticas en lapsos regulares.
	Nivel Individual	Personal debe entender las políticas y sentir que lo fortalecen para seguir la guía de la organización
Se provee guías detallas respecto a Seguridad de la Información, además de motivarlas a participar y mejorar la	Explicación	Se brinda suficientes guías al personal respecto a Seguridad de Información y se los alienta a retar el nivel actual de seguridad de información tanto a nivel organizacional como individual.

situación actual de Seguridad de Información	Nivel Organizacional	Se tiene un proceso de comunicación de dos vías tanto para dar guía como para tener retroalimentación, brindando una oportunidad a las partes interesadas para generar cambios.
	Nivel Individual	La cultura individual permite cuestionar y comentar demostrando la participación de las partes interesadas
Las Partes Interesadas están alertas de cómo identificar y responder a las amenazas de la organización.	Nivel Organizacional	las partes interesadas toman acción en problemas que requieren responsabilidad y disciplina para confirmar su solución
	Nivel Individual	Se requiere que cada individuo entienda sus responsabilidades respecto a seguridad de información.
La Administración es proactiva para anticipar y apoyar con innovaciones y comunicar respecto a seguridad de la información. La empresa es receptiva por informes que reten la seguridad de información.	Explicación	Las innovaciones y desafíos respecto a la seguridad de información son tratados a nivel organizacional a través de equipos de investigación y desarrollo.
	Nivel Organizacional	
	Nivel Individual	La cultura individual contribuye brindando nuevas ideas a las partes interesadas.
La Administración del Negocio se involucra continuamente en colaboraciones multidisciplinarias para lograr programas de Seguridad de Información efectivos y eficientes.	Explicación	La colaboración multifuncionalidad apalanca a la empresa mediante una aceptación organizacional de contar con estrategias y mejoras integradas de la seguridad de información haciéndola un aspecto holístico al negocio.
	Nivel Organizacional	
	Nivel Individual	Los individuos contribuyen al dar a interactuar con toras funciones del negocio y generar nuevas sinergias.
Administración Ejecutiva reconoce el valor para el negocio de la Seguridad de Información.	Explicación	El valor de negocio de la seguridad de información es reconocido a nivel organizacional.
	Nivel Organizacional	La seguridad de información es vista como un medio para mejorar el valor del negocio, transparencia a respuestas de incidentes y entender las expectativas del cliente.

	Nivel Individual	el comportamiento se evidencia en la generación de ideas que mejoren el valor.

Tabla 10: Comportamientos Deseados, , basado en COBIT 5 Seguridad de Información

Hay que tomar en cuenta que para asegurar el cumplimiento de estos comportamientos COBIT 5 sugiere el uso de líderes o campeones (personas motivadas para explicar conceptos de seguridad a otros miembros de la organización). Para la creación de la cultura de seguridad de información.

Cuando se trata de liderazgo existen 3 niveles: Administración de Seguridad de Información, Administración de Unidades de Negocio y Administración Ejecutiva. Dentro de cada uno de estos niveles existen 3 aspectos que deben enfatizarse para facilitar el cumplimiento de los comportamientos:

- Influenciar el comportamiento a través de Comunicación, reglas y normas.
- Influenciar el comportamiento a través de incentivos y recompensas.
- Influenciar el comportamiento a través de concientización.

4.4.5 Información

Hay que resaltar que la información es el activo más importante y que se trata de asegurar a lo largo de este trabajo, pero de la misma manera según COBIT 5 es uno de los catalizadores de seguridad de información.

El catalizador se enfoca en manera en las que se puede administrar la información para emplearla en toma de decisiones. Existen varios documentos base alrededor de la gestión de información, pero después de analizar el análisis realizado en COBIT 5 se determinó que los principales empleados para la evaluación en la guía metodológica serán los siguientes:

- Estrategia de Seguridad de Información
- Presupuesto de Seguridad de Información
- Plan de Seguridad de Información
- Requerimientos de Seguridad de Información
- Material de Concientización
- Reportes de revisión de Seguridad de Información
- “Dashboard” de Seguridad de Información

A continuación, se describe cada uno de los tipos de documentos previamente señalados. Con el objetivo de aclarar cada uno de sus conceptos y dar a entender su importancia.

Estrategia de Seguridad de Información

Debe ser desarrollada por el CISO o ISM, con el propósito de proveer una dirección adecuada a la empresa respecto a Seguridad de Información. Esforzándose en ser un estado del arte y alinearse a principios generalmente aceptados, además de ajustarse al diseño y arquitectura empresarial generando una arquitectura de Seguridad de Información que se acople en todos los niveles a la organización, centrándose en proveer información solamente a quien tiene la necesidad de acceder a la misma.

Presupuesto de Seguridad de información

El presupuesto de información debe ser adecuado, preciso y realista. Se recomienda que la función de seguridad de información sea la encargada y tenga la opción de desarrollar el presupuesto, tomando como responsable al CISO o ISM. El propósito del presupuesto es proveer los fondos necesarios para el programa de seguridad de información y habilitar que la seguridad de información apoye al negocio teniendo en cuenta todas las inversiones necesarias para implementar la arquitectura y estrategia de seguridad de información.

Plan de Seguridad de Información

El plan de seguridad debe ser desarrollado por el CISO o ISM y contar con un seguimiento del ISSC. El plan debe basarse en la estrategia de seguridad de información y estar alineada con la arquitectura y situación actual de la seguridad de información de la organización.

Requerimientos de Seguridad de Información

Los requerimientos de Seguridad de Información deben ser realistas, precisos y estar alineados a regulaciones y necesidades del negocio, además deben estar disponibles en lapsos determinados para las partes interesadas.

Los requerimientos deben ser definidos en los siguientes puntos:

- Al inicio de proyectos del negocio, como parte de toma de requerimientos del negocio y funciones.
- Durante desarrollo de contratos y acuerdos con otras organizaciones
- En procesos de investigación por adquisiciones o uniones de organizaciones.

Material de Concientización

Este material debe contener declaraciones realistas y acertadas, tomando en cuenta prácticas y riesgos. Debe estar enfocado a cada función de forma que sea entendible y relevante para cada uno de los grupos que son objetivos de esta concientización.

El uso adecuado de este material genera que la gente cambie su comportamiento y se los motive a cumplir las políticas de seguridad de información, además se puede minimizar comportamientos riesgosos y no cumplimiento de actividades de seguridad de información.

Reportes de revisión de Seguridad de Información

Los reportes deben identificar las áreas de riesgo y enfocarse en reducir los gastos requeridos para recobrarse de incidentes y vulnerabilidades. Los análisis de amenazas deben identificar todas las amenazas de importancia para el negocio y se deben desarrollar respuestas a los riesgos. Además, el personal de IT y el CISO deben mantenerse informado de las últimas amenazas existentes relacionadas a seguridad de información.

"Dashboard" de Seguridad de Información

El "Dashboard" debe contener todos los eventos además de información adicional al estado de los requerimientos de seguridad de información, con un nivel adecuado de detalle. Los componentes del "Dashboard" deben renovarse en periodos definidos y regulares dependiendo del tipo de información y su grado crítico. Los reportes deben almacenarse de forma centralizada en el "Dashboard" para que sean disponibles a las partes interesadas.

Ciclo de Vida de Información

Todo tipo de información está asociado al siguiente ciclo de vida, la función de seguridad de información es la encargada de hacer seguimiento del ciclo de vida y asegurar su cumplimiento. A continuación, se tiene una descripción breve del ciclo de vida de la información:

Planificación, Diseño, Construcción o Adquisición:

La información es identificada, adquirida y se la clasifica. Esta fase hace énfasis en el desarrollo de estándares y definiciones, registros de creación y compra de datos.

Uso u Operación:

Esta fase contiene las siguientes fases:

- Almacenamiento: La información se mantiene electrónica o físicamente.
- Compartir: La información se hace disponible a través de medios de distribución, involucra procesos en los que se provee acceso y uso a la información a personal que lo necesite ya sea electrónica o físicamente.
- Uso: La información se utiliza para cumplir metas. Además, se tratan actividades de conversión de información de un medio a otro.

Monitoreo

En esta fase se asegura que los recursos de información se empleen de forma adecuada, se tienen actividades de actualización de información y verificación de información.

Desecho

En esta fase se descartan los recursos de información que ya no se utilizan.

Para entender de mejor manera el ciclo de vida se recomienda revisar en el manual de COBIT 5 el proceso BAI08: Procesos Catalizadores. Debido a que se alinea a las fases del ciclo de vida de la información.

4.4.6 Servicios, Infraestructura y Aplicaciones

Las prestaciones de servicios son necesarias para proveer seguridad de información y funciones relacionadas a la organización. Dentro de este trabajo se describen algunos servicios que son necesarios para guiar a una organización en el camino de seguridad de información:

- Proveer arquitectura de Seguridad
- Proveer concientización de Seguridad
- Proveer desarrollo Seguro
- Proveer evaluación de seguridad
- Proveer sistemas adecuadamente configurados y seguros, alineados con requerimientos y arquitectura de seguridad
- Proveer accesos a usuarios y derechos de acceso alineados con requerimientos del negocio
- Proveer protección adecuada contra malware, ataques externos e intentos de intrusión.
- Proveer adecuadas respuestas a incidentes
- Proveer pruebas de seguridad
- Proveer monitorización y servicios de alerta para eventos de seguridad.

4.4.7 Personas, Habilidades y Competencias

Este catalizador se relaciona muy estrechamente con el catalizador de cultura y comportamiento y el catalizador de estructura organizativa, puesto a que se toman en competencias que deben tener las personas para ocupar un puesto en la función de seguridad de información.

- Gobierno de Seguridad de Información
- Formulación de estrategia de seguridad de Información
- Administrador de Riesgos de Información
- Desarrollo de arquitectura de seguridad de información
- Operaciones de Seguridad de Información
- Evaluación, cumplimiento y pruebas de información

En la guía de evaluación se toman en cuenta factores de experiencia y habilidades para describir y facilitar a la organización a realizar un perfil de la persona adecuada para cada una de las posiciones necesarias en el área de seguridad de información.

5. Capítulo: Conclusiones

A lo largo del desarrollo de este trabajo de disertación se obtuvieron los siguientes resultados.

Como primer punto el desarrollo de la guía metodología de evaluación de seguridad del Cloud Computing que ofrecen los proveedores de este servicio, en la ciudad de Quito, como lo expresa el tema de disertación, no fue solo eso, al adentrarse en los conceptos y características que se involucran en la seguridad y fundamentalmente en la seguridad de información, aspecto que más interviene y se maneja en los manuales de COBIT 5, la Guía no se centra en seguridad de Cloud Computing solo aplicable al entorno de proveedores de Quito, incluso no se centra solo al modelo de negocio Cloud Computing. Para manejar la seguridad de una organización proveedora de Cloud Computing se deben gestionar los mismos aspectos que cualquier otra organización que desee ser segura. Los conceptos que intervienen en la seguridad de información son tres (Confidencialidad, Integridad y Disponibilidad) y deben estar presenten en toda organización que aspire a contar con una cultura de seguridad de información independientemente de sus objetivos comerciales. Por otra parte, al emplear como base COBIT 5 un marco de buenas prácticas que tiene un enfoque holístico e integral para ser acoplable a cualquier organización, intrínsecamente la guía de evaluación realizada para esta disertación cumple con estos principios.

Es por esto que como primera conclusión se tiene que la Guía Metodología de evaluación desarrollada en el proceso de disertación es aplicable a cualquier organización no solo a proveedores de Cloud Computing de la ciudad de Quito, esto se debe a que los conceptos de seguridad de información son los mismo independientemente del tipo de negocio o de la locación del mismo.

Como segundo punto los proveedores de Cloud Computing deben asegurarse de emplear tecnologías y metodologías que provean cifrado de la información tanto en la transmisión como en el almacenamiento de la misma, conexiones seguras, emplear múltiples factores de autenticación, buenas prácticas de codificación que aseguren la integridad y seguridad del software y acuerdos a nivel de servicio (SLA) que aseguren la gestión adecuada de la privacidad de la información de sus clientes.

Otro punto de gran importancia es que en la actualidad los incidentes de seguridad son causados principalmente por personas internas a la organización, empleados o exempleados, es por ello que las organizaciones deben tomar medidas que cambien la cultura empresarial y provean de una conciencia de seguridad a todo involucrado además

de realizar un seguimiento al personal de forma constante, contar con una estructura organizativa que cuente con personal responsable de la seguridad de información y matrices RACI para definir responsables de los procesos.

Finalmente, en el proceso de desarrollo de la Guía de Evaluación se determinó que para que una organización cuente con un nivel mínimo adecuado de seguridad de información debe desempeñar de forma adecuada todos los catalizadores de COBIT 5, y en cuanto a los procesos al menos debe contar con un buen desempeño en los siguientes: APO13: Administración de Seguridad, DSS04: Administración de Continuidad y DSS05: Administración de Servicios de Seguridad. Además, es importante y recomendable realizar un análisis del nivel de madurez de los procesos pues esto permitirá contar con una visión más elevada del estado actual de la organización y permitirá determinar los puntos por los que debe empezar el proceso de mejoramiento.

Tabla de Ilustraciones

Lista de Tablas

Bibliografía

Amazon Web Services, Inc. (2016). *Empiece a crear en AWS*. Recuperado el 05 de agosto de 2016, de amazon web services: https://aws.amazon.com/es/

Arora, V. (2010). *Comparing different information security standards: COBIT vs. ISO 27001.* Doha: Carnegie Mellon University, Qatar. Recuperado el 29 de Septiembre de 2016, de https://qatar.cmu.edu/media/assets/CPUCIS2010-1.pdf

Beal, V. (2016). *Cloud Computing (the cloud)*. Recuperado el 28 de 04 de 2016, de Webopedia: http://www.webopedia.com/TERM/C/cloud_computing.html

COBIT 5 Task Force (2009-2011). (2012). *COBIT 5 A business Framework for the Governance and Management of Enterprise IT.* Rolling Meadows, Illinois, USA: ISACA. Recuperado el 16 de Agosto de 2016

Destefani Neto, M. (18 de Marzo de 2014). *A brief history of cloud computing*. Recuperado el 26 de Julio de 2016, de Thoughts On Cloud: http://www.thoughtsoncloud.com/2014/03/a-brief-history-of-cloud-computing/

Google. (2016). *Google App Engine Documentation*. Recuperado el 05 de Agosto de 2016, de Google Cloud Platform: https://cloud.google.com/appengine/docs

Gorelik, E. (2013). *Cloud Computing Models: Comparison of Cloud Computing Service and Deployment Models .* Massachusetts Institute of Technology , Sloan School of Management, Room E62-422 . Cambridge: Massachusetts Institute of Technology . Recuperado el 05 de Agosto de 2016, de http://web.mit.edu/smadnick/www/wp/2013-01.pdf

Hewlett Packard Enterprise Development LP. (2016). *HPE Helion Eucalyptus, Open source hybrid cloud software for AWS users*. Recuperado el 26 de Julio de 2016, de Hewlett Packard Enterprise: http://www8.hp.com/us/en/cloud/helion-eucalyptus-overview.html

IBM, Staff Writer. (05 de Abril de 2015). *Cloud through the ages: 1950s to present day*. Recuperado el 26 de Julio de 2016, de Thoughts On Cloud: http://www.thoughtsoncloud.com/2015/04/a-brief-history-of-cloud-1950-to-present-day/

ISACA. (2012). *COBIT 5 for Information Security.* Rolling Meadows, Illinois, Estados Unidos: ISACA. Recuperado el 20 de 12 de 2016

ISACA. (2012). *COBIT 5 for Information Security Preview Version.* Recuperado el 05 de Septiembre de 2016, de ISACA: http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf

ISACA. (s.f.). *Essential characteristics of Cloud Computing.* Recuperado el 03 de Agosto de 2016, de ISACA: http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/Essential%20characteristics%20of%20Cloud%20Computing.pdf

ISO. (15 de Febrero de 2016). *ISO/IEC 27000:2016*, 4. Recuperado el 29 de Agosto de 2016, de ISO: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=66435

Krebs, R., Momm, c., & Kounev, S. (2012). *Architectural Concerns in Multi-Tenant SaaS Applications.* Universität Würzburg, Infromatik. Walldorf: Conference on Cloud Computing and Services Science. SciTePress. Recuperado el 03 de Agosto de 2016, de https://se2.informatik.uni-wuerzburg.de/pa/uploads/papers/paper-371.pdf

Legal Information Institute (LII) Cornell university Law School. (22 de Septiembre de 2016). *44 U.S. Code § 3542 - Definitions*. Recuperado el 22 de Septiembre de 2016, de https://www.law.cornell.edu/uscode/text/44/3542?qt-us_code_temp_noupdates=0#qt-us_code_temp_noupdates

Linthicum, D. (2009). *Cloud Computing and SOA Convergence in your Enterprise* (Primera ed.). Boston, MA, USA: Pearson Education, Inc. Recuperado el 09 de agosto de 2016, de http://dl.jaytee.in/Ebooks/info_retrieval/%5BDavid_S._Linthicum%5D_Cloud_Computing_and_SOA_Conve(BookFi.org)_4.pdf

NIST. (2011). *The NIST Definition of Cloud Computing.* Gaithersburg: Computer Security Division.

opensource.com. (s.f.). *What is open source?* Recuperado el 26 de Julio de 2016, de opensource.com Discover an open source world.

PwC Argentina. (2016). *Resultados de la Encuesta Global de Seguridad de la Información.* PwC Argentina.

pwc, PrincewaterhouseCoopers LLP. (2016). *Turnaround and transformation in cybersecurity Key findings from The Global State of Information Security Survey 2016.* pwc. pwc. Recuperado el 27 de Septiembre de 2016, de http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html

Real Academia Española. (18 de Septiembre de 2016). *Seguridad*. Recuperado el 22 de Septiembre de 2016, de Diccionario de la Real Academia Española: http://dle.rae.es/?id=XTrIaQd

Rouse, M. (Mayo de 2009). *Public Cloud*. Recuperado el 09 de Agosto de 2016, de SearchCloudComputing: http://searchcloudcomputing.techtarget.com/definition/public-cloud

Rouse, M. (Enero de 2015). *Infrastructure as a Service (IaaS)*. (Techtarget) Recuperado el 05 de Agosto de 2016, de SearchCloudComputing: http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS

Rouse, M. (Marzo de 2015). *private cloud (internal cloud or corporate cloud)*. Recuperado el 09 de Agosto de 2016, de SearchCloudComputing: http://searchcloudcomputing.techtarget.com/definition/private-cloud

Schouten, E. (31 de Enero de 2014). *Cloud computing defined: Characteristics & service levels*. (IBM, Editor) Recuperado el 03 de Agosto de 2016, de Thoughts On Cloud: http://www.thoughtsoncloud.com/2014/01/cloud-computing-defined-characteristics-service-levels/

Sirianni, A. (2016). *Dcode Group Pty LTD*. Recuperado el 21 de Septiembre de 2016, de The importance of Data and Information in Business: https://www.dcode.com.au/blog/the-importance-of-data-and-information-in-business

Srinivasan, S. (2014). Cloud Computing Evolution. En S. i. Engineering, *Cloud Computing Basics* (págs. 1-16). New York, New York, USA: Springer New York. doi:10.1007/978-1-4614-7699-3_1

Stanfod university. (2013). *Folding@home*. Obtenido de What if Even while you Sleep you could help find a cure?: http://folding.stanford.edu/

Tello Meryk, J. (2014). *CONFERENCIA LATINOAMERICANA CACS/ISRM 2014, 234-Mapeando Fortalezas de COBIT 5 Seguridad con ISO/IEC 27001:2013.* ISACA, Latam Consulting Services. ISACA. Recuperado el 29 de Septiembre de 2016

The openStack Project. (2016). *Open source software for creating private and public clouds*. Recuperado el 26 de Julio de 2016, de openstack: https://www.openstack.org/

University of California, Barkeley. (13 de Julio de 2016). *boinc*. Recuperado el 09 de Agosto de 2016, de Open-source software for volunteer computing: https://boinc.berkeley.edu/index.php

WebFinance. (2016). *Business Dictionary*. Recuperado el 21 de Septiembre de 2016, de Information: http://www.businessdictionary.com/definition/information.html#ixzz2KdTVazNt

Wikipedia. (09 de Julio de 2016). *Streaming*. Recuperado el 26 de Julio de 2016, de Wikipedia, La enciclopedia Libre: https://es.wikipedia.org/wiki/Streaming

6. Anexos

GUÍA METODOLÓGICA PARA EVALUACION DE SEGURIDAD DE PROVEEDORES DEL SERVICIO DE CLOUD COMPUTING

Descripción breve

Esta guía forma parte del trabajo de disertación previa obtención del título de Ingeniero de Sistemas y Computación, en la Pontificia Universidad Católica del Ecuador. Basado en las buenas prácticas descritas en COBIT 5 Seguridad de la Información

Johnny Arias
2016

Resumen Ejecutivo

Esta guía de evaluación toma en cuenta las buenas prácticas y conceptos presentados en el marco de referencia de COBIT 5, “COBIT 5 for Information Security”. Se los emplea como base para encontrar métricas y generar matrices de evaluación preliminares para facilitar la valoración del nivel de implementación de los catalizadores[43] y principales procesos involucrados en llevar a la organización a cumplir un nivel aceptable de seguridad de información.

Introducción

Autoría

Este documento fue desarrollado por Johnny Arias como parte del trabajo de disertación: “Desarrollo de una guía metodológica empleando COBIT 5, para evaluar la seguridad del Cloud Computing que ofrecen los proveedores de este servicio, en la ciudad de Quito”, requisito previo a la obtención del título de ingeniero de sistemas y computación, trabajo realizado en la Pontificia Universidad Católica del Ecuador, contando con el apoyo y revisión por parte del Ingeniero Alberto Pazmiño, Director de la Disertación.

Esta guía se enfocará en evaluar la seguridad de la organización tomando en cuenta los catalizadores tratados en COBIT 5 Seguridad de la Información y los siguientes procesos: APO13 Administración de la Seguridad, DSS04: Administración de la continuidad, DSS05 Administración de servicios de Seguridad.

Cabe recalcar que para un cumplimiento total y manejo de seguridad de información a través de la organización se debe aplicar medidas de seguridad a todos los procesos, pero de forma inicial los procesos más relacionados, según COBIT 5, a mantener seguridad de información son los anteriormente mencionados.

Propósito y Alcance

El propósito de este documento es proveer guías de evaluación tanto para organizaciones que brinden servicio de “Cloud Computing” así como entidades que vayan a contratar servicios bajo este modelo de negocio, aunque al basarse en las buenas

[43] Catalizadores (enabler) hacen referencia a cualquier cosa que facilita y soporta el cumplimiento de las metas empresariales. En COBIT 5 se manejan 7 catalizadores.

prácticas de COBIT 5 puede aplicarse a cualquier organización, enfocándose en determinar el nivel de seguridad de su servicio, de acuerdo a las buenas prácticas de los catalizadores y principales procesos relacionados con seguridad presentes en COBIT 5.

Esta guía cuenta con recomendaciones de diseño e implementación de medidas de seguridad que pueden aplicarse en las organizaciones, para una mejor aplicación de técnicas de seguridad de Información, basándose en las buenas prácticas de COBIT 5, otros marcos y estándares empleados en la actualidad.

La intensión de esta guía en ser una guía de apoyo inicial que evalúa los elementos principales relacionados a la seguridad de información de la organización.

Audiencia

Esta guía tiene como objetivo ser empleada por personal de seguridad, administradores de sistemas, administradores de redes y personal técnico de organizaciones relacionadas con servicio de “Cloud Computing” que de preferencia tengan conocimientos de COBIT 5.

Además, al ser parte de un trabajo de disertación otro propósito intrínseco de esta guía es servir como una base de aprendizaje para estudiantes de ingeniería en sistemas que estén interesados en desarrollar servicios “Cloud Computing” o sean usuarios de los mismos, con el objetivo general de que empleen este documento para analizar la seguridad del servicio y así determinar si las condiciones de seguridad son las apropiadas.

Estructura del Documento.

El resto de este documento está organizado de la siguiente manera.

- La primera sección se enfoca en la evaluación de los catalizadores de COBIT 5.
- La segunda sección se enfoca en la evaluación de los principales procesos relacionados con seguridad, el cumplimiento de estos procesos presenta un sistema preliminar de seguridad de la información.

Dentro de cada una de las secciones se encuentran matrices de evaluación y varias recomendaciones y sugerencias en la priorización de implementación de aspectos de cada catalizador, en casos que la organización no cumpla los requisitos mínimos para contar con un nivel adecuado de seguridad de información, además una explicación del análisis y desarrollo de esta guía de evaluación esta descrito en el capítulo 4 de la disertación.

Sección I: Evaluación de Catalizadores

En esta sección se brindarán técnicas de evaluación del nivel del cumplimiento de los catalizadores de COBIT 5, este aspecto permite contar con una apreciación inicial del nivel general de seguridad de Información con el que cuenta la organización. Además, que se darán recomendaciones para contar con un nivel de seguridad inicial aceptable.

Catalizador 1. Principios, Políticas y Marcos de Referencia

Dentro de este catalizador se tratarán dos puntos de evaluación los principios y las políticas. La evaluación de ambos se da tomando en cuenta las guías dadas en el apéndice A[44] del manual COBIT 5 Seguridad de la Información.

Principios de Seguridad de Información

Lo primero que se debe tomar en cuenta es que los principios de seguridad de información son empleados para comunicar todas las reglas a lo largo de la organización y deben alinearse a los objetivos de gobierno y valor empresariales. Están definidos por la junta directiva y ejecutiva.

Los 12 principios que se evaluarán fueron formulados por ISACA, ISF[45] y (ISC)2®[46] con el objetivo de soportar el negocio, defenderlo y promover un comportamiento responsable respecto a la Seguridad de la Información.

Estos principios de Seguridad de información están divididos de la siguiente manera.

- 6 pertenecen a la tarea de Soportar el Negocio.
- 4 Pertenecen a la tarea de Defender el Negocio.
- 2 Pertenecen a la Tarea de Promover un comportamiento responsable respecto a Seguridad de la Información

Para esta evaluación se empleará una matriz, basada en la descrita en COBIT 5, esta matriz cuenta con información referente a que tarea pertenece el principio, el objetivo que debe cumplir este principio, una descripción del principio, esta descripción proveerá información base para en caso de no contar con dicho principio tener ideas base que

[44] (ISACA, 2012, pág. 61)
[45] Information Security Forum (ISF)
[46] International Information System Security Certificaion Consortium (ISC)[2]

ayuden a implementarlo en la organización y por último se tiene la celda de evaluación cuyo objetivo es ser un identificar de cumplimiento.

Principios de seguridad de la Información			
Principio	Objetivo	Descripción	Evaluación
1. Soporte del negocio			
Enfocarse en el negocio	Asegurar que la seguridad de la información está integrada en las actividades esenciales del negocio.	Individuos dentro de la comunidad de seguridad de información deberían formar relaciones con líderes del negocio y mostrar como la seguridad de la información complementa procesos claves del negocio y administración de riesgos.	
Brindar calidad y valor a las partes interesadas	Asegurar que la seguridad de Información entregue valor y cumpla los requerimientos de negocio	Las partes interesadas internas y externas deben comprometerse con una comunicación regular para que los cambios de requerimientos respecto a seguridad de la información se continúen cumpliendo. Promover el valor de la seguridad de información ayuda a ganar apoyo en toma de decisiones, que pueden emplearse para apoyar el éxito de la visión por seguridad de la información	
Cumplir con requerimientos regulatorios y leyes relevantes	Asegurar el cumplimiento de obligaciones	El cumplimiento de obligaciones debe ser identificado, traducido a requerimientos específicos de seguridad de información y comunicación. Además de contar con controles actualizados, monitoreados y analizados a medida que se actualizan los requerimientos legales y regulaciones. Se debe tener claro las penalidades por el no cumplimiento.	
Proveer información oportuna y precisa respecto al rendimiento de la seguridad de Información	Apoyar requerimientos del negocio y administración de riesgos de información	La información debe ser capturada de forma periódica, consistente y de manera rigurosa para mantener su integridad de forma que sea relevante para el cumplimiento de los objetivos de las partes interesadas. Los requerimientos de información deben ser claramente definidos y cumplir con indicadores de seguridad de información.	

Evaluar amenazas de información actuales y futuras	Analizar y evaluar amenazas emergentes de seguridad de información para tomar acciones oportunas, informadas y mitigar riesgos.	Las tendencias y amenazas de seguridad de información deben ser categorizadas de forma integral manteniendo un Framework standard. Los individuos deben actuar proactivamente compartiendo y entendiendo las amenazas y sus causas.	
Promover mejoramientos continuos respecto a seguridad de la información	Reducir costos, mejorar eficiencia y efectividad, promover una cultura de mejoramiento continuo respecto a seguridad de información	Conocimiento de las últimas técnicas de seguridad de información debe mantenerse aprendiendo de incidentes y coordinando con organizaciones de investigación independientes. Las técnicas de seguridad de información deben adaptarse de acuerdo a los cambios de modelos organizacionales.	
2. Defender el Negocio			
Adoptar un enfoque basado en riesgos	Asegurar que los riesgos son tratados de manera constante y efectiva	El manejo de riesgos debe involucrar las siguientes actividades: Aceptar el riesgo, evitar el riesgo, transferir el riesgo y mitigarlo. Para hacer esto de forma adecuada se debe contar con información revisada y decisiones documentadas.	
Proteger información clasificada	Prevenir la divulgación de información confidencial o clasificada a personas no autorizadas.	Toda información debe ser identificada y clasificada acorde a su nivel de confidencialidad, para una protección acorde a dicho nivel y manteniendo su ciclo de vida.	
Concentrarse en aplicaciones críticas del negocio	Priorizar la protección de información de aplicaciones de negocio en las cuales un incidente podría causar el mayor impacto.	El entender el impacto de la falta de disponibilidad o pérdida de integridad de la información causada por aplicaciones de negocio permite entender el nivel de información crítica. A partir de esto se puede enfocar los requerimientos de seguridad de información priorizando información crítica para el negocio.	
Desarrollar sistemas seguros	Construir sistemas de calidad y rentables en los que la gente pueda confiar.	La seguridad de la información debe integrarse al alcance, diseño, construcción y pruebas dentro del sistema de desarrollo y su ciclo de vida. Se deben emplear buenas prácticas de seguridad de información durante todos los niveles de desarrollo.	
3. Promover un comportamiento responsable respecto a Seguridad de la Información			

Actuar de forma profesional y ética	Asegurar que las actividades relacionadas con seguridad de la Información tengan un desempeño confiable, responsable y efectivo.	La seguridad de la Información depende altamente en la habilidad de los profesionales de la organización en realizar sus roles responsablemente y que entiendan como su integridad tiene un impacto directo en protección de la información. Los profesionales de seguridad de información deben comprometerse con cumplir estándares de calidad, demostrar consistencia y comportamientos éticos respetando las necesidades del negocio.	
Fomentar una cultura de Seguridad de Información Positiva	Proveer un comportamiento positivo a los usuarios finales respecto a la seguridad de Información, reducir la posibilidad de que ocurran incidentes de seguridad y limitar su impacto en el negocio.	Se debe enfatizar que la seguridad de la información es un factor clave para el negocio y de esta forma generar toma de conciencia en los usuarios, además hay que asegurar que se cuente con las habilidades necesarias para proteger información crítica o confidencial. Todos los individuos deben conocer los riesgos de la información que manejan para saber cómo protegerla.	

Tabla 11: Matriz de evaluación de Principios de Seguridad de Información, Catalizador 1.

Para la evaluación de principios sugiero realizar dos evaluaciones. Una apreciación general de principios para tener una idea base del estado actual y una evaluación de principios por tareas en la que se enfocará específicamente cada principio acorde a su agrupación.

Apreciación General de Principios

Esta evaluación es un buen punto de inicio para contar con una idea preliminar del nivel de cumplimiento de la organización respecto al manejo de principios de seguridad.

Evaluación general del Cumplimiento de Principios	
# de Principios Guías	12
# de Principios Implementados	
% de Cumplimiento General	(# de principios Implementados) *100 / (# de Principios Guías)

Tabla 12: Apreciación general de Principios de Seguridad de Información

Este indicador de Cumplimiento General no es específico, es general, es por ello que para contar con un indicador representativo que demuestre un nivel aceptable de cumplimiento se debe contar con al menos 75% de cumplimiento, es decir mínimo 9 de los principios deben estar implementados.

Para explicar por qué este indicador puede no ser representativo y fallar en precisar el nivel de real de cumplimiento de los principios, hay que analizar que los 12 principios se dividen en tres (Soporte del Negocio, Defensa del Negocio y Promover un Comportamiento responsable respecto a Seguridad de la Información). Al ser este el caso se podría tener porcentajes de cumplimiento del 50% al 65% que pudiera dar una impresión ligeramente positiva de correcto funcionamiento respecto al manejo de principios de seguridad. Que de cierta forma es acertado, pero falla en claridad y certeza porque en estos casos puede ser que la organización solo cumpla con principios relacionados con una o dos de las tareas, olvidando totalmente al resto de principios.

Es por esto que la siguiente forma de evaluación de manejo de principios es la que se recomienda emplear.

Evaluación de Principios por Tareas.

La primera y más específica involucra una evaluación de cumplimiento de principios dentro de su respectiva tarea, de la siguiente forma:

Primera Tarea: Soporte del Negocio

Tarea	Soporte del negocio
# de Principios asociados	6
# de Principios Implementados	Número de Principios con los que actualmente cuenta la organización
% de Cumplimiento	(# de principios Implementados) *100 / (# de Principios Asociados)

Tabla 13: Evaluación Principios Relacionados Con Soporte de Negocio

Si el porcentaje es al menos del 66%, es decir se cumplen mínimo 4 de los 6 principios se considera un estado aceptable de la implementación actual de estos principios.

Si el valor es menor al 66% la organización debe delegar al Comité Directivo de Seguridad de la Información para énfasis la necesidad de implementar los principios que soporten el negocio.

Segunda Tarea: Defender el Negocio

Tarea	Defender el negocio
# de Principios asociados	4
# de Principios Implementados	Número de Principios con los que actualmente cuenta la organización
% de Cumplimiento	(# de principios Implementados) *100 / (# de Principios Asociados)

Tabla 14: Evaluación Principios Relacionados Con Defender el Negocio

Esta tarea cuenta con principios más allegados al aspecto de seguridad, es por ello que para lograr un nivel aceptable de seguridad se debe tener un porcentaje de cumplimiento mínimo del 75%, es decir al menos 3 de los 4 principios deben estar implementados de forma adecuada.

Hay que recalcar que, si la Organización no maneja principios de seguridad de información, debe priorizar la implementación de los principios pertenecientes a esta tarea debido a que son los más cercanos a conceptos de Seguridad de Información, además que serán una buena base para llevar a cabo el resto de principios.

Tercera Tarea: Promover un comportamiento responsable respecto a Seguridad de la Información

Tarea	Promover un Comportamiento responsable respecto a Seguridad de la Información
# de Principios asociados	2
# de Principios Implementados	Número de Principios con los que actualmente cuenta la organización
% de Cumplimiento	(# de principios Implementados) *100 / (# de Principios Asociados)

Tabla 15: Evaluación Principios Relacionados Promover un comportamiento responsable respecto a Seguridad de la Información

Los principios de esta tarea se enfocan principalmente en las personas del a organización, en su cultura, comportamiento y ética. El cumplimiento de estos principios es fundamental para que la organización cuente con una cultura de Seguridad de la Información consistente y duradera.

Para contar con una gestión buena y debido a que son principios directamente relacionados con la cultura de seguridad organizacional, la organización debe cumplir con ambos principios (100% en esta métrica), esta exigencia se debe a que las estadísticas[47] de seguridad se muestra que la principal fuente de incidentes de seguridad de información son empleados de las empresas.

Si dentro de esta tarea el porcentaje de cumplimiento es del 50%, es decir, se cumple al menos 1 de los principios el nivel de seguridad, la organización es regular y debe enfocarse en completar el desarrollo del otro indicador para contar con una dirección adecuada en gestión de seguridad de información y generación de cultura de seguridad empresarial.

Algo que se debe aclara es que si no se cuenta con alguna implementación de principios en las tareas anteriores (Soporte del negocio y Defensa del Negocio) lo más seguro es que no se tenga una implementación adecuada de este principio, o al menos el monitoreo de estos principios va a ser totalmente dependiente de políticas u otros catalizadores, que no serán exactos, ya que la organización carece totalmente de principios de seguridad. De ser este el caso la principal tarea de los directivos de la organización es enfocar al Comité Directivo de Seguridad de la Información en implementar principios de soporte y defensa de la organización, en la etapa inicial no es necesario ni recomendable lanzarse a completar los principios faltantes, la sugerencia es priorizar la implementación de estos principios acorde a la realidad empresarial y tomar como base el porcentaje de cumplimiento, dado en esta evaluación, como indicador preliminar a cumplir.

Política de Seguridad de la Información

La política se seguridad de Información es fundamental puesto que mediante este documento se materializan las practicas que deben emplearse para lograr el cumplimiento e implementación de los principios de seguridad de la información. Debido a que el documento de política de seguridad varía de acuerdo a la realidad empresarial una forma de evaluación más factible es la de realizar una evaluación del alcance con el que cuenta el documento como tal, para ello se empleará la siguiente matriz.

[47] Encuesta del estado de seguridad de Información provista por PwC, “The Global State of Information Security Survey 2016 The Global State of Information Security Survey 2016”

Alcance de la Política de Seguridad de Información		
Cualidades	Descripción	Cumplimiento
Definición de Seguridad de la Información empresarial	Determinar y delimitar los aspectos fundamentales de la seguridad de la Información de la empresa	
Responsabilidades Asociadas a las Seguridad de Información	Definir las responsabilidades que sean aplicables al cumplimiento de las políticas de Seguridad de Información	
La Visión respecto a Seguridad de Información	Una explicación de cómo la visión apoya a la seguridad de Información, la cultura y toma de conciencia. Incluyendo métricas e indicadores apropiados.	
Alineación con otras políticas	Explicación de maneras en las que la política de Seguridad de Información se alinea con otras políticas empresariales	
Elaboración de temas específicos de Seguridad de Información	Se recomienda tratar temas como administración de información, evaluación de riesgos de información, obligaciones contractuales, aspectos regulatorios y legales.	
Ciclo de vida de Seguridad de Información	Este aspecto debe abarcar administración de costos y presupuestos respecto a la administración de seguridad de la información además de planes estratégicos de seguridad de la información.	

Tabla 16: Evaluación del Alcance de la Política de Seguridad de Información

El objetivo de aplicar esta matriz es entender el nivel de cumplimiento del documento de política de Seguridad de Información, los temas tratados son temas iniciales y fundamentales para lograr una política preliminar, este documento debe progresar a medida que lo hacen las mejores prácticas.

Para contar con un adecuado alcance de la política de Seguridad se espera al menos el cumplimiento de 5 de los 6 puntos previamente mencionados.

Todos los temas tratados deben comunicarse a todos los miembros de la organización, además que se deben definir responsables de la Política de Seguridad de Información, validación y actualización, la recomendación es que un CISO[48] sea el encargado de estas funciones.

[48] Chief Information Security Officer, es decir: Oficial de Seguridad de la Información o Director de seguridad de la Información (CISO)

Políticas Específicas de Seguridad de Información

Este aspecto se refiere a ejemplos de políticas de seguridad de información específicas de la función de Seguridad de Información como tal. Las políticas que se evaluarán a continuación se manejan como políticas principales que deben contar en la organización, a partir de una adecuada implementación de estas se puede extender a otras políticas secundarias de esta función.

Las políticas específicas pertenecientes a la función de Seguridad de la Información que se evaluarán son las siguientes:

- Política de Control de Acceso
- Política de Personal de Seguridad de Información
- Política de Seguridad Física y Ambiental de la Información
- Política de Respuesta a Incidentes de Seguridad

Política de Control de Acceso

Política de Control de Acceso	
Temas Enmarcados	Cumplimiento
Segregación de funciones[49]	
Menos privilegios/ necesidades de Saber	
Accesos de emergencia	
Accesos físicos y lógicos provisionados con el ciclo de vida	

Tabla 17: Evaluación de Política de Control de Acceso

Para ratificar el cumplimiento de los temas anteriormente señalados dentro de la Política de Control de Acceso se puede emplear la siguiente lista de métricas:

- Número de violaciones de acceso que exceden la cantidad permitida
- Cantidad de trabajo interrumpido por la insuficiencia de permisos de acceso.
- Número de incidentes de segregación de funciones[50]
- Hallazgos de auditorías.
- Número de peticiones de accesos de emergencia.
- Número de cuentas de emergencia activas que exceden los tiempos límite.

[49] La segregación de funciones hace referencia a la separación de responsabilidades de actividades que intervienen en un proceso, es decir incluir autorizaciones o controles a dichas actividades del proceso.
[50] Los incidentes hacen referencia a actividades que no se completaron por la segregación de funciones o actividades que carecen de control de responsabilidades.

Para cumplir con una política adecuada al menos se debería contar con un documento que contenga la forma de medir los indicadores previamente descritos.

Política de Personal de Seguridad de la Información

Política de Personal de Seguridad de Información	
Temas Enmarcados	Cumplimiento
Ejecutar verificaciones de antecedentes a todo empleado y personal en posiciones clave.	
Adquisición de información respecto a personal clave en posiciones de Seguridad de Información	
Desarrollar un plan de seguimiento para el personal de seguridad	
Verificar que el personal de seguridad de información cuente con las habilidades necesarias y certificaciones relacionadas.	

Tabla 18: E Política de Personal de Seguridad de Información

Para verificar el cumplimiento de estos temas dentro de la política de personal de seguridad de información, se sugieren los siguientes indicadores:

- Número de verificaciones de antecedentes de personal completados.
- Número de revisiones de antecedentes vencidas, basadas en una frecuencia de revisión definida.
- Número de personal de seguridad de información que no ha rotado acorde a la frecuencia previamente definida.
- Listado de personal clave del área de Seguridad de Información que cuenta con personal de respaldo.
- Número de personal que cuenta con las habilidades necesarias y es calificado.

El contar con la implementación de esta política es fundamental debido a que indica prácticas e indicadores para controlar y manejar un personal de seguridad de información de manera adecuada.

Política física y Ambiental de Seguridad de Información

Política Física y ambiental de Seguridad de Información	
Temas Enmarcados	Cumplimiento
Aseguramiento Físico de Lugares	
Controles Ambientales que apoyen las operaciones.	
Selección de instalaciones	
Estándares de Control Ambiental	
Estándares de control físico de Acceso	
Monitoreo de Seguridad de información y detección de intrusiones físicas	

Tabla 19: Evaluación de Política Física y Ambiental de Seguridad de Información

Para asegurar el cumplimiento de estos aspectos que deben estar enmarcados en la política, se recomienda tomar en cuenta el cumplimiento de los siguientes indicadores.

- Número de incidentes o vulnerabilidades identificadas referentes a amenazas de locaciones físicas.
- Número de incidentes o vulnerabilidades atribuidas a sistemas de control ambientales.
- Tendencias en costos de aseguramiento referente a pérdidas ocasionadas por amenazas ambientales, criminales o físicas.

Política de Respuesta a incidentes de Seguridad.

Política de Respuesta a Incidentes de Seguridad	
Temas Enmarcados	Cumplimiento
Definición de Incidente de Seguridad de información	
Declaración de cómo manejar los incidentes de Información	
Requerimientos para conformación de un equipo de respuesta de incidentes.	
requerimientos para la creación de un plan de pruebas de incidentes.	
Documentación de Incidentes y cerrado de los mismos.	

Para comprobar la adecuada implementación de estas políticas el contar con indicadores similares a los siguientes puede facilitar la evaluación e implementación de la política y la organización como tal.

- Número de incidentes manejados durante el tiempo definido.
- Tiempo promedio de respuesta del equipo para solucionar un incidente crítico.
- Número de procedimientos y guías empleadas en la resolución de incidentes que han sido incluido al plan de pruebas de incidentes.
- Porcentaje de incidentes no resueltos a tiempo.

Además de esto se debe aclarar ciertos aspectos que debe tener el Plan de Respuesta a Incidentes que se formulará dentro de la Política.

- Importancia e Impacto del Incidente.
- Procesos de reporte y escalamiento
- Recuperación
    - RTO's (Objetivo de Tiempo de Respuesta) para regresar al estado de confianza.
    - Procesos de Investigación y prevención.
    - Entrenamiento y Pruebas.
- Reuniones Post-Incidentes.

Es fundamental emplear el Plan de Respuesta a Incidentes puesto a que será el documento en el cual se evidenciará toda vulnerabilidad o incidencia resuelta facilitando mejorar la respuesta y brindando nuevas prácticas para prevenir y solucionar futuras fallas. Esta Política debe incluir a toda la función de seguridad y ser notificada a todos los empleados de la organización.

Políticas Específicas de Seguridad de Información Pertenecientes a otras áreas de la Organización

Para complementar y generar un sistema de políticas que cubra a toda la organización permitiendo extender la cultura de seguridad de información a otras áreas del negocio, para ello se describen en la siguiente matriz varias políticas con sus respectivos alcances que deben tomarse en cuenta.

Políticas específicas de Seguridad de Información de áreas ajenas a Seguridad de Información		
Política	Alcance	Evaluación
Políticas de Continuidad de Negocio y Recuperación de Desastres	Análisis de Impacto del Negocio (BIA)	
	Planes de contingencia y recuperación del negocio	
	Requerimientos de Recuperación para Sistemas Críticos	
	Definir umbrales y factores desencadenantes para contingencia y escalado de incidentes.	
	Plan de Recuperación de Desastres (DRP)	
	Entrenamiento y Pruebas	
Política de Administración de Activos	Clasificación de Datos	
	Propiedad de Datos e Información	
	Sistemas de Clasificación y Propiedad	
	Priorización y Utilización de Activos	
	Administración del Ciclo de Vida de Activos	
	Medidas de Protección de Activos	
Políticas de Comportamiento	Comportamiento y Uso aceptable durante el trabajo: Expectativa de privacidad, Internet, Email, Uso de Activos y Sistemas Empresariales, Accesos Remotos, Mensajería, Uso de Computadoras y Dispositivos para Actividades Empresariales.	
	Comportamiento y Uso aceptable fuera del trabajo: Blogs y Redes Sociales	
Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	Proceso de Ciclo de vida de Seguridad de la Información	
	Proceso de definición de requerimientos de Seguridad de Información	
	Seguridad de Información dentro del proceso de adquisición y contratación	
	Prácticas de Codificación Seguras	
	Integración de Seguridad de Información con administración de Cambios y Configuraciones	

Política de Administración de Proveedores	Administración de contratos: Términos y Condiciones de Seguridad de Información, Evaluación de Seguridad de Información y Monitorear el Cumplimiento de Seguridad de Información de Contratos	
Política de Administración de Operación y Comunicación	Seguridad de Información de IT en la Arquitectura y Diseño de Aplicaciones: (Comité Directivo, estándares y líneas guías)	
	SLA: (operaciones Internas y Externas)	
	Procedimientos operacionales de IT para Seguridad de Información	
Política de Cumplimiento	Procesos de Evaluación de cumplimiento de Seguridad de Información de IT	
	Métricas de desarrollo	
	Repositorios de evaluación: Audiencia, contenido, estructura y seguimiento	
Política de Administración de Riesgos	Plan de Administración de Riegos Organizacional: Alcance, roles y responsabilidades, metodologías, herramientas y técnicas y procesos de repositorio.	
	Perfiles de Riesgos de Información	

Tabla 20: Evaluación de Políticas Específicas de Seguridad de Información de áreas ajenas a Seguridad de Información.

Para realizar una evaluación adecuada se analizará el específico de cada una de las políticas señaladas en la matriz anterior.

Políticas de Continuidad de Negocio y Recuperación de Desastres

Políticas de Continuidad de Negocio y Recuperación de Desastres	
# de Aspectos Guías	6
# de Aspectos Implementados	
% de Cumplimiento	(# de Aspectos Implementados) *100 / (# de Aspectos Guías)

Tabla 21: Evaluación de Políticas de Continuidad de Negocio y recuperación de Desastres.

Para contar con un manejo adecuado de esta política se sugiere al menos cumplir un 66% de los aspectos, es decir 4 de los 6 temas dentro del alcance. Un aspecto fundamental debe ser el cumplimiento del plan de Recuperación de Desastres y el análisis de Impacto del Negocio.

Política de Administración de Activos

Política de Administración de Activos	
# de Aspectos Guías	6
# de Aspectos Implementados	
% de Cumplimiento	(# de Aspectos Implementados) *100 / (# de Aspectos Guías)

Tabla 22: Evaluación de Política de Administración de Recursos

Para asegura un nivel adecuado de cumplimiento de esta política se recomienda al menos tener 4 de los 6 indicadores dentro del documento de políticas, priorizando los sistemas de clasificación y propiedad de datos.

Políticas de Comportamiento

Políticas de Comportamiento	
# de Aspectos Guías	2
# de Aspectos Implementados	
% de Cumplimiento	(# de Aspectos Implementados) *100 / (# de Aspectos Guías)

Tabla 23: Evaluación de Políticas de Comportamiento.

El cumplimiento debe ser del 50%, es decir cumplir al menos un aspecto de los mencionados en el alcance, al contar con este indicador se asegura que él personal maneje de forma adecuada los activos y administren de forma efectiva sus permisos tanto fuera y dentro de la organización, además de contribuir con ajustar el comportamiento del personal para mantener una cultura de seguridad de información adecuada.

Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	
# de Aspectos Guías	5
# de Aspectos Implementados	
% de Cumplimiento	(# de Aspectos Implementados) *100 / (# de Aspectos Guías)

Tabla 24: Evaluación de Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

Para contar con una política adecuada se debe tener al menos el cumplimiento de 3 de los 5 aspectos del alcance, al menos de 60%, priorizando prácticas de codificación seguras y la aplicación de Seguridad de Información en los procesos de adquisición y contratación.

Política de Administración de Proveedores

Política de Administración de Proveedores	
# de Aspectos Guías	1
# de Aspectos Implementados	
% de Cumplimiento	(# de Aspectos Implementados) *100 / (# de Aspectos Guías)

Tabla 25: Evaluación de Política de Administración de Proveedores

Se debe cumplir totalmente el alcance de esta política puesto que es fundamental para la interacción con los proveedores y administrar la información que se comparte con los mismos.

Política de Administración de Operación y Comunicación

Política de Administración de Operación y Comunicación	
# de Aspectos Guías	3
# de Aspectos Implementados	
% de Cumplimiento	(# de Aspectos Implementados) *100 / (# de Aspectos Guías)

Tabla 26: Evaluación de Administración de Operación y Comunicación

El cumplimiento se debe ajustar al menos a 2 de los 3 aspectos del alcance, tomando como parte fundamental el lograr incorporar SLA (acuerdos a nivel de Servicio) puesto que debe contar con una adecuada definición de niveles de operación tanto internos como externos.

Política de Cumplimiento

Política de Cumplimiento	
# de Aspectos Guías	3
# de Aspectos Implementados	
% de Cumplimiento	(# de Aspectos Implementados) *100 / (# de Aspectos Guías)

Tabla 27: Evaluación de Política de Cumplimiento

Para asegurar un adecuado nivel respecto al manejo de esta política se deben cumplir al menos 2 de los 3 aspectos del alcance, como sugerencia lo primordial establecer los procesos de evaluación de cumplimiento de seguridad de Información de IT.

Política de Administración de Riesgos

Política de Administración de Riesgos	
# de Aspectos Guías	2
# de Aspectos Implementados	
% de Cumplimiento	(# de Aspectos Implementados) *100 / (# de Aspectos Guías)

Tabla 28: Evaluación de Política de riesgos

Para conseguir un análisis y evaluación adecuada se debe cumplir al menos 50%, es decir uno de los dos aspectos de alcance, como sugerencia se determinó que se priorice el plan de administración de Riesgos Organizacional.

Catalizador 2. Procesos

La evaluación de este catalizador se maneja de forma distinta debido a que el alcance engloba la implementación adecuada de los procesos de la organización, se debe tener en cuenta que en todo proceso de la organización hay que considerar el factor "Seguridad de Información". Pero según COBIT 5 existen 3 procesos fundamentales por lo que se debe empezar para crear un entorno seguro. Los procesos son los siguientes:

- APO13: Administración de Seguridad
- DSS04: Administración de Continuidad
- DSS05: Administración de Servicios de Seguridad

Como punto de inicio la organización debe definir de forma adecuada estos procesos para contar con un nivel mínimo adecuado de manejo de Seguridad de Información, de no tener estos procesos deben ser implementados de forma inmediata como prioridades.

La evaluación de estos procesos se encuentra en la Sección 2 de esta guía metodológica.

Catalizador 3. Estructuras Organizacionales

Para la evaluación adecuada de este catalizador, se debe tener claro que según COBIT 5 el contar con las siguientes posiciones facilita de gran manera el manejo e interacción con Seguridad de Información. Los puestos son los siguientes:

- Director de Seguridad de Información (CISO)
- Comité Director de Seguridad de Información (ISSC)

- Administrador de Seguridad de la Información (ISM)
- Comité de Gestión de Riesgos de Negocio (ERM Committee)
- Custodios de Información / Dueños del Negocio

Para realizar una evaluación adecuada se empleará una serie de matrices que faciliten evaluar las características, habilidades o composición de cada uno de los roles descritos previamente. Además, se cuenta con un modelo RACI que permite determinar cómo intervienen los distintos puestos en ciertos procesos que se relacionan con seguridad de Información.

Director de Seguridad de Información (CISO)

En primer lugar, la organización debe contar con un CISO, es un requisito fundamental para enfocar a la empresa a una cultura enmarcada en los principios de Seguridad de Información. El CISO es responsable del programa de seguridad de información empresarial.

Para la evaluación se delimitarán áreas de trabajo y características que debe cumplir el CISO, esto con el fin de dar una guía de las responsabilidades que tiene y en base al cumplimiento de las mismas evaluar si se está enfocando adecuadamente esta posición o se deben realizar ajustes de responsabilidades.

Evaluación de CISO		
Área	Características y Responsabilidades	Evaluación
Principios Operativos	Vincula al programa de Seguridad con Administración Ejecutiva	
	Comunica y Coordina las necesidades de protección de la información a las Partes Interesadas	
	Entiende de forma precisa la visión estratégica de la organización	
	Comunicador efectivo	
	Experto en construir relaciones efectivas con líderes del negocio	
	Traslada los objetivos del negocio en Requerimientos de Seguridad	
Alcance del Control	Establecer y Mantener el Sistema de Administración de Seguridad de Información	
	Definir y Administrar el plan de tratamiento a riesgos de Seguridad de Información	
	Revisar y Monitorear el Sistema de Administración de Seguridad de Información	
Nivel de Autoridad	Responsable de Implementar y Mantener la Estrategia de Seguridad de Información	

Tabla 29: Evaluación de Responsabilidades del CISO.

Para contar con un CISO que maneje de forma adecuada su posición se sugiere que al menos se cumplan de forma inicial 8 de los 10 puntos señalados anteriormente, es primordial que administre y desarrolle el plan y estrategia de seguridad de información, si estos aspectos no se cumplen la organización no cuenta con un CISO, puesto a que son las tareas esenciales de esta posición.

Comité Director de Seguridad de Información (ISSC)

Este Comité tiene como objetivo asegurar el uso de buenas prácticas en la aplicación de seguridad de información en la organización de forma efectiva y consistente.

Para la evaluación se emplean dos aspectos, el primero se fundamenta en la composición del Comité con una breve descripción de los mismos para facilitar el entendimiento de su importancia en el mismo.

Evaluación de la Composición de ISSC		
Rol	Descripción	Evaluación
CISO (Director de Seguridad de Información)	Presidente del Comité	
	Vinculación entre el comité y ERM	
	Responsable general sobre la seguridad de información Empresarial	
ISM (Administrador de Seguridad de Información)	Comunicación de prácticas de diseño, monitoreo y diseño	
Dueños del Negocio/ Custodios de Información	A cargo de ciertos procesos y aplicaciones de negocio	
	Responsable de comunicar las iniciativas de negocio que pueden impactar a la Seguridad de la Información y prácticas que puedan impactar a la comunidad	
	Entender riesgos de negocio y operaciones, costos y beneficios y requerimientos de Seguridad de Información.	
Administrador de TI	Reportar el estado de iniciativas de seguridad de información relacionadas con TI	
representantes de Funciones de Especialización	Incluir especialista en la mesa cuando su punto de vista sea necesario.	

Tabla 30: Evaluación de la Composición de ISSC

La organización debe contar con este Comité y asegurar que distintas personas cumplan los requisitos para los distintos roles, asegurando que cumplan los requisitos y cuenten con habilidades necesarias para tener una visión completa.

Además de esto un análisis respecto a las características y responsabilidades que debe cumplir el comité son buenos aspectos para evaluar si el nivel de implantación y manejo del mismo es el adecuado dentro de la organización.

Evaluación de Responsabilidades y Características del ISSC		
Área	Características y Responsabilidades	Evaluación
Principios Operativos	Deben reunirse de forma regular, pueden planificarse reuniones extra a causa de iniciativas o incidentes de urgencia.	
	Substituciones son permitidas, pero deben mantenerse limitadas.	
	El comité está limitado a un pequeño grupo de personas, para asegurar la toma de decisiones y comunicaciones.	
	El presidente del comité es el CISO	
Alcance de Control	El comité es responsable de tomar las decisiones respecto a seguridad de la información empresarial	
Nivel de Autoridad	Responsables de que las decisiones de seguridad de la empresa apoyen las decisiones estratégicas de ERM (Administrador de Riesgos de la Empresa)	

Tabla 31: Evaluación de Responsabilidades y Características del ISSC

Lo fundamental es que el Comité cuente con miembros con la necesaria autoridad pues su principal responsabilidad es aprobar toda medida relacionada con seguridad de información, además de intercalar estas decisiones con los objetivos del negocio.

Administrador de Seguridad de Información

Este cargo es de mucha importancia debido a que se encarga de administrar todo esfuerzo de seguridad de la información, emplea las estrategias y planes de seguridad de información para desarrollar, diseñar e implementar prácticas y reportes de seguridad de información.

Para entender mejor este rol se emplea la siguiente matriz de evaluación, enfocada en las características y responsabilidades del mismo.

Evaluación de ISM		
Área	Características y Responsabilidades	Evaluación
Principios Operativos	Reportes al CISO o incluso a líderes del negocio	
Alcance de Control	Administración de incidentes y amenazas	
	Administración de Accesos	
	Administración de Riesgos y programas de concientización	
	Aplicaciones e Infraestructura de Seguridad de Información	
Nivel de Autoridad	Autoridad de toma de decisiones respecto a prácticas de propiedad de seguridad de información	

Tabla 32: Evaluación de Características y Responsabilidades de ISM.

Se recomienda cumplir con todos los puntos de Nivel de Autoridad y Principios Operativos, además de enfocarse en controlar al menos 3 de las 4 responsabilidades resaltadas en el alcance de control, de forma preliminar.

Comité de Gestión de Riesgos de Negocio

El Comité ERM se responsabiliza de la toma de decisiones respecto a valoración, control, optimización, finanzas y monitoreo de todo riesgo con el propósito de incrementar el valor del negocio.

La evaluación del Comité se fundamentará en la composición del mismo, tomando en cuenta una descripción de cada rol para un mejor entendimiento en su importancia en el comité. A continuación, se muestra la matriz de evaluación.

Evaluación de Composición del Comité ERM		
Rol	Descripción	Evaluación
CISO	Para una composición óptima el CISO debe pertenece al comité, para brindar asesoramiento en temas específicos.	
CEO, COO, CFO, etc.	Representantes de administradores ejecutivos	
Dueños de procesos claves del negocio	Encargado de procesos y aplicaciones del negocio	
	Responsable de comunicar iniciativas y prácticas de negocio que impacten la seguridad de información	
	Puede contar con conocimientos y entendimiento de riesgos de negocio y operación y requerimientos específicos de seguridad de información de áreas específicas del negocio.	

Auditor	Proveer puntos de vista de especialistas cuando sea relevante.	
	Pueden ser miembros permanentes u ocasionales.	
Representativos Legales	Provee punto de vista legal, puede ser miembro ocasional o permanente.	
CRO	Brindar información especializada y relevante. Puede ser miembro ocasional o permanente.	

Tabla 33: Evaluación de la composición del Comité ERM.

Como punto inicial se recomienda al menos contar con los roles de CISO, Representantes Senior (CEO, COO, CFO, etc.) y Dueños de procesos Claves del Negocio. Estos roles deben cumplirse para contar con un Comité ERM, a medida que mejore el manejo de cultura de Seguridad de Información se puede incrementar los miembros del comité, además se recomienda contar con especialistas (legales, auditores y CRO) dependiendo el tipo de incidentes que se presenten y de ser necesario contar con puntos de vista en áreas específicas. Cumpliendo estos aspectos se tiene un comité adecuado para controlar riesgos y administrar un nivel aceptable de seguridad de Información.

Custodios de Información/Dueños del Negocio

La evaluación de esta posición es distinta debido a que debe ser una persona designada por las partes interesadas y de alta confianza, para la evaluación se presenta una matriz de responsabilidades y características que debe tener la persona que cumpla este rol.

Evaluación de Custodios de Información/Dueño el Negocio	
Responsabilidades	Evaluación
Actuar como un enlace entre la función de Seguridad de Información y el Negocio.	
Debe contar con un buen entendimiento del negocio, tipos de información procesada y requerimientos de información.	
Sirve como asesor de confianza dentro del negocio.	
Ser un agente de monitoreo de la información del negocio.	
Equilibrar riesgos del negocio e información.	

Tabla 34: Evaluación de Responsabilidades del Custodio de la Información/Dueño del Negocio

Se recomienda al menos cumplir, preliminarmente, 4 de los 5 aspectos señalados para contar con un custodio de información que realice sus actividades

de forma adecuada, siempre recalcando que debe ser una persona de alta confianza y comprometimiento con la organización.

Catalizador 3. Cultura, Ética y Comportamiento

Para lograr contar con una cultura organizativa enfocada en seguridad de información y valores éticos se deben definir comportamientos adecuados que encaminen al personal hacia el cumplimiento de estas metas, en este catalizador se evalúa los comportamientos primordiales con los que debe contar la organización para contar con una cultura de seguridad de información adecuada.

Comportamientos Deseados

La evaluación de comportamiento se centra en determinar el cumplimiento de 8 comportamientos básicos que guiarán a la organización a tener un mejor manejo de seguridad de información.

Evaluación de Comportamiento	
Comportamiento	Cumplimiento
La Seguridad de la Información es practicada diariamente en toda operación.	
Se Respeta la importancia de los Principios y Políticas de Seguridad de Información	
Se provee guías detallas respecto a seguridad de la Información, además de motivarlas a participar y mejorar la situación actual de Seguridad de Información	
Las partes interesadas están alertas de cómo identificar y responder a las amenazas de la organización.	
La Administración es proactiva para anticipar y apoyar con innovaciones y comunicar respecto a seguridad de la información. La empresa es receptiva por informes que reten la seguridad de información.	
La Administración del Negocio se involucra continuamente en colaboraciones multidisciplinarias para lograr programas de Seguridad de Información efectivos y eficientes.	
Administración Ejecutiva reconoce el valor para el negocio de la Seguridad de Información.	

Tabla 35: Evaluación de comportamiento organizacional.

Al menos se debe cumplir 6 de los 8 comportamientos esenciales para tener un adecuado nivel de cultura organizacional direccionada a la seguridad de información. Priorizando el cumplimiento del comportamiento 1: “La Seguridad de la Información es practicada diariamente en toda operación” puesto que es la base para cambiar la actitud

de los involucrados con la organización y enfocarse en mejorar la cultura del a organización.

Para contar con información adicional y descripciones de los comportamientos se recomienda revisar la disertación adjunta con esta guía metodológica o el manual COBIT 5 Seguridad de Información en el que se basa esta guía.

Cultura de Seguridad de Información

El uso adecuado de los comportamientos debe generar cambios en la forma de actuar del personal (cultura organizacional) y la forma de verificar el nivel de seguridad en actividades operacionales diarias de la organización (Cultura de Seguridad de Información), para esto se cuenta con una matriz guía con métricas que corroborar el cumplimiento de los comportamientos deseados y su adecuada implementación en el entorno empresarial.

Métricas	Cumplimiento
Fortaleza de contraseñas	
Tarjetas de Acceso	
Número de candados de laptops distribuidos a empleados	
Número de candados de laptops usados por empleados	
Discusiones públicas respecto a información confidencial	
Falta de acercamientos a seguridad (compartir contraseñas, seguimientos, etc.)	
Prácticas de protección de contraseñas	
Porcentaje de información identificada y clasificada.	
Responsables de visitantes y registros de visitantes	
Adherencia a las prácticas de gestión del cambio de sistemas y aplicaciones.	

Tabla 36: Ejemplos de métricas de cumplimiento de cultura de Seguridad de Información

Hay que recalcar que son ejemplos de métricas que se pueden emplear, lo fundamental es tomar en cuenta métricas para determinar la seguridad de contraseñas, así como confidencialidad de información como primeros pasos.

Catalizador 5. Información

Para la evaluación de este catalizador se tomará en cuenta los tipos de documentos alrededor de la gestión de información, que se enmarcan en COBIT 5 seguridad de la información:

- Estrategia de Seguridad de Información
- Presupuesto de Seguridad de Información
- Plan de Seguridad de Información
- Requerimientos de Seguridad de Información
- Material de Concientización
- Reportes de revisión de Seguridad de Información
- “Dashboard” de Seguridad de Información

Una organización enfocada a Seguridad de Información debe al menos contar con los tipos de documentos relacionados con la gestión de información señalados anteriormente, si no es este el caso debe priorizarse su implementación.

A continuación, se presenta una evaluación a cada tipo de documento presentado, que facilita el identificar aspectos que carezcan en la organización o ratifica la implementación adecuada del mismo.

Todas las evaluaciones toman en cuenta dos temas fundamentales tratado en el manual de COBIT 5, que son las metas y las buenas prácticas que debe tener cada uno de estos tipos de información.

Estrategia de Seguridad de Información

Evaluación de Metas

La estrategia de Seguridad de Información debe contar con métricas o indicadores que permitan hacer un seguimiento del cumplimiento del mismo. Estas metas se alinean a la realidad del negocio y al estado del arte de Seguridad de Información, por lo que entablar una evaluación puede ser algo dificultoso. Es por ello que se tomará en cuenta indicadores guías enmarcados en COBIT 5 para realizar esta evaluación y formar una base para que la organización forme sus propios indicadores alineados a su realidad.

Métricas	Cumplimiento
Porcentaje de actividades de Seguridad de Información que se guían en un marco de referencia	
Porcentaje de actividades de Seguridad de Información que fueron comparadas con el rendimiento de sus pares.	

Número de incompatibilidad entre la Estrategia y Arquitectura de Seguridad de Información con la Arquitectura del Negocio	
Porcentaje de Las Partes interesadas que no tiene acceso a la Estrategia de Seguridad de Información	
Número de violaciones de Seguridad de información	

Tabla 37: Evaluación de Metas de la Estrategia de Seguridad de Información.

Estos son ejemplos que se alinean a las características básicas que debe tener una estrategia de Seguridad de Información.

Evaluación de Buenas Prácticas

El documento de Estrategia de Seguridad de información debe cumplir al menos los siguientes aspectos. Para ser adecuado para guiar a la organización a una cultura de Seguridad de Información.

Buenas Prácticas	Cumplimiento
Se toma en cuenta las restricciones (legales, regulatorias, etc.) durante el desarrollo de la estrategia de Seguridad de Información	
Alineamiento de las actividades de Seguridad de Información con los objetivos de la organización	
Administración de Riesgos de Información (definición, vista estratégica, etc.)	
Principios generales y acercamiento hacia la administración y gobierno.	
Arquitectura de Seguridad de Información.	
Grados de Cumplimiento	
Operaciones de Seguridad de Información	
Mapa de Seguridad de Información (estados deseados)	

Tabla 38: Evaluación de Buenas Prácticas dentro de la Estrategia de Seguridad de Información.

Como punto inicial al menos se debe cumplir 6 de los 8 aspectos señalados en la matriz, lo ideal es tomar en cuenta todos para que encaminen a la organización y sean una guía para las partes interesadas del rumbo que tomará la organización respecto a seguridad de información.

Presupuesto de Seguridad de Información.

Evaluación de Metas

Para la evaluación de metas se muestran métricas básicas que funcionan como guía para determinar el cumplimiento y la implementación adecuada del presupuesto, tomando como enfoque el adecuado seguimiento de metas del presupuesto de seguridad de información.

Métricas	Cumplimiento
Número de peticiones adicionales de presupuesto después del año presupuestado (para medir la evolución del presupuesto)	
Número de discrepancias entre el presupuesto de Seguridad de Información con las necesidades en general	
Diferencia entre el presupuesto y los costos reales	
Porcentaje de partes interesadas sin acceso al presupuesto de seguridad de información	

Tabla 39: Evaluación de Métricas del Presupuesto de Seguridad de Información

Evaluación de Buenas Prácticas

En esta subsección se describe los contenidos que debe tener el presupuesto de seguridad de Información para su evaluación.

Buenas Prácticas	Cumplimiento
Presupuesto para la operación de la función de seguridad de información	
Presupuesto para el programa de seguridad de información	

Tabla 40: Evaluación de Buenas Prácticas de Presupuesto de Seguridad de Información

La organización debe cumplir con ambos aspectos para tener un adecuado presupuesto, Para explicar más de mejor manera se extenderá en contenidos que pueden abarcarse dentro del presupuesto. Se debe tomar en cuenta los siguientes temas:

- Costos de personal, de infraestructura, de proyectos
- Inversiones iniciales para la función de seguridad de información
- Costos recurrentes de operación
- Costos de respuesta a incidentes
- Costos de programas de concientización de seguridad
- Certificaciones de seguridad organizacionales

- Costos de auditorías externas

Es fundamental hacer un seguimiento regular del presupuesto y cumplimiento del mismo, para cumplir los requerimientos de seguridad de la mejor manera, el presupuesto de seguridad se recomienda que el presupuesto se planifique para implementaciones anuales.

Plan de Seguridad de Información

Evaluación de Metas

En esta evaluación se listan métricas que deben cumplirse al contar con un plan de seguridad de información implementado de forma adecuada.

Metas	Cumplimiento
Número de acciones que no pudieron ser implementadas	
Número de incompatibilidades entre el plan de seguridad de información y la arquitectura de seguridad de información	
Porcentaje de partes interesadas que no tiene acceso al plan de seguridad de información	
Número de violaciones cometidas al plan	

Tabla 41: Evaluación de metas del Plan de Seguridad.

Si el plan de seguridad cumple al menos estos indicadores se puede decir que está encaminado en el rumbo adecuado, se recomienda que se implementen otros indicadores de acuerdo a la realidad empresarial.

Evaluación de Buenas Prácticas

El plan de Seguridad de Información debe contener los siguientes temas para cumplir normas básicas que permitan a la organización tener un adecuado funcionamiento de seguridad de información.

Buenas Prácticas	Cumplimiento
Procesos que necesiten ser definidos, implementados o fortalecidos	
Estructuras organizacionales que necesiten ser instanciadas o fortalecidas.	
Flujos de información relacionados con administración de seguridad de información que deben ser implementados	
Políticas y procedimientos que deben definirse y ponerse en práctica	

Cultura de Seguridad de Información que debe ajustarse y mantenerse	
Comportamientos y habilidades que necesitan construirse y cambiarse	
Capacidades (Competencias) que necesitan adquirirse	

Tabla 42: Evaluación de Buenas Prácticas del Plan de Seguridad de Información.

Para un adecuado nivel de seguridad, o nivel inicial, se recomienda que el plan de seguridad de información sea al menos de 5 de los 7 temas.

Requerimientos de Seguridad de Información

Evaluación de Metas

Las métricas descritas en esta sección facilitan el determinar si los requerimientos de seguridad de información cumplen los aspectos básicos, a partir de los indicadores que se presentan se recomienda ampliar a más de los indicadores acorde la realidad empresarial.

Metas	Cumplimiento
Número de requerimientos incumplidos	
Número de proyectos que contienen requerimientos de seguridad de información que fueron revisados por personal de seguridad de información	
Número de proyectos que se entregaron a la organización	
Número de proyectos que fallaron en su entrega.	
Número de firmas aceptando la recepción y conocimiento hacia los requerimientos de seguridad de información.	

Tabla 43: Evaluación de Metas de requerimientos de Seguridad de Información.

Evaluación de Buenas Prácticas

Todo requerimiento de información debe contar con los siguientes temas que serán evaluados en la matriz.

Buenas Prácticas	Cumplimiento
Los requerimientos definen al responsable y usuario final	
Debe definirse el impacto en el negocio	
Definirse los criterios de Disponibilidad	
Definirse criterios de Integridad	
Definirse criterios de Confidencialidad	

Tabla 44: Evaluación de Buenas Prácticas de Requerimientos de Información.

Todos los temas señalados deben cumplirse al momento de generar requerimientos de seguridad de información, es fundamental tener claro los criterios de Disponibilidad, Integridad y Confidencialidad pues son primordiales para que la información cumpla características de seguridad.

Material de Concientización

Evaluación de Metas

La siguiente matriz cuenta con una serie de indicadores que son base para determinar la adecuada implementación de un modelo inicial de material de concientización.

Metas	Cumplimiento
Número de actualizaciones al material de concientización de seguridad de información	
Porcentaje de empleados que pasaron pruebas.	
Porcentaje de empleados que incorporan metas de seguridad de información a sus planes de desempeño	
Número de participantes que proveen respuestas a preguntas	

Tabla 45: Evaluación de Metas de Material de Concientización.

Se recomienda incorporar más indicadores que se ajusten a la realidad actual de la organización, además de emplear las métricas de ejemplo que dan a conocer el uso de pruebas para asegurar que el personal comprende y asimila el material de concientización.

Evaluación de Buenas Prácticas

Los siguientes temas asegurar que el material de concientización cuente con temas esenciales para direccionar al personal de la organización a entender la importancia de la seguridad de información, así como el estado actual de la misma.

Buenas Prácticas	Cumplimiento
El diseño y la implementación del programa de concientización debe contar con el apoyo del personal ejecutivo.	
Debe contener mandatos[51] de información: Políticas de Seguridad de Información, Políticas de uso aceptable y objetivos de seguridad de información que impulsen al negocio	

[51] Criterios y restricciones de orden

El Programa debe direccionar la cultura de seguridad de información a basarla en las metas empresariales.	
El material de concientización debe desarrollarse tomando en cuenta la audiencia al a que va dirigida.	
La organización debe implementar y definir procesos repetibles de concientización para ayudar a las partes interesadas a cumplir requerimientos del negocio diariamente.	
Los administradores son responsables de asegurar la participación de empleados en programas de concientización	
La información del material de concientización debe basarse en procedimientos entregados por parte de los expertos de Seguridad de Información	
El CISO o ISM es el responsable de la ejecución del programa de concientización	
Se debe tomar en cuenta la tecnología por la que se impartirá el material de concientización	
El material debe estar disponible por múltiples canales	
Este material se emplea como base para los perfiles de riesgo, programas de administración y diseño de seguridad de información	
El programa de concientización debe ser monitorizado y contar con reportes para su seguimiento.	

Tabla 46: Evaluación de Buenas Prácticas para el Material de Concientización.

Es de suma importación que el material sea desarrollado por expertos puesto que es distribuido a toda la Organización para darles a conocer las medidas y procedimientos de seguridad de información que se implementan, además que es el paso inicial para los perfiles de riesgo. La Organización para contar con un material de concientización de nivel inicial adecuado al menos debe cumplir 9 de los 12 indicadores señalados anteriormente, teniendo en cuenta que el material debe ser siempre desarrollado por expertos.

Reportes de revisión de Seguridad de Información

Evaluación de Tipos de Reportes

A continuación, se presenta una matriz que permite evaluar los tipos de reportes que la organización debe manejar para estar enfocada a una cultura de seguridad de información, además que gracias a ello se facilita el seguimiento de incidentes o amenazas de seguridad de información.

Tipos de Reportes	Cumplimiento
Hallazgos de auditorías de Seguridad de Información	
Reportes de madurez de Seguridad de Información	
Análisis de amenazas de riesgos de seguridad de información	
reportes de evaluación de vulnerabilidades	
Análisis de Impacto del Negocio	

Tabla 47: Evaluación de Tipos de reportes necesarios para adecuada Seguridad de Información.

Como base la organización debe contar con reportes de análisis de impacto del negocio (BIA), de amenazas y vulnerabilidades. Estos son la esencia para encaminar la revisión de reportes hacia una cultura de seguridad de información, además que a partir de ellos se puede contar con análisis de madurez de seguridad de información y determinar causas de las amenazas y soluciones o actualizaciones a vulnerabilidades.

Evaluación de Metas

La revisión de reportes debe tener como metas los siguientes puntos (como mínimo).

Metas	Cumplimiento
Número de amenazas identificadas	
Número de amenazas encontradas al año	
Porcentaje de amenazas solucionadas empleando prácticas de seguridad de información	
Porcentaje de actualizaciones realizadas según calendario	
Número de violaciones de seguridad de información identificadas	
Número de vulnerabilidades encontradas en el año	

Tabla 48: Evaluación de Metas de Reportes de Seguridad de Información.

Como sugerencia la organización debe al menos cumplir con la generación de reportes que tomen en cuenta temas de vulnerabilidades, auditorias, análisis de amenazas

de información y de Impacto del negocio, para contar con un nivel inicial de seguridad de información aceptable que sea la base para mejorar el manejo de reportes en la organización.

Dashboard[52] de Seguridad de Información

Evaluación de Metas

Para que la organización tenga el uso adecuado del “Dashboard” es recomendable tomar en cuenta estas metas.

Metas	Cumplimiento
Número de Problemas de precisión dados en el "Dashboard"	
Numero de incompatibilidades entre los contenidos del "Dashboard" y los requerimientos de seguridad de información	
Tiempo necesario para analizar el "Dashboard" y obtener los requerimientos de información	
Porcentaje de actualizaciones realizadas según planificación	
Porcentaje de partes interesadas que no tiene acceso al "Dashboard"	
Numero de violaciones de seguridad de información que van contra el "Dashboard"	

Tabla 49: Evaluación de Metas del Dashboard de Seguridad de Información

Se recuerda que son indicadores ejemplo para una evaluación preliminar, la organización tiene como responsabilidad el emplear indicadores y métricas acordes a su realidad empresarial.

Evaluación de Buenas Prácticas

Se debe contar con un “Dashboard” que soporte un entorno fuerte de información respecto a seguridad, la organización y las partes interesadas contarán con una herramienta que facilite entender de mejor manera la realidad actual y defenderse de mejor manera de incidentes y amenazas.

Buenas Prácticas	Cumplimiento
Debe contener Información Operacional	

[52] Dashboard, hace referencia a un cuadro de mando (de gestión, de rendimiento) que permita visualizar los principales indicadores que intervienen en el cumplimiento de objetivos empresariales, en este caso de objetivos de seguridad de información.

Contener Información de amenazas de seguridad de Información, niveles de amenazas y vulnerabilidades.	
Se deben definir e implementar procesos SIEM (Manejo de Eventos y Seguridad de Información) que asistan a las partes interesadas del negocio a cumplir tareas diarias.	
Contiene el grado de efectividad y eficacia de actividades de seguridad de información	
Información de áreas donde se necesitan mejoras	
Acciones requeridas que ayuden a minimizar el riesgo de información	
Detalles de progresos hechos en base a reportes	
Información financiera respecto a costos de controles de seguridad de información e impacto financiero de incidentes de seguridad de información	

Tabla 50: Evaluación de Buenas Prácticas del "Dashboard" de seguridad de información

Para la construcción y operación de un “Dashboard” de seguridad todos los aspectos previamente señalados deben tomarse en cuenta. Esto es debido a que el “Dashboard” debe contener información de todos los eventos de seguridad de información.

Catalizador 6. Servicios, Infraestructura y Aplicaciones

Para la evaluación de las prestaciones de servicios se evaluarán atributos que debe cumplir cada una de las prestaciones de servicios para asegurar un nivel inicial adecuado de seguridad de información.

Para la evaluación de cada prestación se tomarán en cuenta los atributos, metas y una descripción que deben tener para contar con implementaciones adecuadas.

Arquitectura de Seguridad

Evaluación de Capacidades de la arquitectura de seguridad

Prestación de Servicio	Descripción	Cumplimiento
Incluir seguridad de información en la arquitectura	asegurar la inclusión de requerimientos de seguridad de información en la arquitectura.	
Mantenimiento de seguridad de arquitectura	Mantener un repositorio que contenga estándares de seguridad de información, componentes reusables, modelos y dependencias de la arquitectura organizacional y su mantenimiento.	
Instalación y mantenimiento de inventario de activos	Proveer un inventario de activos físico y de información, detallado, con propietarios, nivel crítico y apropiada clasificación	
Proveer administración de configuración de seguridad de información	Administración de configuración proveer los datos necesarios para identificar y avanzar en incidentes de seguridad de información	
	Utilizar el Sistema de administración de configuraciones (CMS) para evaluar el impacto de los incidentes e identificar los usuarios afectados por el problema	
	El Sistema de Administración de Configuraciones (CMS) categoriza los incidentes	
Establecer y mantener el descubrimiento de infraestructuras	Habilitar el descubrimiento de nuevos activos y entidades que se desarrollan en el entorno.	

Tabla 51: Evaluación de capacidades de Arquitectura de Seguridad.

Para contar con un nivel base de la arquitectura de seguridad es fundamental que la organización al menos cuente con el sistema de administración de configuraciones y que la arquitectura de seguridad incluya los requerimientos de información. A partir de estas capacidades se puede mejorar la arquitectura de seguridad.

Evaluación de Atributos de Arquitectura de Seguridad

Prestación de Servicios	Tecnologías Soportadas	Cumplimiento
Instalación y mantenimiento de inventario de activos	Base de Datos de Administración de Configuraciones (CMDB)	
	Sistemas de Administración de Activos	
	Protocolo Simple de Administración de Red (SNMP)	
	Agentes de Reporte	
Proveer administración de configuración de seguridad de información	Base de Datos de Administración de Configuraciones (CMDB)	
	Analizadores de vulnerabilidades	
	Soluciones de monitoreo en tiempo real de actividades de bases de datos	
	Soluciones de auditoria de políticas	
Establecer y mantener el descubrimiento de infraestructuras	Base de Datos de Administración de Configuraciones (CMDB)	
	Herramientas de descubrimiento de redes	
	Sistemas de Administración de Activos	
	Protocolo Simple de Administración de Red (SNMP)	
	Agentes de Reporte	

Tabla 52: Evaluación de Atributos de Arquitectura de Seguridad.

Para un correcto funcionamiento la arquitectura de seguridad al menos debe contar con los sistemas de administración de activos, de configuraciones de base de datos (CMDB) y el Protocolo Simple de Administración de Red (SNMP), con estas tecnologías es mucho más fácil que la arquitectura de seguridad de información se implemente de forma adecuada.

Evaluación de Metas de Arquitectura de Seguridad

Prestación de Servicio	Calidad de la Meta	Cumplimiento
Incluir seguridad de información en la arquitectura	Requerimientos de seguridad de Información están embebidos dentro de la arquitectura empresarial	
	Los Requerimientos de Seguridad de Información son trasladados de forma formal a la arquitectura de seguridad de información	
Mantenimiento de seguridad de arquitectura	La Arquitectura de seguridad de Información está alineada y evoluciona con los cambios de arquitectura empresarial	
Instalación y mantenimiento de inventario de activos	Todos los activos deben estar en inventario (correctamente y con información actualizada	
	nuevos activos y entidades pueden ser descubiertas de forma precisa y en lapsos determinados.	
Proveer administración de configuración de seguridad de información	Existe una configuración actualizada, completa y precisa de los activos y entidades dentro de la administración de configuración	
Establecer y mantener el descubrimiento de infraestructuras	nuevos activos y entidades pueden ser descubiertas de forma precisa y en lapsos determinados.	

Tabla 53: Evaluación de Metas de Arquitectura de Seguridad

Es importante que se cumplan al menos 3 de las 5 calidades de metas para contar con una arquitectura que tenga un desempeño adecuado en el cumplimiento de metas organizacionales.

Concientización de Seguridad

Evaluación de Capacidades de la Concientización de Seguridad

Prestación de Servicio	Descripción	Cumplimiento
Proveer comunicaciones con Seguridad de Información (permitiendo concientización y entrenamiento)	Proveer contenido, análisis, entrenamiento relacionado con Seguridad de Información.	

Tabla 54: Evaluación de Capacidades de Concientización de Seguridad

Esta capacidad es fundamental para que el servicio de concientización de seguridad sea útil, sin una comunicación adecuada no se tendrá un plan de concientización empresarial efectiva.

Evaluación de Atributos de Concientización de Seguridad

Prestación de Servicio	Tecnologías Soportadas	Cumplimiento
Proveer comunicaciones con Seguridad de Información (permitiendo concientización y entrenamiento)	Cursos de Entrenamiento	
	Noticias de Retroalimentación	
	Bases de Conocimiento (KBs)	
	Herramientas de entrenamiento	
	Redes Sociales	
	Email	
	Herramientas de Colaboración	
	Avisos de Vendedores y de Industria	
	Aviso CERT (Computer emergency Response Team)	

Tabla 55: Evaluación de Atributos de Concientización de Seguridad

Es recomendado que para un nivel inicial aceptable al menos se cumplan 6 de los 9 atributos señalados. Se alienta al a organización a implementar una base de conocimiento pues el uso de la misma facilita el tiempo de respuesta y soluciones de incidencias o problemas comunes, además contar con herramientas de entrenamiento es útil para guiar al personal en eventos que tratarán día a día.

Evaluación de Metas

Prestación de Servicio	Descripción	Cumplimiento
Proveer comunicaciones con Seguridad de Información (permitiendo concientización y entrenamiento)	Comunicación de seguridad de información efectiva, eficiente y a tiempo	
	Entrenamientos efectivos	

Tabla 56: Evaluación de Metas de Concientización de Seguridad

Es importante que se cumpla la comunicación adecuada como primer punto ya que es un factor necesario para lograr entrenamientos efectivos.

Desarrollo Seguro

Evaluación de Capacidades del Desarrollo Seguro

Prestación de Servicio	Descripción	Cumplimiento
Desarrollo de Prácticas de codificación seguras	Entrega y distribución de prácticas de codificación, ejemplos y demostraciones de código seguro	
Desarrollo de librerías de infraestructuras de seguridad	Diseño y entrega de información relacionada al entorno y módulos de seguridad de información	

Tabla 57: Evaluación de Capacidades del Desarrollo Seguro.

Para un nivel inicial de seguridad se recomienda implementar ambas capacidades del servicio de desarrollo de seguridad, puesto que son complementarias y necesarias para infraestructura y aplicaciones de seguridad de información.

Evaluación de Atributos del Desarrollo Seguro

Prestación de Servicio	Tecnologías Soportadas	Cumplimiento
Desarrollo de Prácticas de codificación seguras	Compiladores y linkers	
	Recursos de codificación segura (libros, cursos, ejemplos)	
	Herramientas de análisis binario y estático	
	escáner de Código	
Desarrollo de librerías de infraestructuras de seguridad	Lenguajes de desarrollo	
	Recursos de codificación segura (libros, cursos, ejemplos)	
	escáner de Código	
	Herramientas de Analisis binario y estático	
	Compiladores y linkers	

Tabla 58: Evaluación de Atributos del Desarrollo Seguro.

Como se puede ver en la matriz los atributos para ambas capacidades del servicio son los mismos, es por ello que se recomienda que se cumpla en totalidad esta matriz de evaluación.

Evaluación de Metas del Desarrollo Seguro

Prestación de Servicio	Calidad de Metas	Cumplimiento
Desarrollo de Prácticas de codificación seguras	Identificación precisa de riesgos de información y efectos en el negocio o activos de los mismos	
Desarrollo de librerías de infraestructuras de seguridad	Mejora en alinear los requerimientos de seguridad de información con el sistema de configuración de seguridad de información	

Tabla 59: Evaluación de Metas del Desarrollo Seguro

Se recomienda al menos cumplir una de las metas del desarrollo seguro como forma inicial en la implementación de una cultura de seguridad de información empresarial, se recuerda que es fundamental para cualquier desarrollo el tomar en cuenta los requerimientos de seguridad de información.

Evaluación de Seguridad

Evaluación de Capacidades de Evaluación de Seguridad

Prestación de Servicio	Descripción	Cumplimiento
Realizar evaluaciones de Seguridad de Información	Evaluación de rendimiento de seguridad de información, de sistemas, procesos, aplicaciones o unidades organizacionales, incidentes de seguridad de información	
realizar evaluaciones de Riesgos de Información	Procesos de identificación evaluación, estimación y análisis de amenazas y vulnerabilidades de entidades, sistemas, procesos o unidades organizacionales	
	Análisis base para identificación apropiada y mediciones de gastos efectivas para determinación de riesgos.	

Tabla 60: Evaluación de Capacidades de Evaluación de Seguridad.

Es importante que se cumplan al menos 2 capacidades pues su intervención en la identificación de amenazas y riesgos es fundamental para un correcto funcionamiento de este servicio.

Evaluación de Atributos de Evaluación de Seguridad

Prestación de Servicio	Tecnologías Soportadas	Cumplimiento
Realizar evaluaciones de Seguridad de Información	Escáner de vulnerabilidades	
	sniffers, fuzzers	
	Analizadores de protocolos	
	Analizadores de red pasivos y activos	
	Honeypots	
	Agentes "Endpoint"	
	Escáner de aplicaciones	
	Administración de Cumplimiento	
	Herramientas de reportes	
	Accesos remotos	
realizar evaluaciones de Riesgos de Información	Escáner de vulnerabilidades	
	sniffers, fuzzers	
	Analizadores de protocolos	
	Analizadores de red pasivos y activos	
	Honeypots	
	Agentes "Endpoint"	
	Escáner de aplicaciones	
	Administración de Cumplimiento	
	Herramientas de reportes	
	Accesos remotos	

Tabla 61: Evaluación de Atributos de la Evaluación de Seguridad.

Hay que recalcar que ambos servicios soportan las mismas capacidades por eso es recomendado cumplir con ambos para un servicio de evaluación segura, y al menos deben cumplirse 7 de las 10, priorizando las tecnologías que más apoyen al negocio, en el caso de organizaciones de Cloud Computing se recomienda tomar en cuenta tecnologías de análisis de red, de Endpoints, sniffers y accesos remotos como prioridades puesto que se ajustan de mejor manera al modelo de negocio.

Evaluación de Metas de la Evaluación de Seguridad

Prestación de Servicio	Calidad de Metas	Cumplimiento
Realizar evaluaciones de Seguridad de Información	Identificación precisa de debilidades, deficiencias, vulnerabilidades y amenazas de seguridad de información en activos o entidades.	
Realizar evaluaciones de Riesgos de Información	Identificación precisa de todos los riesgos de información y riesgos o efectos al negocio.	

Tabla 62: Evaluación de Metas de la Evaluación de Seguridad.

Las metas son muy similares en ambos aspectos evaluados es por ello que se requiere un cumplimiento de calidad total en esta evaluación para conseguir un adecuado rendimiento de las evaluaciones de seguridad.

Sistemas adecuadamente configurados y seguros, alineados con requerimientos y arquitectura de seguridad

Evaluación de Capacidades de sistemas adecuadamente configurados y seguros, alineados con requerimientos y arquitectura de seguridad

Prestación de Servicio	Descripción	Cumplimiento
Proveer adecuadamente alta seguridad y Sistemas configurados, alineados con requerimientos y arquitectura de la seguridad de información	proveer configuraciones y ajustes de seguridad de información para asegurar la postura de seguridad de información de un determinado sistema, basándose en requerimientos y diseños de arquitectura	
Proveer protección a dispositivos de seguridad	Proporcionar medidas y actividades de seguridad de información específicas para los dispositivos	
Proveer protección a información física	proporcionar adecuadas medidas de seguridad para de datos e información.	

Tabla 63: Evaluación de Capacidades de sistemas adecuadamente configurados y seguros, alineados con requerimientos y arquitectura de seguridad

Es recomendado que al menos se cumplan 2 de las 3 capacidades presentes en la matriz para contar con un nivel inicial de este servicio.

Evaluación de Atributos de sistemas adecuadamente configurados y seguros, alineados con requerimientos y arquitectura de seguridad

Prestación de Servicio	Tecnologías Soportadas	Cumplimiento
Proveer adecuadamente alta seguridad y Sistemas configurados, alineados con requerimientos y arquitectura de la seguridad de información	Protocolo de transferencia de Datos (FTP)	
	métodos de actualización CMDB	
	soluciones de Verificación de Firmas	
	Monitorear integridad de archivos	
	Módulos de Kernel	
	Requerimientos de Seguridad de Información Arquitectura de Seguridad de Información	
	Administración de Seguridad	
	Administración de Patch	
	Administración de Virtualización	
	Administración de la Nube	

Proveer protección a dispositivos de seguridad	Sistemas Operativos de Dispositivos	
	Sistemas de Administración de Plataformas	
Proveer protección a información física	CCTV (Televisión de circuito cerrado)	
	Candados (seguros)	
	Alarmas	
	Controles de Acceso	
	Bóvedas	
	Reportes de Inteligencia	
	Interfaces de primera respuesta	
	Soluciones de Administración de Locaciones	
	Sistemas de protección contra incendios	
	Cerraduras temporales	
	Soluciones de accesos físicos	

Tabla 64: Evaluación de Atributos de sistemas adecuadamente configurados y seguros, alineados con requerimientos y arquitectura de seguridad

Para esto se recomienda que para el segundo atributo (Proveer protección a dispositivos de seguridad) se cumplan los dos soportes de tecnología, mientras que para los demás se deben cumplir al menos 80% de sus soportes tecnológicos.

Es importante recalcar que se debe priorizar la protección de la información puesto a que es fundamental para generar valor para el negocio.

Evaluación de Metas de sistemas adecuadamente configurados y seguros, alineados con requerimientos y arquitectura de seguridad

Prestación de Servicio	Metas de Calidad	Cumplimiento
Proveer adecuadamente alta seguridad y Sistemas configurados, alineados con requerimientos y arquitectura de la seguridad de información	mejoras en configuración de seguridad de información de sistemas alineados con los requerimientos de seguridad de información	
Proveer protección a dispositivos de seguridad	mejoras en configuración de seguridad de información en dispositivos alineados con los requerimientos de seguridad de información	
Proveer protección a información física	Controles Físicos alineados con requerimientos de seguridad de información	

Tabla 65: Evaluación de Calidad de Metas de sistemas adecuadamente configurados y seguros, alineados con requerimientos y arquitectura de seguridad

Es recomendado que se cumplan todas las metas señaladas en la matriz para asegurar la implementación adecuada de este servicio.

Accesos a usuarios y derechos de acceso alineados con requerimientos del negocio

Evaluación de Capacidades accesos a usuarios y derechos de acceso alineados con requerimientos del negocio

Prestación de Servicio	Descripción	Cumplimiento
Proveer servicios de autenticación	Proporcionar un conjunto de capacidades para desempeñar identificaciones de usuarios utilizando factores definidos en las políticas de seguridad y requerimientos de accesos de control	
Proporcionar servicios de provisión de seguridad de la información	Proporcionar un conjunto de capacidades para crear, entregar y administrar tecnologías que faciliten a la seguridad de información.	
Evaluar servicios de clasificación de entidades de seguridad de información	Evaluar las categorías, clasificaciones y niveles de seguridad de información.	
Proporcionar servicios de revocación	Proporcionar un conjunto de capacidades para cancelar, retirar o terminar los derechos de seguridad de información a una entidad, sistema, aplicación, etc.	
Proveer autenticaciones de usuarios y derechos de autorización alineados con requerimientos del negocio	proporcionar un conjunto de capacidades y prácticas de mantenimiento que permitan identificar usuarios empleando factores que están determinados en políticas de seguridad de información y requerimientos de control de acceso, todo definido por los requerimientos del negocio.	

Tabla 66: Evaluación de Capacidades de accesos a usuarios y derechos de acceso alineados con requerimientos del negocio

Para que la organización se encuentre direccionada hacia la seguridad de la información es esencial que cumpla con estos servicios de controles de acceso. Se recomienda un cumplimiento total.

Evaluación de Atributos accesos a usuarios y derechos de acceso alineados con requerimientos del negocio

Prestación de Servicio	Tecnologías Soportadas	Cumplimiento
Proveer servicios de autenticación	Biométricos	
	Certificaciones	
	llaves electrónicas	
	Tarjetas inteligentes	
	Dispositivos con Ids embebidos	
	contraseñas de un uso (OTPs)	
	usuarios y contraseñas	
	Identidad como un servicio (IDaaS), códigos de barras, códigos de productos universales (UPC)	
	Lista de Revocación de certificados (CRL), ID federation	
	Certificados "Root"	
	Servicios de administración clave	
	Servicios de locación	
	Servicios de reputación	
	infraestructura de llave pública (PKI)	
Proporcionar servicios de provisión de seguridad de la información	Open Mobile Alliance (OMA), Administración de suministro de dispositivos (DM)	
	Subscriber identity module (SIM), certificaciones	
	Servicios de cifrado locales y remotos	
	Servicios de administración clave	
	Soluciones de administración de dispositivos y sistemas de servicios de localización	
	Soluciones de distribución de software	
	Retroalimentación de Recursos Humanos	
Evaluar servicios de clasificación de entidades de seguridad de información	Herramientas de visualización y diagramas	
	Herramientas de clasificación	
	CMDB	
	Arquitectura empresarial	
	Estándares de Clasificación	

	Adelantar soluciones tipo "release candidate" RC	
Proporcionar servicios de revocación	SIM, certificados	
	Servicios de cifrado locales y remotos	
	Servicios de administración clave	
	Servicios de locación	
	Retroalimentación de Recursos Humanos	
	PKI	
Proveer autenticaciones de usuarios y derechos de autorización alineados con requerimientos del negocio	SIM, certificados	
	Servicios de cifrado locales y remotos	
	Servicios de administración clave	
	Servicios de locación	
	PKI	

Tabla 67: Evaluación de Atributos de accesos a usuarios y derechos de acceso alineados con requerimientos del negocio

Debido a que hay varias tecnologías soportadas que intervienen en varios servicios, se recomienda que al menos se cumpla un 80% de los atributos en esta evaluación para mantener un nivel adecuado en este servicio.

Evaluación de Metas accesos a usuarios y derechos de acceso alineados con requerimientos del negocio

Prestación de Servicio	Calidad de Metas	Cumplimiento
Proveer servicios de autenticación	Autenticaciones precisas, completas y oportunas a las entidades y servicios	
Proporcionar servicios de provisión de seguridad de la información	Provisiones completas, precisas y oportunas a todos los servicios y elementos de seguridad de información	
Evaluar servicios de clasificación de entidades de seguridad de información	Clasificaciones de las entidades completas y precisas.	
Proporcionar servicios de revocación	Revocaciones oportunas y precisas a servicios y entidades	
Proveer autenticaciones de usuarios y derechos de autorización alineados con requerimientos del negocio	Autenticaciones y autorizaciones precisas, completas y oportunas a las entidades y servicios	

Tabla 68: Evaluación de Metas de accesos a usuarios y derechos de acceso alineados con requerimientos del negocio

Es de suma importancia que la organización al menos cumpla 3 de las 5 metas de estos servicios para tener un nivel inicial aceptable.

Protección adecuada contra malware, ataques externos e intentos de intrusión

Evaluación de Capacidades de protección adecuada contra malware, ataques externos e intentos de intrusión

Prestación de Servicio	Descripción	Cumplimiento
Proveer seguridad de información y medidas contra amenazas	Planear, implementar, mantener y mejorar medidas y actividades, acciones, procesos, sistemas que se enfoquen en vulnerabilidades, riegos y amenazas.	
Proveer protección de datos	Proporcionar un conjunto de capacidades y prácticas de administración para implementar protección, confidencialidad, integridad y disponibilidades de datos en cualquiera de sus estados.	

Tabla 69:Evaluar las Capacidades de protección adecuada contra malware, ataques externos e intentos de intrusión

Es necesario que se cumplan en totalidad estos dos puntos de evaluación.

Evaluación de Atributos de protección adecuada contra malware, ataques externos e intentos de intrusión

Prestación de Servicio	Descripción	Cumplimiento
Proveer seguridad de información y medidas contra amenazas	Cifrado	
	PKI, sniffers, Inspección a profundidad de Paquetes (DPI)	
	Firewalls	
	Sensores, analizadores de paquetes	
	Administración de cumplimiento	
	Requerimientos y arquitectura de seguridad de información	
	CMDB	
	Administración de virtualización	
	Administración de la nube	
	Administración de agentes y proveedores	
	Repositorios de Software Open Source	

	Consejos de proveedores de seguridad de información, Bases de Conocimiento (KBs)	
	Antimalware, antiroots, antispyware, antiphishing	
	Protección de navegadores, inspección de contenidos	
	Servicios de Reputación	
Proveer protección de datos	PKI, sniffers, Inspección a profundidad de Paquetes (DPI)	
	Cifrado	
	Prevención de perdida de Información (DLP)	
	soluciones de administración de Dispositivos y Sistemas	
	Soluciones de Distribución de Software	
	Sistemas de administración remota	
	Soluciones de administración de Nube y virtualización	
	Administración de documentación	
	Sistemas de clasificación de información	

Tabla 70: Evaluación de Atributos de protección adecuada contra malware, ataques externos e intentos de intrusión

Algunas de las tecnologías presentes en esta evaluación son recurrentes en otros servicios, por lo cual se recomienda cumplir al menos un 80% de tecnologías soportadas debido a su interacción con otros servicios de la función de seguridad de información.

Evaluación de Metas de protección adecuada contra malware, ataques externos e intentos de intrusión

Prestación de Servicio	Descripción	Cumplimiento
Proveer seguridad de información y medidas contra amenazas	Maximizar la protección contra amenazas conocidas y desconocidas	
Proveer protección de datos	Maximizar la protección de datos en cualquiera de sus estados	

Tabla 71: Evaluación de Metas de protección adecuada contra malware, ataques externos e intentos de intrusión

Es crucial que se cumplan ambas metas para que la organización este orientada e implemente de forma adecuada este servicio.

Adecuadas respuestas a incidentes

Evaluación de Capacidades de adecuadas respuestas a incidentes

Prestación de Servicio	Descripción	Cumplimiento
Proveer servicios de escalamiento de seguridad de información	Proporcionar un conjunto de capacidades y prácticas de administración para resolver incidentes de seguridad de información a tiempo	
Proveer análisis forense de seguridad de información	Proporcionar un conjunto de capacidades forenses para aplicarlas en sistemas, procesos, aplicaciones, servicios, dispositivos y apoyando investigaciones y colecciones de evidencia	
	Asegurar que las capacidades se usen de forma legal y manteniendo la cadena de custodia como lo enmarcan procedimientos gubernamentales y legales	

Tabla 72: Evaluación de Capacidades de adecuadas respuestas a incidentes

Se enfatiza el cumplimiento de todas las capacidades de este servicio debido al nivel de importancia que se tiene al momento de cumplir normativas legales en actividades forenses.

Evaluación de atributos de adecuadas respuestas a incidentes

Prestación de Servicio	Tecnologías Soportadas	Cumplimiento
Proveer servicios de escalamiento de seguridad de información	Administración de Vulnerabilidades	
	Consejos de proveedores de Seguridad de Información	
	Consejos de la Industria de Seguridad de Información	
	Sistemas de escalamiento Jerárquico (en base a la organización)	
	Políticas de Seguridad de Información	
Proveer análisis forense de seguridad de información	Herramientas de inspección de memoria	
	analizadores de Red	
	Analizadores de Log	

	Herramientas de inspección de Datos y Aplicaciones	
	Herramientas de Ingeniería inversa	
	Herramientas de análisis de Malware	
	Herramientas forenses Open Source (OSS[53]) y de proveedores	
	Trafico de Red	
	Malware y snippets de códigos	
	SIEM (security Information and Even Management)	

Tabla 73: Evaluación de Atributos de adecuadas respuestas a incidentes

Para contar con servicios de nivel aceptable se recomienda que en la evaluación la organización cumpla al menos 10 de los 15 atributos y soportes tecnológicos.

Evaluación de Metas de adecuadas respuestas a incidentes

Prestación de Servicio	Calidad de Metas	Cumplimiento
Proveer servicios de escalamiento de seguridad de información	Procedimientos de escalamiento oportunos, efectivos y eficientes	
Proveer análisis forense de seguridad de información	Análisis y recolección de información precisa y completa.	

Tabla 74: Evaluación de Metas de adecuadas respuestas a incidentes

Para pasar la evaluación es necesario que este servicio cumpla ambas metas.

Pruebas de Seguridad

Evaluación de Capacidades de Pruebas de Seguridad

Prestación de Servicio	Descripción	Cumplimiento
Realizar pruebas de seguridad de Información	Proporcionar pruebas relacionadas con seguridad de información y evaluaciones de servicios, pruebas de protección de datos y validación de integridad, entre otras.	

Tabla 75: Evaluación de Capacidades de Pruebas de Seguridad

Es necesario que la organización cumpla con esta capacidad del servicio, para administrar de forma correcta las pruebas de seguridad.

[53] Open Source Software

Evaluación de Atributos de Pruebas de Seguridad

Prestación de Servicio	Tecnologías Soportadas	Cumplimiento
Realizar pruebas de seguridad de Información	Herramientas de seguridad de información	
	scripts de pruebas	
	SDKs	
	Métodos alternativos de arranque (boot)	
	herramientas de análisis de regresión	
	Herramientas de pruebas de seguridad de información	
	Sistemas y herramientas de pruebas unitarias	

Tabla 76: Evaluación de Atributos de Pruebas de Seguridad

En esta evaluación al menos se requieren 4 de las 7 tecnologías soportadas para que la organización tenga una implementación de nivel inicial aceptable.

Evaluación de Metas de Pruebas de Seguridad

Prestación de Servicio	Metas	Cumplimiento
Realizar pruebas de seguridad de Información	Mejorar la configuración de seguridad de información alineándola a los requerimientos de seguridad de información	

Tabla 77: Evaluación de Metas de Pruebas de Seguridad

Esta meta debe cumplirse obligatoriamente debido a que está asociada con otros servicios de seguridad de información.

Monitorización y servicios de alerta para eventos de seguridad

Evaluación de Capacidades de Monitorización y servicios de alerta para eventos de seguridad

Prestación de Servicio	Descripción	Cumplimiento
Proveer servicios de monitoreo para procesos y eventos de seguridad de información	Proporcionar un conjunto de capacidades para permitir la monitorización y uso de Dashboard.	
Proveer servicios de alerta y reportes de procesos, prácticas y eventos de seguridad de información	Proporcionar un conjunto de capacidades que permitan reportes y correlación de eventos, incidentes y procesos.	

Proveer métricas e indicadores de seguridad de información	Proporcionar un conjunto de capacidades que entreguen indicadores y métricas de seguridad de información para su análisis y determinación de rendimiento.	

Tabla 78: Evaluación de Capacidades de Monitorización y servicios de alerta para eventos de seguridad

Para contar con un servicio de nivel inicial aceptable la organización al menos debe contar con 2 de las 3 capacidades evaluadas.

Evaluación de Atributos de Monitorización y servicios de alerta para eventos de seguridad

Prestación de Servicio	Tecnologías Soportadas	Cumplimiento
Proveer servicios de monitoreo para procesos y eventos de seguridad de información	Logs	
	Protocolo Simple de Administración de Red (SNMP)	
	Sistemas de Alerta	
	SIEM (security Information and Even Management)	
	Administración de Dashboard	
	Centro de operaciones de Redes (NOCs)	
Proveer servicios de alerta y reportes de procesos, prácticas y eventos de seguridad de información	Logs	
	Protocolo Simple de Administración de Red (SNMP)	
	Sistemas de Alerta	
	SIEM (security Information and Even Management)	
	Administración de Dashboard	
	Centro de operaciones de Redes (NOCs)	
Proveer métricas e indicadores de seguridad de información	hojas de Evaluación e indicadores	
	SIEM (security Information and Even Management)	
	Administración de Dashboard	
	Sistemas de Alerta	
	Herramientas de respuesta a incidentes	
	Políticas de Seguridad de Información	

Tabla 79: Evaluación de Atributos de Monitorización y servicios de alerta para eventos de seguridad

Debido a que se repiten muchos atributos, tecnologías soportadas se recomienda el cumplimiento de al menos el 80% en esta matriz de evaluación.

Evaluación de Metas de Monitorización y servicios de alerta para eventos de seguridad

Prestación de Servicio	Descripción	Cumplimiento
Proveer servicios de monitoreo para procesos y eventos de seguridad de información	Monitorizar procesos y eventos de seguridad de información	
Proveer servicios de alerta y reportes de procesos, prácticas y eventos de seguridad de información	Alertar de eventos críticos de seguridad de información	
Proveer métricas e indicadores de seguridad de información	Métricas de seguridad de información deben alinearse con requerimientos de seguridad de información	

Tabla 80: Evaluación de Metas de Monitorización y servicios de alerta para eventos de seguridad

Todas las metas deben cumplirse para una ejecución adecuada de este servicio, debido a que varias de las metas se relacionan muy cercanamente con otros servicios o catalizadores.

Catalizador 7. Personas, Habilidades y Competencias

Para la evaluación de este catalizador se emplean los siguientes parámetros: Experiencia, Títulos, conocimiento y habilidades. Es importante entender que los títulos son obligatorios para cada una de las evaluaciones y no se los tomarán en cuenta en la explicación.

Evaluación del Gobierno de Seguridad de Información

Requerimientos	Descripción	Cumplimiento
Título	CISM[54]	
Experiencia	Varios años en áreas de seguridad de información y TI	
	Creación e implementación de políticas de seguridad de información	
	Alineación de estrategias de seguridad de información con el gobierno de la organización	
	Alineación de políticas de seguridad con necesidades del negocio	

[54] CISM: Certified Information Security Manager, Certificación otorgada por ISACA para Administradores de Seguridad de Información

Conocimientos	Desarrollar casos de negocio para justificar inversiones de seguridad de información	
	Definición de métricas aplicaciones a la gobernabilidad de seguridad de información	
	Regulaciones y aspectos legales que afectan los requerimientos de seguridad de información	
	Reconocer estándares internacionales, marcos de referencia y buenas prácticas de gobierno y desarrollo de seguridad de información	
	Métodos de implementación de políticas de seguridad de información	
Habilidades	Orientación a procesos	
	Buen entendimiento de prácticas de seguridad de información	
	Liderazgo	
	Comunicación	

Tabla 81: Evaluación del Gobierno de Seguridad de Información

Para este cargo, debido a su alto nivel de importancia y puesto que es un cargo de gobierno es fundamental que se cumplan todos los requisitos, se necesita un 100% en esta evaluación.

Formulación de estrategia de seguridad de Información

Requerimientos	Descripción	Cumplimiento
Título	CISM, CISO o ISSC	
Experiencia	Varios años en áreas de seguridad de información y TI	
	Experiencia con estrategia y gobierno de seguridad de información	
	Amplio entendimiento de la relación entre el negocio y la función de seguridad de información	

	Experiencia en la creación e implementación de estrategias, principios, políticas y prácticas de seguridad de información	
Conocimientos	Entendimiento de la cultura y valores empresariales	
	Regulaciones y aspectos legales que afectan los requerimientos de seguridad de información	
	Desarrollo de políticas de seguridad de información	
	Definir estrategias de seguridad de información que se alinean a las estrategias de la organización	
	Métodos de implementación de políticas de seguridad de información	
	Reconocer estándares internacionales, marcos de referencia y buenas prácticas de gobierno y desarrollo de seguridad de información	
Habilidades	Liderazgo	
	Alto nivel de abstracción	
	Pensamiento estratégico	
	Orientación a negocios	
	Comunicación	

Tabla 82: Evaluación de Formulación de estrategia de seguridad de Información

Es importante que al menos se cumpla con el 80 por ciento de requerimientos para delimitar un perfil adecuado e inicial que aporte adecuadamente para mejorar el nivel de seguridad de información de la organización.

Administrador de Riesgos de Información

Requerimientos	Descripción	Cumplimiento
Título	CRISC	
Experiencia	Varios años en áreas de seguridad de información y TI	
	Administrador de riesgos y evaluación de amenazas	
	Mitigación de riesgos basados en necesidades de la organización	
	Evaluar riesgos relacionados a prácticas de seguridad de información	
Conocimientos	Evaluación de riegos	
	Procesos del negocio y funciones	
	Métodos para establecer modelos de clasificación de información	
	Estándares de Seguridad de Información (NIST, PCI, etc.)	
	Leyes y regulaciones relacionadas a seguridad de información	
	modelos de referencia de cuantificación y reporte de riesgos	
Habilidades	Orientación a procesos	
	Alto nivel de abstracción	
	Experto en resolución de problemas	
	Entendimiento de prácticas de seguridad de información	
	Análisis y mitigación de riesgos	

Tabla 83: Evaluación de Administrador de Riesgos de Información

Para contar con personal que administre de forma adecuada los riesgos se determina que el perfil adecuado debe cumplir con al menos 80% de los requisitos presentados en la anterior matriz.

Desarrollo de arquitectura de seguridad de información

Requerimientos	Descripción	Cumplimiento
Título	CRISC, CISSP	
Experiencia	Varios años en áreas de seguridad de información y TI	
	Experiencia trabajando con software y hardware, OS, aplicaciones de bases de datos y redes	
	Entendimiento técnico de interconexión de sistemas	
Conocimientos	Buen entendimiento de protocolos de redes, bases de datos, OS y su aplicación al negocio	
	Buen entendimiento del funcionamiento de las tecnologías empresariales	
	Arquitectura de seguridad de información (TOGAF, SABSA)	
	Métodos de diseño de prácticas de seguridad de información	
	estándares y buenas prácticas de seguridad de información (ISO/IEC 27000's, NIST, PCI)	
	Tecnologías y metodologías emergentes de seguridad de información	
	Administración de programas, políticas, prácticas estándares de seguridad de información que pertenecen a las actividades del negocio	
Habilidades	Capacidades técnicas	
	Alto nivel de abstracción	
	Experto en resolución de problemas	
	Alto conocimiento de tendencias de TI	
	Experto en operaciones computacionales	

Tabla 84: Evaluación de Desarrollo de arquitectura de seguridad de información

Para esta posición el perfil que sea escogido por la organización debe cumplir al menos un 80% de los requerimientos de esta matriz de evaluación, esto asegurará el

desarrollo de aplicaciones, servicios que cumplan buenas prácticas y estándares de seguridad de información, minimizando vulnerabilidades y riesgos.

Operaciones de Seguridad de Información

Requerimientos	Descripción	Cumplimiento
Título	CRISC, CISSP	
Experiencia	Experiencia en Ti y Seguridad de Información	
	Antecedentes en seguridad de información	
	Conocimiento de la alineación del negocio con la seguridad de información	
Conocimientos	Implementación de programas de administración de seguridad de información	
	Monitoreo y análisis de Log's	
	Administración de redes de seguridad de Información	
	Administración de "endpoint" de seguridad de información	
Habilidades	Alto conocimiento de administración de proyectos	
	Comunicación	
	Pensamiento analítico	
	Orientación a detalles	
	Planificación y manejo de tiempo	

Tabla 85: Evaluación de Operaciones de Seguridad de Información

Se debe contar con una evaluación superior al 80% para que la organización tenga un perfil que se desempeñe de forma adecuada.

Evaluación, cumplimiento y pruebas de información

Requerimientos	Descripción	Cumplimiento
Título	Certificación CISA	
Experiencia	Varios años en áreas de seguridad de información y TI	
	Auditoría	
	Aseguramiento de prácticas y políticas de Seguridad de Información	
Conocimientos	estándares de auditoria de seguridad de Información	
	técnicas para planificación de proyectos y auditorias	
	estándares y buenas prácticas de seguridad de información (ISO/IEC 27000's, NIST, PCI)	
	Leyes y regulaciones relacionadas a seguridad de información	
Habilidades	Altos niveles de valores éticos	
	Orientación a Procesos	
	Excelentes habilidades de negociación	

Tabla 86: Evaluación de la Evaluación, cumplimiento y pruebas de información

Es fundamental que para este perfil se cumplan al menos 90% de los requerimientos pues esta posición se encargará de verificar el cumplimiento de los procesos, políticas y regulaciones relacionadas con seguridad de la información de los miembros de la organización

Sección II: Evaluación de Procesos

En esta sección se realiza una evaluación a los 3 procesos cuya implementación se relaciona de forma directa y enmarca aspectos de seguridad de información. La implementación adecuada de estos procesos es el mínimo requerimiento para contar con una organización enfocada en seguridad de Información.

Para la valoración de los procesos se realiza una evaluación de las actividades específicas de seguridad de información que intervienen en las prácticas de gobierno de cada proceso.

APO13: Administración de Seguridad

Descripción del proceso: Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.

Propósito del proceso: 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.

Evaluación de Actividades Específicas de Seguridad de Información

Prácticas de Gobierno	Actividades Específicas de Seguridad de Información	Cumplimiento
APO13.01 Establecer y mantener un Sistema de Administración de Seguridad de Información (ISMS).	Definir el alcance y límites del ISMS en términos de las características de la empresa, la organización, su localización, activos y tecnología. Incluir detalles de y justificación para, cualquier exclusión del alcance.	
	Definir un ISMS de acuerdo con la política empresarial y alinearlo con la empresa, la organización, su localización, activos y tecnología.	
	Alinear el ISMS con el enfoque global de la gestión de la seguridad en la empresa.	
	Obtener autorización de la dirección para implementar y operar o cambiar el ISMS.	
	Preparar y mantener una declaración de aplicabilidad que describa el alcance del ISMS.	
	Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información.	
	Comunicar el enfoque de ISMS.	

APO13.02 Definir y gestionar un plan de tratamiento de riesgos de la seguridad de la información.	Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura de la empresa. Asegurar que el plan identifique las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, las responsabilidades y las prioridades asociadas para gestionar los riegos identificados de seguridad de información.	
	Mantener un inventario de componentes de la solución implementada para gestionar los riesgos relacionados con la seguridad como parte de la arquitectura de la empresa.	
	Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información, sustentados en casos de negocio adecuados que incluyan consideren la financiación la asignación de roles y responsabilidades.	
	Proporcionar información para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas en base al plan de tratamiento de riesgos de seguridad de información.	
	Definir la forma de medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizar estas mediciones para evaluar la efectividad y producir resultados reproducibles y comparables.	
	Recomendar programas de formación y concientización en seguridad de la información.	
	Integrar la planificación, el diseño, la implementación y la supervisión de los procedimientos de seguridad de información y otros controles que permitan la prevención y detección temprana de eventos de seguridad, así como la respuesta a incidentes de seguridad.	
APO13.03 Supervisar y revisar el SGSI.	Realizar revisiones periódicas del ISMS, incluyendo aspectos de políticas, objetivos y prácticas de seguridad del ISMS. Considerar los resultados de auditorías de seguridad, incidentes, resultados de mediciones de efectividad, sugerencias y retroalimentación de todas las partes interesadas.	
	Realizar auditorías internas al ISMS a intervalos planificados.	

	Realizar revisiones periódicas del ISMS, por parte de la Dirección para asegurar que el alcance sigue siendo el adecuado y que se han identificado mejoras en el proceso del ISMS.	
	Proporcionar información para el mantenimiento de los planes de seguridad para que consideren las incidencias de las actividades de supervisión y revisión periódica.	
	Registrar acciones y eventos que podrían impactar en la efectividad o el desempeño del ISMS.	

Tabla 87: Evaluación de Actividades de Proceso del APO13: Administración de Seguridad.

Para que la organización cuente con una implementación adecuada del proceso se debe contar con un cumplimento superior al 80% en cada una de las prácticas de gobierno. Es importante recalcar que estas actividades también influyen en determinar la madurez del proceso.

DSS04: Administración de Continuidad

Descripción del proceso: 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.

Propósito del proceso: Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa.

Evaluación de Actividades Específicas de Seguridad de Información

Prácticas de Gobierno	Actividades Específicas de Seguridad de Información	Cumplimiento
DSS04.01 Definir la política de continuidad de negocio, objetivos y alcance.	Asegurar que la seguridad de información sea parte del ciclo de vida de continuidad del Negocio	
DSS04.02 Mantener una estrategia de continuidad.	Incluir escenarios que tomen en cuenta la seguridad de información	
DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.	Incluir requerimientos de seguridad de información en el Plan de Continuidad del Negocio (BCP)	

DSS04.04 Ejercitar, probar y revisar el Plan de Continuidad del Negocio (BCP). *(No aplican actividades específicas de seguridad, por lo que se emplean las actividades del proceso).	Definir los objetivos para ejercitar y probar los sistemas del plan (de negocio, técnicos, logísticos, administrativos, procedimentales y operacionales) para verificar la completitud del BCP para enfrentarse a los riesgos de negocio.	
	Definir y acordar ejercicios que sean razonables con las partes interesadas, validar los procedimientos de continuidad, e incluir roles y responsabilidades y acuerdos de retención de datos que ocasionen la mínima disrupción en los procesos de negocio.	
	Asignar roles y responsabilidades para realizar ejercicios y pruebas del plan de continuidad.	
	Planificar ejercicios y actividades de prueba tal como esté definido en el plan de continuidad.	
	Realizar un análisis y revisión post-ejercicio para considerar el logro.	
	Desarrollar recomendaciones para mejorar el plan de continuidad actual en base a los resultados de la revisión.	
DSS04.05 Revisar, mantener y mejorar el plan de continuidad.	Considerar incidentes de seguridad de información como disparadores importantes para mejorar el BCP	
DSS04.06 Proporcionar formación en el plan de continuidad. *(No aplican actividades específicas de seguridad, por lo que se emplean las actividades del proceso).	Definir y mantener los planes y requerimientos de formación para quienes realicen de manera continuada planificación de la continuidad, análisis de impacto, evaluaciones de riesgos, comunicación con los medios y respuesta a incidentes. Asegurar que los planes de formación consideren la frecuencia de formación y los mecanismos de entrega de la formación.	
	Desarrollar competencias basadas en formación práctica que incluyan la participación en ejercicios y pruebas.	
	Supervisar habilidades y competencias basándose en los resultados de los ejercicios y las pruebas.	
DSS04.07 Gestionar acuerdos de respaldo.	Asegurar que los requerimientos de seguridad de información estén incluidos en procesos de respaldo (backup) y restauración.	
DSS04.08 Ejecutar revisiones post-reanudación.	Asegurar que la seguridad de información este incluida en revisiones posteriores a reanudación	

Tabla 88: Evaluación de Evaluación de Actividades Específicas de Seguridad de Información

Para este proceso se recomienda que para las prácticas de gobierno DSS04.04 y DSS04.06 se tenga un nivel de cumplimento superior al 80%.

Mientras que para las demás prácticas se debe tener un cumplimiento total de las actividades específicas de seguridad, además que las implementaciones de las prácticas del proceso deben ser aceptables como mínimo.

DSS05: Administración de Servicios de Seguridad

Descripción del Proceso: 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.

Propósito del Proceso: Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.

Evaluación de Actividades Específicas de Seguridad de Información

Prácticas de Gobierno	Actividades de Procesos	Cumplimiento
DSS05.01 Proteger contra software malicioso (malware).	Comunicar concientización sobre el malware y fortalecer procedimientos y responsabilidades de prevención.	
	Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de malware que se actualicen según sea requerido.	
	Distribuir todo el software de protección de forma centralizada empleando una configuración centralizada y la gestión de cambios.	
	Revisar y evaluar regularmente la información sobre nuevas posibles amenazas.	
	Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada.	
	Realizar formación periódica sobre malware en correos electrónicos e Internet. Formar a los usuarios para la no instalación de software compartido o no autorizado.	

DSS05.02 Gestionar la seguridad de la red y las conexiones.	Establecer y mantener una política de seguridad para las conexiones tomando como base el análisis de riesgos y los requerimientos del negocio,	
	Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña.	
	Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.	
	Cifrar la información en tránsito de acuerdo con su clasificación.	
	Aplicar los protocolos de seguridad aprobados a las conexiones de red.	
	Configurar los equipos de red de forma segura.	
	Establecer mecanismos de confianza para apoyar transmisión y recepción segura de información.	
	Realizar pruebas de intrusión periódicas para determinar la adecuación protección de la red.	
	Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación protección del sistema.	
DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Configurar los sistemas operativos de forma segura.	
	Implementar mecanismos de bloqueo de dispositivos.	
	Cifrar la información almacenada de acuerdo a su clasificación.	
	Gestionar el acceso y control remoto.	
	Gestionar la configuración de la red de forma segura.	
	Implementar el filtrado del tráfico de la red en dispositivos de usuario final.	
	Proteger la integridad del sistema.	
	Proveer de protección física a los dispositivos de usuario final.	

	Deshacerse de los dispositivos de usuario final de forma segura.	
DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. Alineando la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos tomando como base los principios de menor privilegio, necesidad de tener y necesidad de conocer.	
	Identificar unívocamente todas las actividades de proceso de la información por roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos consistentemente, incluyendo roles definidos por el propio negocio en las aplicaciones de procesos de negocio.	
	Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación con aplicaciones usadas en procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.	
	Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.	
	Segregar y gestionar cuentas de usuario privilegiadas.	
	Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.	
	Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información por usuario.	
	Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible.	

DSS05.05 Gestionar el acceso físico a los activos de TI.	Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento. Las peticiones formales de acceso deben ser completadas y autorizadas por la dirección de la ubicación de TI, y guardado el registro de petición. Los formularios deberían identificar específicamente las áreas a las que el individuo tiene acceso concedido.	
	Asegurar que los perfiles de acceso están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en funciones de trabajo y responsabilidades.	
	Registrar y supervisar todos los puntos de entrada a las ubicaciones de TI. Registrar todos los visitantes de la ubicación, incluyendo contratistas y vendedores.	
	Instruir a todo el personal para mantener visible la identificación en todo momento. Prevenir la expedición de tarjetas o placas de identidad sin la autorización adecuada.	
	Escoltar a los visitantes en todo momento mientras estén en la ubicación. Si se encuentra a un individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, se deberá alertar al personal de seguridad.	
	Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores. Asegurar que los dispositivos registren el acceso y disparen una alama en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas llave, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos.	
	Realizar regularmente formación de concienciación de seguridad física.	
DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida, dentro, en y fuera de la empresa.	

	Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basados en el principio del menor privilegio, equilibrando riesgo y requerimientos de negocio.	
	Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones.	
	Establecer salvaguardas físicas apropiadas sobre formularios especiales y dispositivos sensibles.	
	Destruir la información sensible y proteger dispositivos de salida (por ejemplo, desmagnetizando soportes magnéticos, destruir físicamente dispositivos de memoria, poniendo trituradoras o papeleras cerradas disponibles para destruir formularios especiales y otros documentos confidenciales).	
DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Registrar los eventos relacionados con la seguridad, reportados por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo. Retenerla por un periodo apropiado para asistir en futuras investigaciones.	
	Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta conmensurada.	
	Revisar regularmente los registros de eventos para detectar incidentes potenciales.	
	Mantener un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales y asegurar que todos los empleados están concienciados de los requerimientos.	
	Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.	

Tabla 89: Evaluación de Actividades Específicas de Seguridad de Información

Se recomienda contar con al menos 80% de cumplimiento para esta evaluación, esto garantizará un adecuado nivel preliminar de desempeño para la organización en este

proceso y ayudar a conseguir una organización que gestione de forma adecuada su seguridad de información.

Lista de Tablas de la Guía Metodológica