Universidad de Buenos Aires

Facultad de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Título del Trabajo:

Diseño de un Plan Estratégico de Seguridad de la Información en una Organización Pública según COBIT 5

Autor:

Ing. Sergio Luis Correa Rovira

Tutor de Trabajo Final:

Mg. Marcia Maggiore

Año de presentación 2019

Cohorte del cursante 2015

Declaración jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Sergio Luis Correa Rovira
DNI 32.140.003

Resumen

Las organizaciones padecen con frecuencia ataques informáticos debido a diversas razones entre las que se pueden mencionar a modo de ejemplo ataques de denegación de servicio, phishing, descarga de software malicioso, ausencia de buenas prácticas de gestión, fugas de información debido a agentes externos o internos, etc. Las consecuencias de estos ataques pueden ser la pérdida, manipulación o problemas de disponibilidad de la información, penalidades por incumplimiento de legislaciones o hasta el cierre de la organización.

Las organizaciones están tomando conciencia sobre la seguridad de la información y los riesgos que implica no tener esta actividad en cuenta.

Para cumplir con todas estas exigencias existen marcos metodológicos que ayudan a gestionar y gobernar con mejores prácticas en distintas temáticas. COBIT 5[1] de ISACA[2] es un marco que hace foco en el gobierno y gestión de las tecnologías de la información.

El presente trabajo desarrolla los lineamientos para la definición de un Plan Estratégico de Seguridad de la Información en una organización pública, basado en COBIT 5. Abarca una parte teórica en la cual se describe dicho marco y otra donde se lo aplica en el desarrollo de los mencionados lineamientos para una organización pública. La implementación está fuera del alcance de este trabajo, pero se establece una serie de buenas prácticas y algunas tareas que pueden ayudar a completar este objetivo con éxito.

Palabras Clave:

Gestión y gobierno de la Seguridad de la Información, Seguridad de la Información, COBIT 5, ISACA, Plan Estratégico de Seguridad de la Información, Diseño de un Plan Estratégico de Seguridad de la Información

[1] COBIT 5 - Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa

[2] ISACA (del inglés Information Security Audit and Control Association), Asociación de Auditoría y Control de los Sistemas de Información)

Contenido:

Índice de Figuras

Índice de Tablas

Agradecimientos

Nómina de abreviaturas

- ASI, Agencia de Sistemas de Información de la Ciudad de Buenos Aires
- COBIT, Control Objectives for Information and related Technology
- GDPR, General Data Protection Regulation
- ISACA, Information System Audit and Control Association
- ISO/IEC, International Organization of Standardization/ International Electrotechnical Commission
- ITIL, Information Technology Information Library
- NIST, National Institute of Standards and Technology
- ONG, Organizaciones No Gubernamentales
- ONTI, Oficina Nacional de Tecnologías de la Información
- OSI, Oficina de Seguridad Informática
- PESI, Plan estratégico de Seguridad Informática
- SI, Seguridad de la Información
- SGSI, Sistema de Gestión de Seguridad de la Información
- TI, Tecnologías de la información

1. Introducción

1.1 Motivación del Trabajo

Una empresa es una organización que persigue como uno de sus fines generar utilidades. Una organización no necesariamente persigue este objetivo económico. Un grupo de personas que buscan un objetivo común se puede llamar organización[1], como las ONG, organizaciones sin fines de lucro que realizan actividades de interés social. Otro tipo de organizaciones son las públicas que brindan distintos servicios para mantener el orden social y poder ofrecer las condiciones para el desarrollo de los ciudadanos dentro de la sociedad. Existen múltiples servicios que éstas pueden entregar, entre los que se puede mencionar: la seguridad, la educación, la salud, el desarrollo social, etc.

Una organización pública, que en adelante se referenciará como organización, tienen las siguientes características [2]:

- Son controladas conforme a las leyes que reglamentan su ejercicio
- En teoría todos los ciudadanos tienen participación en ella
- Todos los ingresos que tienen son canalizados de acuerdo al presupuesto de cada una de ellas y de conformidad con sus objetivos.
- El Estado (federal, provincial o municipal), a través de los órganos de control, supervisa su funcionamiento.
- Este tipo de organización no interesa a la mayoría de los inversores, pero la sociedad no puede funcionar sin ellas.
- Puesto que no hay competencia, no hay una necesidad urgente para atender los deseos de los consumidores o para la innovación, lo cual aumenta el potencial de ineficiencia

Con el advenimiento de la tecnología, los servicios que ofrecen estas organizaciones se ven cada día más sumergidos en el ámbito de las TI. Los servicios que brindan suelen estar en aplicaciones accesibles por Internet y

pueden ser vulnerables si no se toman las correctas medidas de seguridad. Estos servicios pueden ayudar a hacer algún tipo de transacción, trámite o pedido de documentación. Además, algunos de ellos pueden ser internos a la organización como por ejemplo el correo electrónico, Intranet, bases de datos con información confidencial, servicios web[3], etc. El uso de las TI, por lo tanto, implica algunos riesgos:

- El incorrecto tratamiento de la información puede causar de manera voluntaria o involuntaria la pérdida o manipulación no autorizada de la misma.
- Debido a que hay tantos cambios tecnológicos suele suceder que las personas no están correctamente capacitadas para desempeñar su función. Los recursos que utilicen las TI deben están capacitados y tener las competencias necesarias.
- Los distintos ataques cibernéticos, como por ejemplo Ramsonmware[4] WannaCry[5] o Petya[6] (algunos de ellos desarrollados en 2017), las vulnerabilidades como por ejemplo KRACK[7], los ataques de denegación de servicio, etc. pueden afectar la disponibilidad de los servicios de TI.
- Existen distintas leyes que pueden aplicar según el tipo de información, en el lugar donde aplica, el grado de confidencialidad, etcétera. En Argentina rige la ley 25.326 [3], de Habeas Data[8], que protege los datos

[3] Un servicio web, o Web Service en inglés, es una tecnología que utiliza un conjunto de estándares y protocolos que sirven para intercambiar datos entre distintas aplicaciones en Internet, desarrolladas en diferentes lenguajes y se ejecutan en diferentes plataformas.

[4]Ramsonware es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado y pide un rescate a cambio de quitar esa restricción.

[5]WannaCry es un ataque ransomware que afectó gran cantidad de dispositivos en mayo del 2017. Estos ataques eran dirigidos al sistema operativo Windows de Microsoft y pedían un rescate con moneda Bitcoin.

[6]Petya es un ransomware descubierto en junio del 2017. Se esparce como troyano en la nube de Dropbox

[7] Es un ataque de repetición que afecta a las redes de Wifi WPA2 descubierto en 2016 pero publicado en octubre del 2017

[8] Ley 25.326 de Protección de Datos Personales. Extracto Artículo 1: Tiene por objeto la protección integral de los datos almacenados, ya sean públicos o privados para garantizar el derecho al honor y la intimidad de las personas, así como también el acceso sobre la información que sobre las mismas se registre, de acuerdo a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional

personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados. Existen distintas legislaciones dependiendo del país donde se encuentra y del tipo de información que se va a manipular, por ejemplo, la existencia de datos sensibles. El no cumplimiento de estas legislaciones puede implicar multas, causas penales, etcétera.

En este contexto, la seguridad de la información se vuelve cada día más relevante para las organizaciones, ya sean públicas o privadas, porque la pérdida de la información puede impactar negativamente dentro y fuera de las mismas.

Para lograr que las organizaciones públicas o privadas trabajen de la manera aceptada por los expertos en temas de seguridad de la información se necesita de una planificación con objetivos posibles y ordenados. La utilización de estándares internacionales puede lograr la mejora de la calidad de los servicios ofrecidos y agregar valor a la organización.

Para implementar las buenas prácticas se necesita de un gobierno que dirija, supervise y oriente a la organización y una gestión que planifique, ejecute, chequee y supervise los proyectos que se ejecutan.

Existen estándares internacionales que se basan en la experiencia y conocimiento adquirido en diversos temas. Por citar algunos ejemplos, una de estas normativas es COBIT 5 de ISACA que es un marco que basa su enfoque en la separación del gobierno y la gestión de las tecnologías de la información. Otro ejemplo es la ISO/IEC 27001[9][4], que es un estándar que hace foco en la gestión de la seguridad de la información.

El presente trabajo final de especialización aborda la problemática de la mejora de la calidad de los servicios ofrecidos por una organización

[9] Es un estándar para la seguridad de la información. Especifica los requisitos para establecer, implantar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI). Es un estándar publicado por International Organization for Standarization y por la International Electrotechnical Commision (ISO/IEC)

pública, enfocando dicha mejora sobre la seguridad de la información, la cual agrega valor a las organizaciones. La hipótesis del trabajo consiste en considerar que la adopción e implementación del marco COBIT 5 de ISACA ayuda a lograr la mejora planteada. En tal sentido, el objetivo de este trabajo es el de mostrar la experiencia realizada en una organización pública, definiendo un Plan Estratégico de Seguridad de la Información a partir de las premisas del mencionado estándar.

Debido a la necesidad de guardar la confidencialidad de la información de la organización que se toma como ejemplo, se ha evitado efectuar referencias que permitan identificarla.

1.2 Objetivo del Trabajo

Elaborar un Plan Estratégico de Seguridad de la Información basado en el marco metodológico COBIT 5 que sirva como base fundamental para mejorar la postura de Seguridad de la Información en la Organización.

1.2.1 Objetivos Específicos

- Describir el marco metodológico COBIT 5
- Describir el contexto organizacional donde se aplicará el mencionado plan
- Establecer un plan de acción o ruta de las actividades que deben ser realizadas para llevar a cabo un Plan Estratégico de Seguridad de la Información en función de la normativa COBIT 5.

1.3 Estructura del Trabajo

Capítulo 1: Introducción

Establece las motivaciones por las cuales las organizaciones deben tener en cuenta la seguridad de la información. Establece el contexto en el cual las organizaciones se desenvuelven y contiene una breve descripción de las organizaciones públicas y los objetivos que persiguen.

Capítulo 2: Descripción de la Organización

Describe la organización, el contexto de la misma y su estructura organizacional con los distintos departamentos.

Capítulo 3: ¿Por qué elegir un estándar o regulación para gestionar la organización?

Expone el marco legislativo de Argentina en el que se desenvuelve la organización. Explica diversos marcos metodológicos y la elección de COBIT 5 como metodología.

Capítulo 4: Objetivo y alcance de COBIT 5

Explica el marco teórico de COBIT 5, los objetivos y los principios en los cuales se basa este marco metodológico.

Capítulo 5: Evaluación de la Capacidad de procesos

Expone el modelo de capacidad de procesos en el cual se basa COBIT 5 para comprender los resultados que se obtuvieron de un informe previo al armado del Plan Estratégico de Seguridad de la Información.

Capítulo 6: Plan Estratégico de Seguridad de la Información (PESI)

Contiene la ruta de las actividades que deben ser realizadas para elaborar el Plan Estratégico de Seguridad de la Información (PESI). Enumera cada uno de los principios de COBIT y detalla cómo mapear los conceptos con el PESI.

Capítulo 7: Implementación

Describe los puntos claves para tener en cuenta a la hora de implementar un PESI.

Capítulo 8: Conclusiones

Las conclusiones del trabajo de tesis de especialización. Describe los aportes realizados y oportunidades de mejora para futuros trabajos.

Capítulo 9: Apéndice

El apéndice contiene un plan de implementación de un SGSI como ejemplo de los procesos que se deben definir e implementar para llevar a cabo el PESI con éxito.

Capítulo 10: Bibliografía

Contiene toda la bibliografía en la cual se basó este trabajo.

2. Descripción de la Organización

La Organización en la que se basa el presente trabajo es de un tamaño relativamente grande ya que tiene más de 3.000 empleados que trabajan de manera directa con los servicios que brinda.

El gobierno de la Organización está formado por un Consejo Directivo de 9 miembros, de los cuales algunos son elegidos por el voto de otros integrantes de la organización y el resto por órganos externos. Entre sus funciones está dirigir, orientar, supervisar y controlar la organización.

Los miembros del Consejo Directivo permanecen 4 años en sus funciones y no pueden ser reelegidos por periodos consecutivos. El mencionado consejo elige un Presidente quien, además, es el que representa legalmente a la Organización.

Se cuenta con distintos departamentos para brindar apoyo y lograr las metas de la organización. Entre estos se puede mencionar el área de recursos humanos, operaciones, logística, compras, legales e informática.

Tiene empleados que están contratados bajo diferentes modalidades, muchos de los cuales trabajan de manera full time. Al mismo tiempo, hay empleados que trabajan de manera part-time.

La infraestructura de comunicaciones está compuesta por una red propia y otra contratada que da soporte a varios edificios ubicados en distintos puntos geográficos del país, así como por servicios que se brindan a través de internet.

La forma de contratación de los servicios informáticos, ya sea recursos especializados de TI, software o hardware puede ser directa, solo con la aprobación de uno o varios directivos hasta un determinado monto o por licitación pública, para montos mayores o cuando los proyectos son estratégicos.

Este trabajo se va a centrar en el área de TI ya que es la que definió un Plan Estratégico de Seguridad de la Información (PESI).

2.1 Estructura Organizacional del área de TI

El área de TI está compuesta por la Dirección de Informática y las jefaturas que de ella dependen. Las jefaturas, en algunos casos, están conformadas por departamentos.

A continuación, se describen las funciones de las distintas jefaturas:

- Mesa de ayuda es la jefatura que se encarga de brindar asistencia a los usuarios para el equipamiento tecnológico, servicios o aplicaciones. Consta de personal para dar distintos niveles de soporte y herramientas para gestión de tickets. Posee un soporte telefónico de primer nivel y luego un servicio de segundo nivel con personal con mayor conocimiento técnico para dar soporte telefónico o en el lugar físico
- Soporte de Redes es la jefatura encargada de mantener los servicios de redes y el mantenimiento de los centros de cómputos. Es la encargada de monitorear y mantener los servicios de red de los distintos edificios de acuerdo a los niveles de servicio establecidos.
- Planificación e Infraestructura es la jefatura encargada de gestionar y planificar las compras desde licencias de software hasta los servicios contratados de mantenimiento de centros de cómputos y aires acondicionados. Se encarga de dar servicio a los usuarios si necesitan equipamiento o acondicionar algún espacio.
- Soporte de Aplicaciones es la jefatura encargada de crear, modificar y mantener las aplicaciones de la Organización. Es responsabilidad de esta área mantener las bases de datos y realizar mejoras a determinadas aplicaciones. Tiene a su cargo distintos entornos de trabajo de producción, desarrollo y pruebas de aplicaciones y hay distintos especialistas dependiendo del lenguaje de programación o tipo de bases de datos.
- Gestión Estratégica es la jefatura encargada de planificar las tareas estratégicas para la Dirección. Parte de su función es estar en contacto

constantemente con las distintas jefaturas para determinar oportunidades de mejora de servicio.

- Seguridad de la Información, dependiente de la jefatura de Gestión Estratégica, es la oficina encargada de gestionar y ejecutar el plan estratégico de seguridad de la información (PESI). Entre sus responsabilidades se encuentra mantener la confidencialidad de la información, desarrollar políticas de seguridad de la información, definir procedimientos y estrategias para mantener la integridad y la disponibilidad de la información y de los servicios

En la siguiente figura se muestra el organigrama actual de la organización:

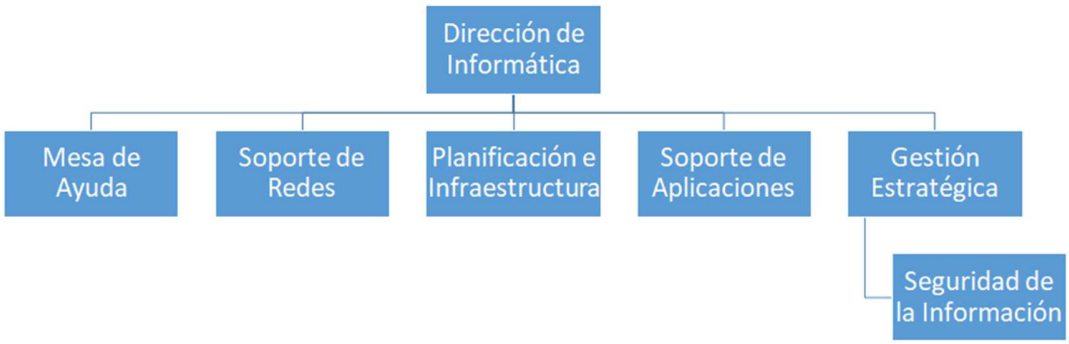

Figura 1- Organigrama de la Organización

3. ¿Por qué elegir un estándar o regulación para gestionar la organización?

Una organización, ya sea del sector gubernamental o privada, debe establecer una forma de trabajo para gobernar y gestionar los servicios que ofrece. Existen distintas maneras de gestionar los recursos de una organización, distintas estructuras organizacionales, diferentes procesos y servicios que se deben cumplir.

Las organizaciones deben adecuarse al contexto en el cual se desarrollan. Esto requiere adaptarse a diversas normativas o regulaciones.

En Argentina hay algunos marcos legales que deben ser cumplidos, desde la Constitución Nacional hasta leyes que aplican a diferentes industrias, actividades, objetos, grupos sociales, etc. En este contexto aplica la ley de habeas data (Ley 25.326) [3], la ley de delitos informáticos (Ley 26.388) [5] y la Ley de Propiedad Intelectual (Ley 11.723) [16] y sus modificatorias.

Además, hay estándares que son referencias internacionales que cubren distintos ámbitos. Temas como la arquitectura física de los centros de cómputos pueden ser cubiertos, por ejemplo, por la normativa ANSI/TIA 942 [6]. Dependiendo del tipo de centro de cómputos (tamaño, tipo de información, entre otras características), hay distintas categorías para definir el nivel de redundancia, el diseño la distribución física de los equipos, aires acondicionados, arquitectura, etc.

Por último, son fundamentales las cuestiones relacionadas con la cultura y la ética organizacional, el comportamiento y el liderazgo, así como las habilidades, competencias y motivación de las personas.

Es por esto que es importante recurrir a marcos metodológicos de trabajo que tienen en consideración estos temas y establecen las mejores prácticas para tener en cuenta desde los aspectos legales o normativos, los aspectos culturales y éticos de la organización hasta aspectos técnicos que se deben cumplir, por ejemplo, por una limitación tecnológica.

Cuando se estudió la factibilidad de definir un Plan Estratégico de Seguridad de la Información, se consideraron diversos marcos de trabajo. En un comienzo solo se consideró la normativa ISO/IEC 27001 [4]. ISO es un organismo de normalización internacionalmente reconocido. Están involucrados en él más de 160 países, trabajan a nivel de comités técnicos y tienen al menos 19.000 estándares publicados. El estándar ISO/IEC 27001 es la norma principal de la serie ISO/IEC 27000 y contiene los requisitos para establecer un SGSI. Es una norma certificable para las empresas, está conformada por 10 capítulos y especifica los lineamientos necesarios para

evaluar todo tipo de riesgos y amenazas susceptibles de poner en peligro la información de la organización. Establece además los controles y estrategias adecuadas para eliminar dichos peligros. Tiene un enfoque basado en el ciclo de mejora continua de Deming[10] (planear, hacer, ejecutar y actuar).

Además de la serie ISO/IEC 27000, se consideró el marco COBIT 5 que ayuda a generar valor a partir de las TI y además incluye el estándar mencionado anteriormente como norma a utilizar en la implementación de los procesos relacionados con la seguridad de la información. COBIT 5 ayuda a separar el gobierno de la gestión de las TI y mantiene un equilibrio entre la realización de beneficios, la optimización de los niveles de riesgo y la utilización de los recursos. Este marco normativo se describe a continuación.

El 14 de noviembre de 2018 se publicó una extensión de la normativa COBIT 5, llamada COBIT 2019 [7]. COBIT 2019 es una extensión de COBIT 5 [8]. A continuación, se muestra la secuencia cronológica de COBIT.

[10]William Edwards Deming (14 de octubre de 1900-20 de diciembre de 1993) fue un estadístico estadounidense, profesor universitario, autor de textos, consultor y difusor del concepto de calidad total. Su nombre está asociado al desarrollo y crecimiento de Japón después de la segunda guerra mundial.

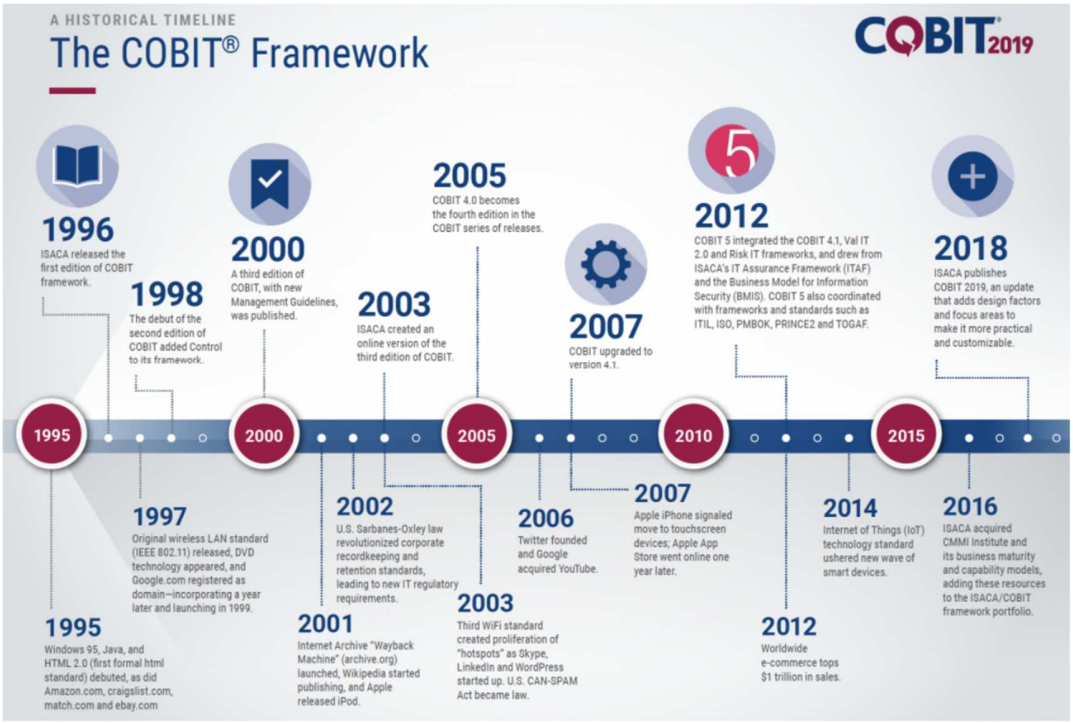

Figura 2- Cronología de COBIT – Fuente: ISACA - COBIT 2019

Esta nueva normativa no es un reemplazo de COBIT 5, es una actualización del marco normativo. Seguirán conviviendo en paralelo COBIT 5 y COBIT 2019. Las nuevas características de este marco, entre otras, incluyen un sistema personalizable de gobierno, la diferenciación entre el sistema de gobierno y el marco de gobierno y la actualización de los principios, procesos y metas en cascada.

COBIT 5 permanece vigente y es por este motivo que se continúa con este marco metodológico. Eventualmente, en futuras mejoras, se puede incorporar COBIT 2019.

4. Objetivo y alcance de COBIT 5

COBIT 5 es una normativa que permite a las organizaciones basarse en un marco de trabajo integral. Ayuda a las organizaciones a lograr sus metas y entregar valor mediante el gobierno y la gestión de las TI. Permite que las mismas se administren de manera holística a nivel de toda la

organización incluyendo todas las áreas de responsabilidad funcional y de negocios, considerando los intereses internos y externos relacionados con la TI. [9][10][11].

COBIT 5 se basa en 5 principios que son genéricos y útiles para las organizaciones de cualquier tamaño, ya sean comerciales, sin fines de lucro o del sector público**.** Ellos son:

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

A continuación, se explicará en detalle cada uno de estos principios

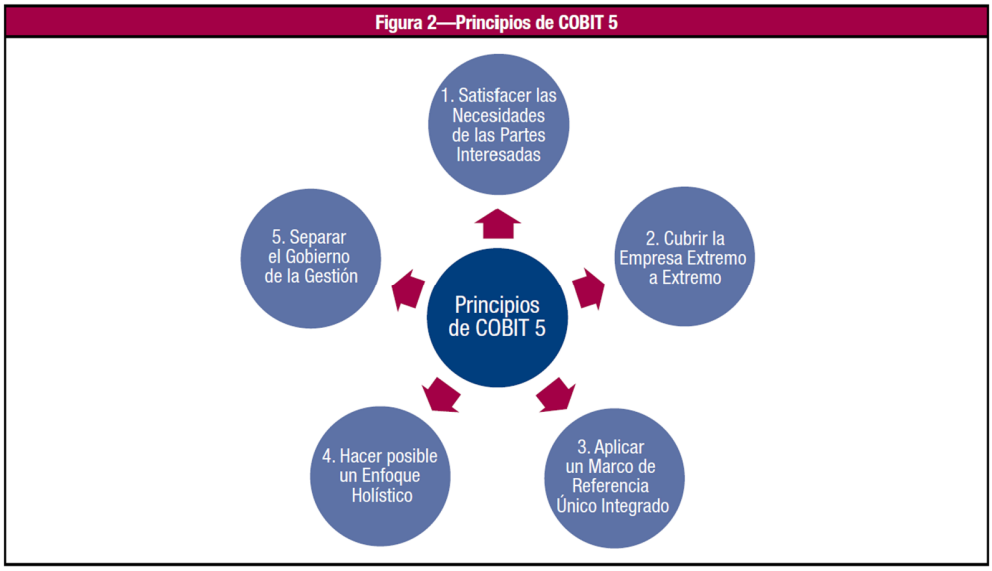

Figura 3- Principios de COBIT 5 – Fuente: COBIT 5 – Un Marco de Negocio para el Gobierno y la Gestión de las TI en la Empresa

4.1. Principio 1: Satisfacer las necesidades de las partes interesadas

Las organizaciones tienen como objetivo crear valor para sus partes interesadas

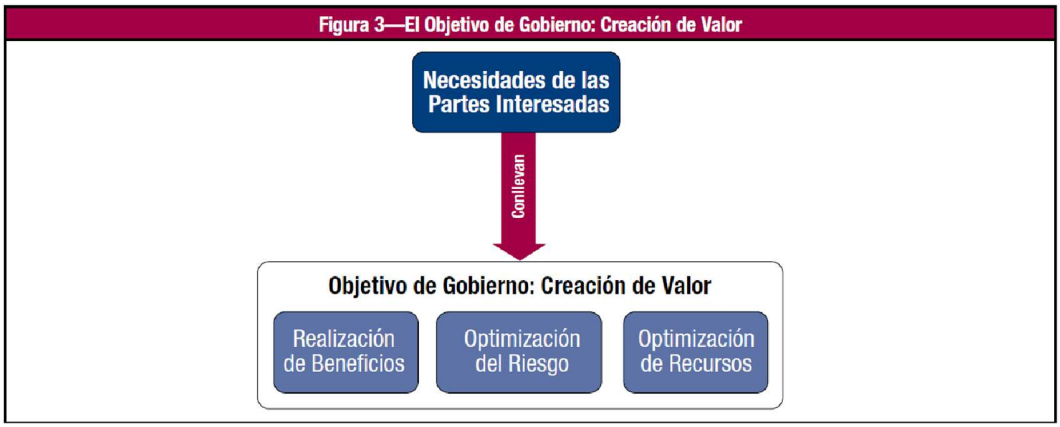

Figura 4- El Objetivo de Gobierno: Creación de Valor - Fuente: COBIT 5 – Un Marco de Negocio para el Gobierno y la Gestión de las TI en la Empresa

La organización tiene distintos actores con diferentes intereses, muchas veces generadores de conflicto entre ellos. El gobierno debe tener la capacidad de negociar entre los distintos intereses para poder aumentar el beneficio, optimizando el riesgo y los recursos.

Las necesidades de la organización deben ser transformadas en una estrategia accionable. Para esto, COBIT 5 establece una serie de metas en cascada que traducen las necesidades de las distintas partes interesadas en metas específicas, accionables y personalizadas dentro del contexto de la organización. Desde las metas de la organización hasta las relacionadas con las TI y metas habilitadoras. Permite establecer las prioridades para implementar, mejorar y asegurar el gobierno corporativo de la TI, en base de los objetivos (estratégicos) de la organización y los riesgos relacionados [9].

4.2. Principio 2: Cubrir la compañía de forma integral

El marco de COBIT 5 tiene una perspectiva del gobierno y la administración de las TI, relacionadas de forma integral a toda la organización. Esto implica que:

- El gobierno de las TI se integra con el gobierno corporativo alineando las visiones del gobierno de la organización
- Se consideran todas las funciones y procesos dentro de la organización. No solamente los relacionados con las TI.

4.3. Principio 3: Aplicar un solo marco integrado

COBIT 5 puede ser implementado como un marco de referencia único e integrado porque se alinea con otros estándares y marcos de referencia relevantes. Se pueden mencionar a modo de ejemplo:

- A nivel corporativo: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000
- Relacionado con TI: ISO/IEC 38500, ITIL, la serie ISO/IEC 27000, TOGAF, PMBOK/PRINCE2, CMMI

Ser un marco integrado con otras normativas fue uno de los disparadores para elegir COBIT 5. El requerimiento inicial de la dirección de informática fue trabajar con ISO/IEC 27001 y el marco normativo de COBIT 5 no solo permite trabajar con esta normativa, sino que además puede incluir otras metodologías de trabajo y estándares.

4.4. Principio 4: Habilitar un enfoque holístico

Se requiere para un gobierno y gestión de las TI efectivo y eficiente que se tenga en consideración un enfoque holístico en el cual varios componentes o procesos interactúan juntos o por separado.

COBIT 5 define un conjunto de catalizadores o habilitadores que son factores que individual o colectivamente, influyen sobre si algo funcionará [12]. En líneas generales, son factores que influyen para conseguir las metas de la organización. Los catalizadores están divididos en 7 categorías:

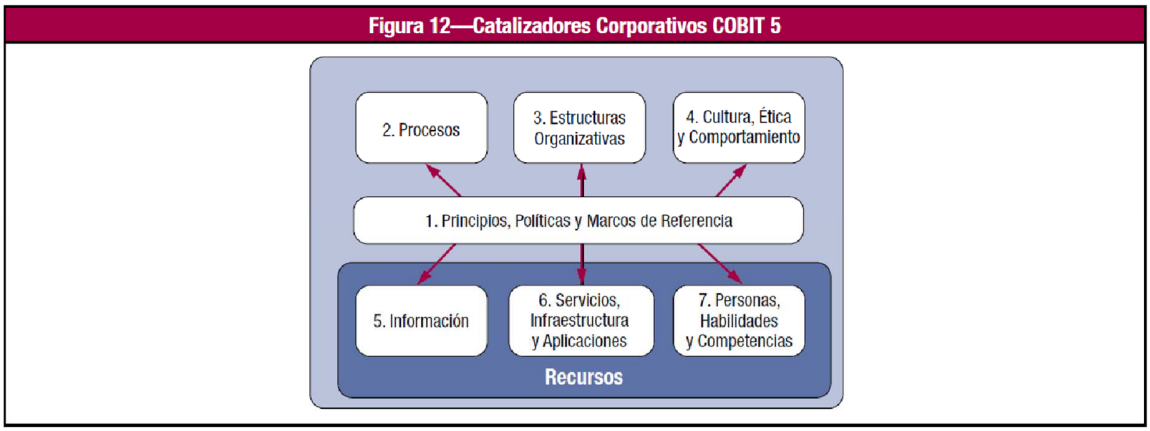

Figura 5- Catalizadores o Habilitadores de COBIT 5 - Fuente: COBIT 5 – Un Marco de Negocio para el Gobierno y la Gestión de las TI en la Empresa

1. *Principios, políticas y marcos de referencia* son el vehículo para traducir el comportamiento deseado en guías prácticas de la gestión del día a día.

2. Los *procesos* describen un conjunto organizado de prácticas y actividades para alcanzar objetivos y producir un conjunto de resultados que soportan las metas relacionadas con TI.

3. Las *estructuras organizativas* son entidades que cumplen diferentes roles tales como tomar decisiones, influenciar y asesorar y cuyas metas incluyen un mandato adecuado, principios operativos bien definidos y la aplicación de buenas prácticas.

4. La *cultura, ética y comportamiento* de los individuos de la organización son un factor de éxito determinante en las actividades de gobierno y gestión.

5. La *información* abarca a toda la organización e incluye toda la información producida y utilizada por ella. La información es necesaria para mantener la organización funcionando y bien gobernada, pero a nivel operativo, la información es a menudo el producto clave en sí mismo.

6. Los *servicios de infraestructura y aplicaciones* incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la organización, servicios y tecnologías de procesamiento de la información.

7. Las *personas, habilidades y competencias* están relacionadas con las personas y son necesarias para poder completar todas las actividades y para tomar decisiones adecuadas y ejecutar las acciones correctivas.

4.5. Principio 5: Separar el gobierno de la gestión

COBIT 5 realiza una distinción entre gobierno y gestión. Estas disciplinas engloban diferentes tipos de actividades, requieren estructuras organizativas diferentes y sirven para diferentes propósitos

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 y el cumplimiento respecto a la dirección y metas acordadas[11]

La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales[12]

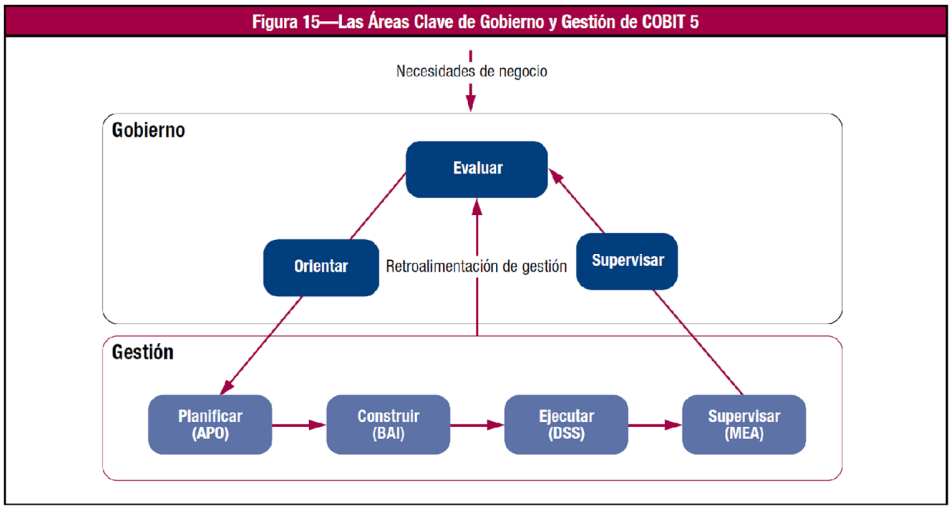

Figura 6- Las áreas Clave de Gobierno y Gestión de COBIT 5 - Fuente: COBIT 5 – Un Marco de Negocio para el Gobierno y la Gestión de las TI en la Empresa

[11] Definición de Gobierno extraída de COBIT 5 Un Marco de Negocio para el Gobierno y Gestión de las TI de la Empresa- Página 14

[12] Definición de Gestión extraída de COBIT 5 Un Marco de Negocio para el Gobierno y Gestión de las TI de la Empresa- Página 14

El modelo de referencia de COBIT 5 divide los procesos de gobierno y gestión de la TI empresarial en dos dominios principales de procesos:

- Gobierno, contiene cinco procesos de gobierno; dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión (EDM por sus siglas en inglés)
- Gestión, contiene 4 dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar (PBRM por sus siglas en inglés) y proporciona cobertura de extremo a extremo de las TI.

En la Figura 7 se puede observar los distintos procesos habilitadores del gobierno y la gestión.

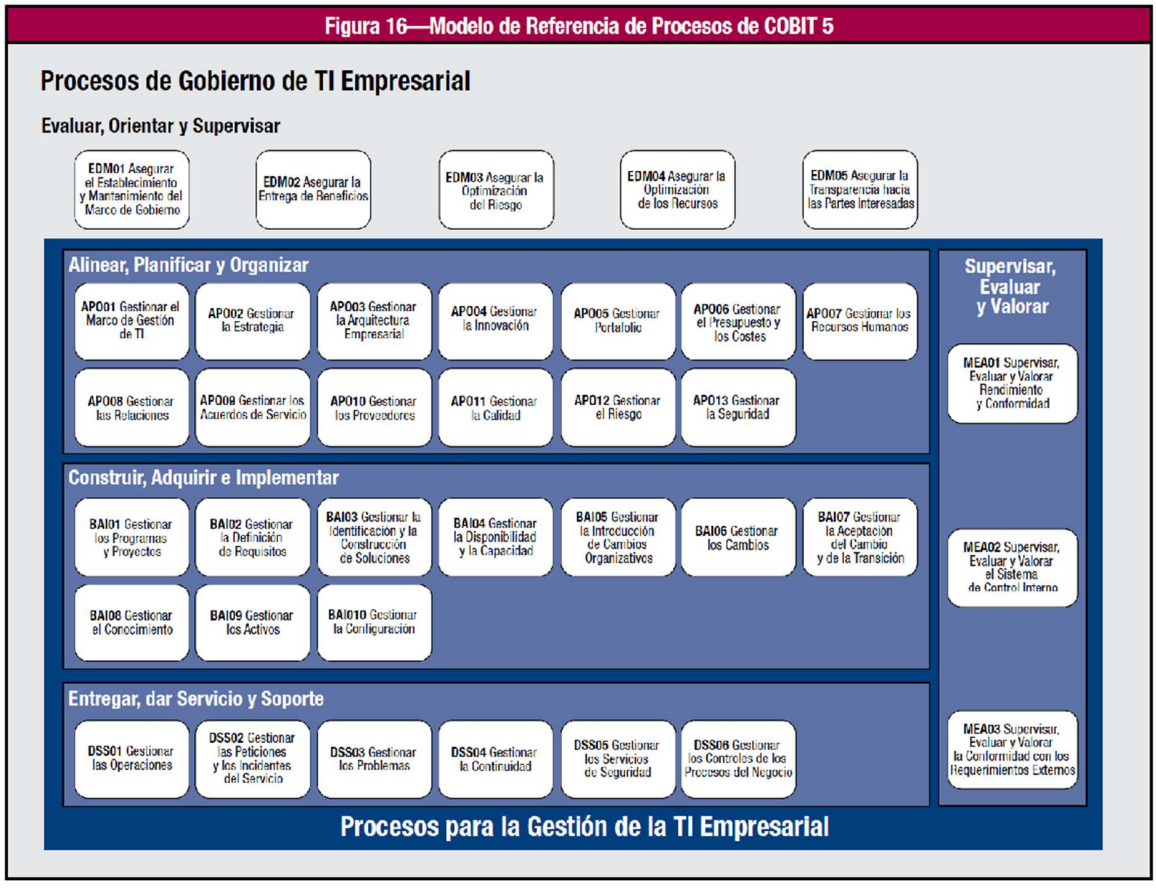

Figura 7- Modelo de Referencia de Procesos de COBIT 5 - Fuente: COBIT 5 – Un Marco de Negocio para el Gobierno y la Gestión de las TI en la Empresa

5. Evaluación de capacidad de los procesos

Un modelo de capacidad de los procesos es un medio para medir el desempeño de cualquiera de los procesos de gobierno y gestión. Esta medición ayuda a identificar áreas de mejora de una organización. Está basado en la normativa ISO/IEC 15504[13]y permite:

- Obtener un sistema de medición único aplicable a todos los procesos de la organización.
- Comparar la organización con otras entidades externas de acuerdo a estándares internacionales
- Diagnosticar el nivel de capacidad en el que se encuentra cada proceso y qué debemos realizar para alcanzar el nivel deseado

Una mejora en la capacidad de los procesos ayuda a mejorar la efectividad y la eficiencia de la organización. Además, ayuda a determinar las fortalezas y debilidades de un proceso seleccionado con respecto a un requerimiento particular.

A continuación, se explica brevemente el proceso de evaluación de la capacidad de procesos.

5.1. Modelo de Capacidad de procesos de COBIT 5

El proceso de evaluación de capacidad de procesos implica establecer una clasificación de la capacidad para cada proceso dentro de la organización[14]. Esto considera:

- Niveles de capacidad definidos (ver figura 8)
- Atributos de proceso, utilizado para evaluar cada proceso (ver figura 9)
- Indicadores de evaluación para cada proceso
- Una clasificación estándar

Los niveles de capacidad de proceso se pueden ver a continuación:

Figura 1. Niveles de capacidades de procesos	
Nivel de proceso	**Capacidad**
0 (Incompleto)	El proceso no se ha implementado o no logra su propósito. En este nivel, hay evidencia escasa o nula de un logro sistemático del propósito del proceso.
1 (Realizado)	El proceso implementado logra su propósito.
2 (Gestionado)	El proceso realizado ahora se implementa de manera gestionada (planificada, supervisada y ajustada) y sus productos de trabajo se establecen, controlan y mantienen de forma apropiada.
3 (Establecido)	El proceso gestionado ahora se implementa mediante un proceso definido que es capaz de lograr los resultados del proceso.
4 (Predecible)	El proceso establecido ahora opera dentro de los límites definidos para lograr los resultados del proceso.
5 (Optimización)	El proceso predecible se mejora continuamente para cumplir con las metas del negocio, tanto actuales como proyectadas.
Fuente: ISACA, *Guía de Auto-Evaluación: Usando COBIT 5*, EE. UU., 2013	

Figura 8- Niveles de Capacidades de Procesos - Fuente: ISACA, Guía de Auto-Evaluación: Usando COBIT 5, EE. UU., 2013

La siguiente figura incluye los atributos de proceso para cada nivel de capacidad:

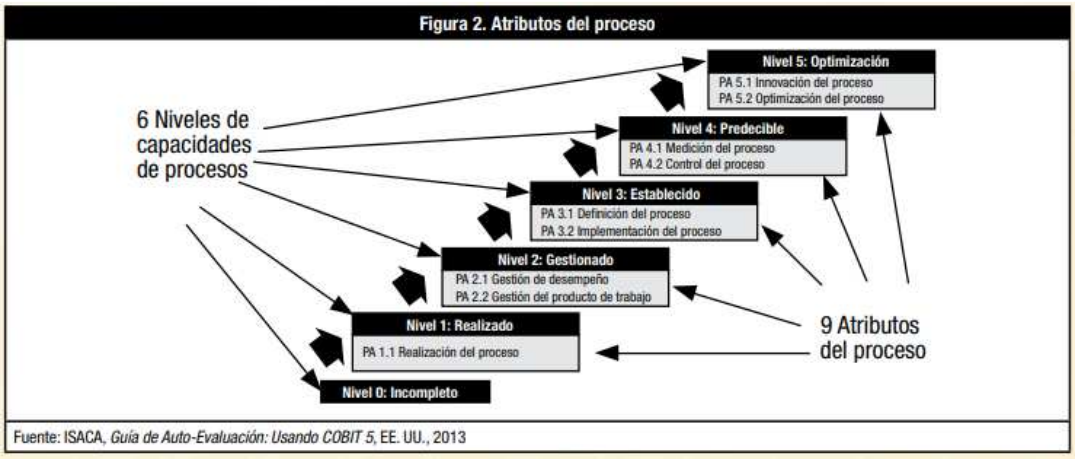

Figura 9- Atributos del proceso - Fuente: ISACA, Guía de Auto-Evaluación: Usando COBIT 5, EE. UU., 2013

Los indicadores de evaluación se utilizan para determinar si los atributos de proceso (PA) han conseguido su objetivo. Los atributos se analizan desde el nivel 1 y una vez que un atributo se cumple, pueden ser analizados los atributos de los niveles superiores. De esta forma se determina el nivel de capacidad de procesos. Para determinar el nivel en el

que se encuentra el proceso, es necesario comprobar que cumple con lo requerido por los atributos de ese nivel.

En la figura siguiente, se muestra cómo se relaciona el modelo de capacidad de procesos con COBIT 5.

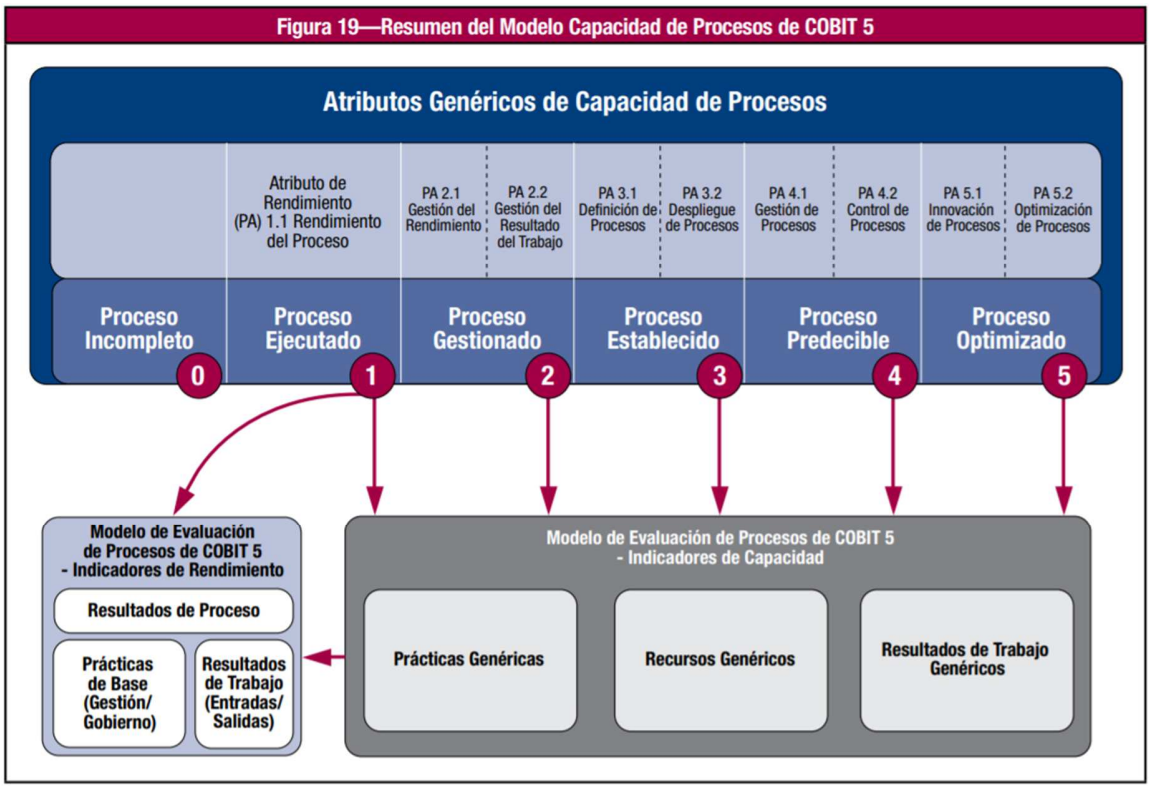

Figura 10- Modelo de Capacidad de Procesos de COBIT 5 - Fuente: COBIT 5 – Un Marco de Negocio para el Gobierno y la Gestión de las TI en la Empresa

6. Plan Estratégico de Seguridad de la Información (PESI)

A continuación, se establecen los lineamientos para la definición de un Plan Estratégico de Seguridad de la Información para la Organización basado en el marco COBIT 5. El capítulo se estructura según los principios y habilitadores de la norma.

6.1. Satisfacer las necesidades de las partes interesadas

Las empresas se crean con el objetivo de obtener un beneficio realizando determinada actividad o servicio. Las organizaciones, como pueden ser las ONG o las organizaciones públicas tienen un fin social. Pueden tener como objetivo, por ejemplo, defender a las minorías, proteger a los ciudadanos y/o brindar un servicio público de calidad. Si bien los objetivos de la empresa o la organización suelen ser claros, dentro de la misma cambian los intereses según las partes interesadas.

El marco COBIT 5 propone definir metas en cascada para la Organización, desde las necesidades de las partes interesadas hasta las metas de TI, lo cual permite establecer metas específicas en todos los niveles y en todas las áreas, en apoyo de los objetivos del negocio. Para ello, se deben conocer las necesidades de las distintas partes interesadas para entender dónde hay conflicto de intereses y así poder definir y alinear las metas de TI con los objetivos del negocio [15].

En la siguiente tabla se identifican a nivel general las partes interesadas:

Tabla 1- Distintas Partes Interesadas dentro de la Organización

Nro.	Parte Interesada	Tipo de Parte Interesada	Necesidades
1	Presidente de la organización y Consejo Directivo	Interno	- Dirigir la organización hacia la excelencia - Mejorar el uso de los recursos - Supervisar el trabajo de la organización

			- Cumplimiento de leyes y regulaciones internas - Entregar un servicio de calidad. - Gestionar los riesgos
2	Directores de la organización	Interno	- Entregar un servicio de calidad. - Cumplir con el presupuesto asignado - Gestionar los riesgos
3	Entidades Auditoras	Externo	- Transparencia en los procesos
4	Otras Entidades Gubernamentales	Externo	- Cumplimiento de la legislación. - Transparencia de los Procesos
5	Empleados (empleados de planta permanente dentro de la organización, dentro del convenio de trabajo)	Interno	- Seguridad Laboral - Cobrar el sueldo en tiempo y forma - Balance vida laboral/vida familiar
6	Contratados (empleados con contrato de trabajo)	Externo	- Seguridad Laboral - Reconocimiento del trabajo realizado. - Ser empleados planta permanente en la organización - Cobrar el trabajo realizado en tiempo y forma
7	Ciudadanos	Externo	- Recibir un servicio de calidad, que cumpla con los tiempos y resultados esperados.
8	Proveedores	Externo	- Cobrar por el servicio brindado. - Brindar un servicio de calidad. - Aumentar las ganancias en sus estados contables. - Establecer contratos a largo plazo con la organización

En las organizaciones públicas, los clientes principales son los ciudadanos, y brindarles un buen servicio no es una tarea sencilla. La entidad debe tener la capacidad de atender los pedidos que ellos realicen y de resolverlos en el tiempo adecuado.

El gobierno de la Organización descrita, ejercido por la Presidencia y el Consejo Directivo, debe tener la capacidad de entender los conflictos de intereses que existen entre las distintas partes y debe priorizarlos para tener una visión objetiva de las metas a alcanzar.

Con las necesidades de las distintas partes interesadas, es posible identificar las metas de la Organización y así poder lograrlas.

COBIT 5 propone 17 metas genéricas en las cuales se pueden traducir las necesidades de las organizaciones. Desde el punto de vista de la Organización que se está analizando, solo se tuvieron en cuenta las consideradas más relevantes. A continuación, se exponen las distintas necesidades de las partes interesadas en relación con las metas organizacionales que permitirían cumplir con dichas necesidades.

Tabla 2- Metas de la Organización

Nro.	Parte Interesada	Necesidades	Metas de la Organización	Prioridad
1	Presidente de la Organización y Consejo Directivo	- Dirigir la organización hacia la excelencia - Mejorar el uso de los recursos - Supervisar el trabajo de la organización - Cumplimiento de leyes y regulaciones internas - Entregar un servicio de calidad. - Gestionar los riesgos	- Valor para las partes Interesadas de las Inversiones del Negocio - Cartera de productos y servicios de calidad - Cumplimiento de leyes y regulaciones externas - Transparencia financiera - Riesgos del Negocio Gestionados - Cultura de servicio orientada a los ciudadanos	Primaria
2	Directores de la Organización	- Entregar un servicio de calidad - Cumplir con el presupuesto asignado	- Cultura de servicio orientada al cliente - Optimización de los costes de los procesos de negocio	Primaria

		- Gestionar los riesgos	- Riesgos de la organización gestionados	
3	Entidades Auditoras	- Transparencia en los procesos	- Cumplimiento de leyes y regulaciones externas - Transparencia financiera	Primaria
4	Entidades Gubernamentales	- Cumplimiento de la legislación. - Transparencia de los Procesos	- Cumplimiento de leyes y regulaciones externas - Transparencia financiera	Primaria
5	Empleados (empleados de planta permanente dentro de la organización, dentro del convenio de trabajo)	- Seguridad Laboral - Pagar en sueldos en tiempo y forma - Balance vida laboral/vida familiar	- Personas preparadas y motivadas -Cumplimiento con las políticas internas - Productividad operacional y de los empleados	Primaria
6	Contratados (empleados con contrato de trabajo)	- Seguridad Laboral - Reconocimiento del trabajo realizado. - Ser empleados planta permanente en la organización	- Personas preparadas y motivadas	Secundaria
7	Ciudadanos	- Recibir un servicio de calidad, que cumpla con los tiempos y resultados esperados.	- Cultura de servicio orientada al cliente - Continuidad y disponibilidad del servicio de negocio	Primaria
8	Proveedores	- Cobrar por el servicio brindado. - Brindar un servicio de	- Personas preparadas y motivadas - Cartera de productos y	Secundaria

		calidad. - Aumentar las ganancias en sus estados contables. - Establecer contratos a largo plazo con la organización	servicios competitivos	

Para el caso en análisis, se tuvieron en cuenta 12 de las metas de la Organización, las cuales se relacionaron con metas específicas de TI, obteniendo la tabla que se muestra a continuación.

Tabla 3- Metas de TI

Nro.	Metas de la Organización	Metas de TI	Prioridad
1	Valor para las partes Interesadas de las Inversiones del Negocio	ITRG01[13] Alineamiento de TI y estrategia del negocio ITRG03 Compromiso de la Dirección ejecutiva para tomar decisiones relacionadas con TI	Primaria
2	Cartera de productos y servicios de calidad	ITRG01 Alineamiento de TI y estrategia del negocio ITRG07 Entrega de servicios de TI de acuerdo a los requisitos del negocio ITRG13 Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	Primaria
3	Riesgos de la organización gestionados	ITRG04 Riesgos del negocio relacionado con las TI	Primaria

[13] ITRG, del inglés Information Technology Related Goals. En COBIT 5 se establecieron una serie de 17 metas de TI genéricas, que aplican a cualquier organización, para conseguir los objetivos empresariales.

		gestionados	
4	Cumplimiento de leyes y regulaciones externas	ITRG02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Primaria
5	Transparencia financiera	ITRG06 Transparencia de los costes, beneficios y riesgos de las TI	Secundaria
6	Cultura de servicio orientada al cliente	ITRG07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	Secundaria
7	Continuidad y disponibilidad del servicio de negocio	ITRG08 Uso adecuado de aplicaciones, información y soluciones tecnológicas ITRG10 Seguridad de la Información, infraestructura de procesamiento y aplicaciones	Primaria
12	Optimización de los costes de los procesos de negocio	ITRG01 Alineamiento de TI y estrategia del negocio ITRG03 Compromiso de la Dirección ejecutiva para tomar decisiones relacionadas con TI ITRG06 Transparencia de los costes, beneficios y riesgos de las TI ITRG11 Optimización de activos, recursos y capacidades de las TI	Secundaria
15	Cumplimiento de las políticas internas	ITRG02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas ITRG10 Seguridad de la Información, infraestructura de	Primaria

		procesamiento y aplicaciones ITRG15 Cumplimiento de las políticas internas por parte de las TI	
16	Personas preparadas y motivadas	ITRG01 Alineamiento de TI y estrategia del negocio ITRG16 Personal del negocio y de las TI competente y motivado	Primaria

El cumplimiento de las metas de TI permite el logro de las metas organizacionales. Para poder visualizar el cumplimiento de estos objetivos, es necesario establecer una serie de métricas que ayuden a observar su evolución permitiendo así que el gobierno de TI puede tomar decisiones basadas en esta información. La información ha sido agrupada utilizando el cuadro de mando integral (CMI) o en inglés Balanced Score Card (BSC) desarrollado por Robert Kaplan y David Norton[14]. La tabla siguiente identifica algunas métricas para cumplir con los objetivos:

Tabla 4- Establecimiento de Métricas en Función de las Necesidades de TI

Nr	Dimensión CMI	Necesidad de TI	Métricas
1	Financiera	ITRG01Alineamiento de TI y estrategia del negocio	- Porcentaje de metas estratégicas alineados con metas de TI estratégicas - Nivel de satisfacción de las partes interesadas con los servicios brindados - Porcentaje de objetivos de TI alineados con el negocio
2	Financiera	ITRG02	- Coste de incumplimientos de TI

[14] Es un sistema de control de gestión introducido en el ámbito empresarial, diseñado para permitir a las empresas monitorizar sus estrategias. Se divide en varias categorías: Desarrollo y aprendizaje, Interna del negocio, del cliente y financiera. Estas 4 categorías ayudan a monitorizar si la empresa va a cumplir sus metas estratégicas.

		Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Número de incumplimientos de TI reportados - Número de incumplimiento relacionados con proveedores de servicio
3	Financiera	ITRG03 Compromiso de la Dirección ejecutiva para tomar decisiones relacionadas con TI	- Frecuencia de las reuniones del consejo directivo - Número de veces que TI está en la agenda del consejo directivo
4	Financiera	ITRG 04 Riesgos del negocio relacionado con las TI gestionados	- Porcentaje de procesos de TI críticos cubiertos por evaluaciones de riesgo - Frecuencia de actualización del perfil de riesgo - Número de incidentes que no fueron identificados en evaluaciones de riesgos
5	Financiera	ITRG 06 Transparencia de los costes, beneficios y riesgos de las TI	- Porcentaje de casos de negocio de inversiones de TI con costos de TI y beneficios esperados claramente definidos y aprobados - Porcentaje de servicios TI con costos operativos y beneficios esperados claramente definidos y aprobados - Encuesta de satisfacción de interesados clave en relación con el nivel de transparencia, comprensión y precisión de información financiera de TI
6	Cliente	ITRG 07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	- Número de interrupciones de negocio debidas a incidentes de TI - Porcentaje de partes interesadas en el negocio satisfechas de que la entrega de servicios cumpla los niveles de servicio acordados - Porcentaje de usuarios satisfechos con la calidad de entrega de servicios de TI

			- Nivel de satisfacción de los usuarios de los procesos de TI - Porcentaje de propietarios de procesos de negocio satisfechos con el apoyo de productos y servicios de TI
7	Cliente	ITRG 08 Uso adecuado de aplicaciones, información y soluciones tecnológicas	- Porcentaje de propietarios de procesos de negocio satisfechos con el apoyo de productos y servicios TI - Nivel de entendimiento de los usuarios del negocio sobre cómo las soluciones tecnológicas apoyan sus procesos - Nivel de satisfacción de los usuarios de negocio con la formación y los manuales de usuario
8	Interno	ITRG 10 Seguridad de la Información, infraestructura de procesamiento y aplicaciones	- Número de incidentes de seguridad - Número de servicios de TI sin requerimientos de seguridad destacables - Frecuencia de evaluaciones de seguridad en relación a los últimos estándares y guías - Tiempo de concesión, cambio y eliminación de privilegios de acceso comparado con los niveles de servicio acordados
9	Interno	ITRG 11 Optimización de activos, recursos y capacidades de las TI	- Frecuencia de evaluaciones de la capacidad de procesos y de la optimización de los costos - Nivel de satisfacción de la alta dirección del negocio y de TI con los costos y capacidades de TI - Cantidad de activos críticos del negocio
10	Interno	ITRG 13 - Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	- Número de proyectos en tiempo y presupuesto - Porcentaje de interesados satisfechos con la calidad del servicio del proyecto - Costo de mantenimiento de las aplicaciones respecto al costo global de TI

11	Interno	ITRG 15 Cumplimiento de las políticas internas por parte de las TI	- Número de incidentes relacionados con el incumplimiento de políticas - Porcentaje de personal de TI que entienden las políticas - Frecuencia de revisión y actualización de las políticas - Porcentaje de cumplimiento de las políticas de la seguridad de la información
12	Aprendizaje y Conocimiento	ITRG 16 Personal del negocio y de las TI competente y motivado	- Porcentaje de personal cuyas habilidades de TI son suficientes para la competencia requerida - Porcentaje de personal satisfecho con sus roles en TI - Número de horas de aprendizaje/ formación por miembro de personal - Número de incidentes de seguridad causantes de pérdidas financieras, interrupción del negocio o pérdida de imagen pública de la organización

Cabe destacar que el conjunto de métricas definido es suficiente para el alcance del proyecto, pero no se limita solo a estas referencias. Cualquier indicador que sirva para la toma de decisiones de la organización puede darse por válido.

Las métricas deben cumplir con el criterio denominado SMART (Specific, Measurable, Achievable, Relevant and Time Bound) - específicas, medibles, posibles de lograr, pertinentes y oportunas.

6.2. Cubrir la empresa de extremo a extremo

Las distintas áreas de la organización deben estar involucradas en el proceso de elaboración del plan estratégico de seguridad de la información para poder cubrir todos los procesos.

El relacionar las metas de la organización con las metas de TI y en consecuencia con sus métricas es el punto de partida para cubrir la

organización de forma integral. Debe ser factible relacionar las métricas bien definidas con las distintas áreas de la organización.

Cubrir la empresa de extremo a extremo abarca también el gobierno y la gestión de la organización.

6.3. Aplicar un solo marco integrado

COBIT 5 relaciona diversos marcos de trabajo y estándares para cubrir las necesidades de la organización.

De dichos estándares, los que deben ser tenidos en cuenta para diseñar el PESI son: ISO/IEC 27001, ISO/IEC 27005 (la última no cubierta en el presente trabajo, pero contemplada para futuras implementaciones), PMI e ITIL. Para la infraestructura de los centros de cómputos, el estándar ANSI/TIA 942 TIER III.

Asimismo, es posible tener en cuenta como referencia, algunas políticas desarrolladas por la ASI [17] y algunos estándares desarrollados por la ONTI [18].

6.4. Habilitar un enfoque holístico

Los habilitadores o catalizadores son elementos que ayudan a mejorar el funcionamiento de algo. Pueden trabajar de manera individual o colectiva y están guiados por las metas en cascada definidas anteriormente. Proporcionan una ayuda de alto nivel a TI para determinar lo que se desea conseguir. A continuación, se mencionan cada uno de los habilitadores a ser considerados en el desarrollo del PESI.

6.4.1. Principios, políticas y marcos de referencia

Los principios, políticas y marcos de referencia son el motor para conseguir el comportamiento deseado dentro de la organización, ayudan al gobierno de la organización a cumplir con las metas y objetivos deseados. Debería indicarse en estos documentos los valores deseados por la organización y las distintas partes involucradas. Deben estar alimentados

por las necesidades de las distintas partes involucradas y las metas en cascada.

El marco de las políticas debería:

- Definir los roles que aprobarán las políticas de la organización.
- Las políticas tienen un ciclo de vida. Éstas se deben actualizar con una frecuencia determinada gestionando los cambios.
- Definir penalidades por incumplimiento de las políticas.
- Establecer el manejo de casos excepcionales.
- Establecer la manera de verificar y medir el cumplimiento de las políticas, cómo realizar su comunicación y con qué frecuencia.

Dentro del marco del PESI, se sugieren una serie de actividades para trabajar sobre los principios, políticas y marcos de referencia:

- Conformar un comité para la revisión y aprobación de las políticas de seguridad de la información.
- Definir un propietario de las políticas y procedimientos.
- Actualizar la política de seguridad de la información de la organización.
- Revisar con una frecuencia establecida las políticas relacionadas con la seguridad de la información.
- Definir/modificar las siguientes políticas de la organización, entre otras:
    - Políticas de gestión de los activos.
    - Clasificación de la información.
    - Política de uso aceptable de los activos informáticos,
    - Política de uso de dispositivos de propiedad de los usuarios (BYOD - del inglés Bring Your Own Device).
    - Política de gestión de riesgos.
    - Plan de continuidad de negocio.
- Crear/modificar procedimientos para estandarizar los procesos que se realizan en las distintas áreas de soporte tecnológico

- Establecer métricas para medir la creación/modificación de políticas y procedimientos
- Establecer métricas para medir el cumplimiento por parte de los empleados, de las políticas establecidas según aplica en cada caso

Las políticas son documentos estratégicos dentro de la organización. Deben ser las guías para alcanzar los objetivos dentro y fuera de la misma. Tienen que estar adaptadas al contexto de la organización y ser alimentadas por las metas en cascada. Deben estar escritas en un alto nivel y no describir ninguna tecnología o persona en particular. Es recomendable que incluyan, además, las penalidades por no cumplimiento.

6.4.2. Procesos

El modelo de procesos según COBIT 5 "*es una colección de prácticas influidas por las políticas y procedimientos de la empresa que toma entradas de una serie de recursos (incluyendo otros procesos), manipula las entradas y produce salidas (por ejemplo, productos y servicios)*"[15]

El modelo de procesos integra los intereses de las partes interesadas, las metas en cascada de la organización, el ciclo de vida de los procesos y las buenas prácticas.

El modelo subdivide los procesos de gobierno y de gestión de las TI. Las prácticas de gobierno son definidas como: evaluar, orientar y supervisar (EDM, por sus siglas en inglés) desarrolladas en la organización por la presidencia y el Consejo Directivo y las de gestión definidas como: planificar, construir, ejecutar y monitorear (PBRM, por sus siglas en inglés). Ver figura 6 del capítulo 4.

El modelo de referencia de procesos de COBIT 5, donde se describen prácticas, actividades y actividades detalladas, permitirá enunciar las buenas prácticas a considerar.

[15] COBIT 5 Procesos Catalizadores - Capítulo 3 - El modelo de Procesos de COBIT 5

En la figura 11 se puede observar los procesos habilitadores incluidos en el Marco de Referencia de Procesos de COBIT 5

El proceso habilitador seleccionado para el PESI fue el que se muestra marcado en rojo en la figura siguiente:

Figura 11-Modelo de Referencia de Procesos - Fuente: COBIT 5

6.4.2.1 Gestionar la Seguridad (APO13)

Proceso habilitador que se encuentra dentro del Área de Gestión (APO13) [12], figuras 6 y 7 del Capítulo 4. Este proceso describe cómo definir, operar y supervisar el sistema de gestión de seguridad de la información dentro de la organización.

Tiene como propósito el de mantener el impacto y ocurrencia de los incidentes de seguridad de la información dentro de niveles de riesgo aceptables por la organización.

Este proceso contribuye al logro de los objetivos de TI y por consecuencia a las metas en cascada que están alineadas con los objetivos del negocio.

Este proceso tiene 3 prácticas claves de gestión:

- APO13.01 - Establecer y mantener un SGSI
- APO13.02 - Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información
- APO13.03 - Supervisar el SGSI

Las Actividades propuestas alineadas también con la normativa ISO/IEC 27001 [19] son las siguientes:

- Definir el alcance del SGSI en términos de las características de la organización
- Definir un SGSI de acuerdo a las características de la organización
- Alinear el SGSI con las necesidades de la organización
- Obtener respaldo de la dirección para implementar el SGSI
- Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI
- Definir y comunicar los roles y responsabilidades de la gestión de la seguridad de la información
- Comunicar el enfoque de SGSI
- Formular y mantener un plan de tratamiento de riesgos de seguridad alineado con los objetivos estratégicos de la organización
- Mantener un inventario de los activos informáticos de la organización
- Realizar auditorías o revisiones periódicas
- Realizar revisiones periódicas del SGSI por la dirección para asegurar que el alcance sigue siendo el adecuado

Las guías relacionadas con estas actividades para elaborar el PESI y contemplar la elaboración de un SGSI están vinculadas con los siguientes estándares:

- ISO/IEC 27001:2013 - Sistema de gestión de seguridad de la información - Requisitos, sección 4
- NIST SP 800-53 Rev. 1 - Controles de Seguridad recomendados para sistemas de información federales de EEUU.
- ITIL V3 2011 - Diseño de Servicio, 4.7 Gestión de la Seguridad de la información

A continuación, y a modo de ejemplo, se muestra una tabla RACI asociada al proceso que nos ocupa:

Tabla 5- Matriz RACI para Proceso Habilitador APO13

	Presidente	Comité de SI	Auditor Externo	Auditor Interno	Dpto Soporte Tec.	Dpto Arq Tec.	Dpto Plan e Infra.	Dpto de Aplicaciones	Dpto de Seg Informática	Dpto Gestion Op y Tec.
APO13.01 - Establecer un SGSI	C	R	I	I	I	I	I	I	A	C
APO13.02 - Definir y gestionar un plan de tratamiento del riesgo de la SI	I	R	I	C	C	C	C	C	A	C
APO13.03 Supervisar y Revisar el SGSI	C	R	I	I	I	I	I	I	A	C

6.4.3. Estructuras Organizacionales

El organigrama de la organización se muestra en la figura 1 del capítulo 2. Este gráfico muestra algunas oportunidades de mejora que se mencionan a continuación como recomendaciones:

- Crear un comité de seguridad de la información. Este comité debe reunir las distintas partes interesadas.
- El área de Seguridad de la información depende del área de gestión estratégica. Se recomienda que el área de Seguridad de la información sea una jefatura independiente de esta área.

- Asignar una oficina u oficial de seguridad de la información que se encargue de la operación y la implementación de los controles de seguridad de la información

El organigrama de la organización propuesto es el siguiente:

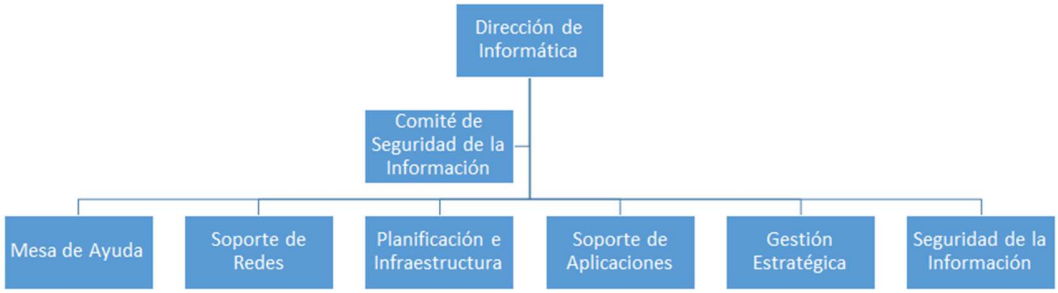

Figura 12- Organigrama propuesto para la organización

Además de la modificación del organigrama, se propone también la definición de los siguientes roles en función de la seguridad de la información, estos son [20]:

Tabla 6- Descripción de roles relacionados con la Seguridad de la Información

Rol	Descripción del Rol
Comité de Seguridad de la Información	Definir las metas de seguridad de la información en relación con las de la organización. Facilitar los recursos necesarios para concretar el PESI. Formular, revisar y aprobar la política de seguridad de la información. Asegurarse a través del monitoreo y revisión de las buenas prácticas de seguridad de la información son aplicadas consistentemente dentro de la organización
Jefe de Seguridad	Ejecutar y gestionar el PESI. Establecer las métricas

de la Información	para gestionar la seguridad de la información. Responsable de la gestión de los riesgos. Coordinación de la implantación de controles de seguridad de la información.
Oficial de Seguridad de la Información	Implementar los controles de seguridad de la información. Monitoreo de las actividades relacionadas con la seguridad de la información, como antivirus, firewall, SIEM (Security Information Event Management), etc. Crear y actualizar procedimientos relacionados con la seguridad de la información
Custodio de los activos informáticos	Resguardar la integridad, confidencialidad y disponibilidad del activo informático asignado

6.4.4. Cultura, Ética y Comportamiento

La cultura, ética y comportamiento comprende toda la organización. Están involucrados las partes interesadas internas de la organización, los directores y el Presidente, como así también entidades externas como agencias auditoras, entes gubernamentales y los individuos que la componen.

La organización descrita en el presente trabajo es de un ámbito público [21], es decir, que los ingresos de la misma dependen de las contribuciones de los ciudadanos. Esta situación genera algunos problemas culturales, éticos y de comportamiento, como los que se mencionan a continuación:

- Salarios relativamente bajos e inequidad interna. Hay funcionarios públicos que realizan la misma función y los salarios no son iguales.

- Uno de los aspectos valorados dentro de la organización es la estabilidad laboral. Los empleados no tienen temor a perder su empleo.
- Los empleados están muchos años en la misma posición y no hay un claro plan de desarrollo.
- No hay metodologías rigurosas de control de tareas internas, esto no permite que los trabajadores estén motivados para realizar su trabajo
- No hay procesos homogéneos dentro de la organización. En consecuencia, los resultados de los distintos procedimientos pueden ser diferentes.
- No hay una cultura clara de seguridad de la información

La cultura trasciende la organización y evoluciona a través del tiempo. Los comportamientos se van adaptando y la concientización de la seguridad de la información puede incrementarse o no. Para medir el cambio cultural es posible implementar distintas métricas que pueden ayudar a ver la evolución:

- Complejidad de las contraseñas
- Cantidad de laptops que usan candados de seguridad
- Cantidad de documentos que tienen aplicadas las políticas de clasificación de la información
- Cantidad de personas que dejan la computadora/laptop desbloqueada
- Entrenamientos de seguridad de la información a los empleados encargados de la seguridad y la infraestructura de la organización

6.4.5. Información

La información es considerada un activo fundamental para el correcto funcionamiento de la organización. El tratamiento y el cuidado de la información debe ser gestionados y se debe tener en cuenta las características de la organización para una correcta clasificación.

Con la clasificación de la información se debe identificar la información crítica del negocio. En el presente trabajo, está dentro del

alcance la información relacionada con la seguridad de la información, la cual cubre entre otros, al Plan Estratégico de Seguridad de la Información (PESI), el presupuesto, las políticas y procedimientos y el perfil de riesgo de la organización. Es necesario considerar en el PESI, la documentación necesaria relacionada con la protección de la información como, por ejemplo:

- Políticas de clasificación de la información
- Clasificación y desclasificación de la información de la organización
- Archivo de la información (tanto digital como en papel) luego de un tiempo establecido
- Custodia de todos los documentos confidenciales que tienen que moverse físicamente
- Acciones relacionadas con el cuidado de la información que se maneja en escritorios (físicos o digitales) e impresoras.

Se detalla una serie de documentos [19] que debieran ser enunciados en el PESI como necesarios para el establecimiento del Sistema de Gestión de Seguridad de la Información (SGSI – mencionado en el proceso APO13). En la matriz RACI siguiente se pueden observar las distintas responsabilidades de acuerdo al tipo de documento:

Tabla 6- Documentos necesarios para establecer el SGSI y las responsabilidades

Documentos	Presidente de la Institución	Comité de SI	Director de Sistemas	Dpto Soporte Tec.	Dpto Arq Tec.	Dpto Plan e Infra.	Dpto de Aplicaciones	Dpto de Seg Informática	Dpto Gestion Op y Tec.
Definir y elaborar un un PESI	I	R	I	C	C	C	C	A	C
Definir alcance del SGSI	I	R	I	C	C	C	C	A	C
Política de SI y Objetivos	I	R	I	C	C	C	C	A	C
Metodología y Tratamiento del Riesgo	I	R	I	C	C	C	C	A	C
Plan de Tratamiento del Riesgo	I	R	I	C	C	C	C	A	C
Informe sobre la evaluación de riesgos	I	R	I	C	C	C	C	A	C
Definición de Roles y responsabilidades de la Seguridad	I	R	I	C	C	C	C	A	C
Inventario de Activos	I	R	I	C	C	C	C	A	C
Uso Aceptable de los Activos	I	R	I	C	C	A	C	C	C
Política de Control de Acceso	I	R	I	C	C	A	C	C	C
Procedimientos de Operación para gestión de TI	I	R	I	C	C	C	C	C	A
Principios de Ingeniería de Sistemas seguros	I	R	I	C	C	A	C	C	C
Política de Seguridad para proovedores	I	R	I	C	C	A	C	C	C
Procedimiento para gestión de Incidentes	I	R	I	C	C	C	C	C	A
Procedimientos de Continuidad del negocio	I	R	I	C	C	C	C	A	C
Requerimientos legales, regulatorios y contractuales	I	R	I	C	C	C	C	A	C

Cada documento tiene que tener un ciclo de vida, es decir, debe pasar por una etapa de plan, diseño, elaboración, implementación y revisión periódica. El proceso de aprobación de la documentación debe pasar por un proceso de gestión de cambios, el cual requiere una serie de correcciones y aprobaciones para que el documento sea considerado aprobado.

6.4.6. Servicios, Infraestructura y Aplicaciones

La organización brinda servicios a través de Internet. Estos servicios deben estar disponibles toda vez que sea necesario su acceso, la información contenida debe ser confiable y la información confidencial se debe gestionar correctamente.

Los servicios web y aplicaciones están soportados por una infraestructura propia y son desarrollados por el departamento de aplicaciones de la organización.

La organización cuenta con el apoyo de diversos proveedores los cuales brindan soporte de la infraestructura, servicios de consultoría o desarrollo de aplicaciones.

Se consideraron las siguientes tareas dentro del PESI para mejorar la infraestructura de la red dentro de la organización:

- Acondicionamiento de los centros de cómputos. Esto incluye control de acceso, refrigeración, sistemas contra incendios, UPS, generadores.
- Redundancia en el equipamiento y en los servicios brindados.
- Plan de mantenimiento del equipamiento
- Gestión de la configuración de los equipos
- Configuración y optimización del sistema de resguardo

Dentro del departamento de aplicaciones se consideró implementar las siguientes tareas y/o políticas:

- Todas las aplicaciones deben tener usuarios únicos y no deben ser compartidos.
- Implementar una política de contraseñas.
- Implementar un gestor centralizado de logs (SIEM).
- Cambiar todos los usuarios administradores por defecto por otros que sean difíciles de identificar como administrador.
- Implementar un gestor de contraseñas para los usuarios administradores.
- Implementar el principio de mínimo privilegio de las aplicaciones.
- Implementar distintos ambientes de trabajo, por ejemplo, Desarrollo, Testing, Producción y Capacitación.
- Implementar el concepto de segregación de funciones.

6.4.7. Personas, Habilidades y Competencias

Las personas deben tener las competencias apropiadas para desempeñar el puesto de trabajo. Se propuso lo siguiente:

- Revisar/Modificar/Crear una descripción detallada de las funciones y alcance de los departamentos

- Revisar/Modificar/Crear las responsabilidades de cada uno de los puestos de trabajo dentro de la estructura organizacional
- Revisar/Modificar/Crear una lista con toda la experiencia, profesiones según el puesto y cursos requeridos para cada posición
- Establecer un plan de capacitación a todos los empleados que deberían realizar según el tipo de función y rol dentro de la organización
- Establecer un plan de concientización de los empleados

6.5. Separar el Gobierno de la Gestión

El gobierno es ejercido por el Presidente de la Organización siendo éste la máxima autoridad encargada de dirigir orientar y controlar la organización. Para el desempeño de estas tareas se requiere tener las herramientas necesarias para poder tomar las decisiones adecuadas. Muchas de las decisiones se toman por el buen criterio y voluntad del gobierno, pero no son apoyadas con métricas y fundamentos adecuados.

El Consejo Directivo es un grupo de personas representantes de la organización. Entre sus funciones está la de lograr acuerdos entre las distintas áreas, brindar el apoyo legal, así como estimular el buen funcionamiento de la organización. Son participantes en la toma de decisiones de gobierno en conjunto con la presidencia.

Los directores de los distintos departamentos son los encargados de implementar, planificar y gestionar las actividades de su área. Están actividades se realizan en base a las directivas de la presidencia y el consejo directivo.

Se recomienda como parte del PESI, armar un tablero de gestión en el cual reflejar con métricas las actividades de la organización siendo de acuerdo al criterio SMART previamente mencionado. Con este esquema, se pueden reflejar métricas acordes a las necesidades de la organización dando las directivas necesarias para poder gobernar la organización

cumpliendo con las expectativas de todas las partes interesadas, minimizando el riesgo, optimizando los recursos y con mayor transparencia.

7. Implementación

La ejecución del PESI basado en COBIT 5 puede alcanzar los objetivos satisfactoriamente si se logra adaptar el plan al contexto de la organización.

Para que el proceso de implementación del PESI sea ejecutado con éxito, es importante considerar algunas actividades que facilitarán su implementación:

- Reconocer puntos débiles y eventos desencadenantes. Donde es conveniente minimizar el riesgo y donde se puede trabajar para lograr un mayor resultado con el menor esfuerzo
- Crear un entorno apropiado para la implementación. Esto es, realizar presentaciones del plan como reuniones de arranque de proyecto, crear equipos de trabajo, tener el presupuesto requerido, el apoyo de la dirección.
- Usar COBIT 5 para identificar carencias y guiar en el desarrollo de elementos facilitadores como políticas, procesos, principios, estructuras organizativas y roles y responsabilidades.

7.1. Considerando el Contexto organizacional

Es importante para la organización tener en cuenta el contexto organizacional. El plan de trabajo debe ser diseñado en función de lo siguiente:

- Ética y cultura. Es primordial poder establecer una cultura de trabajo orientado hacia la protección de la información [22].
- Leyes aplicables, regulaciones y políticas. De acuerdo a la legislación argentina, aplica la Ley de Habeas Data (Ley 25.326) [3], la Ley de Delitos

Informáticos (Ley 26.388) [5] y la Ley de Propiedad Intelectual (Ley 11.723) [16] y sus modificatorias.

- Misión, visión y valores. Con las metas en cascada se pueden alinear las metas del área de sistemas con la organización. La misión y la visión es poder dar un servicio de calidad a los ciudadanos.
- Políticas y prácticas de Gobierno. Las políticas y prácticas de gobierno son tomadas como referencia para proponer modificar nuevas políticas y nuevas prácticas de gobierno.
- Plan de negocio y perspectivas estratégicas. Es necesario optimizar el uso de los recursos y con una visión estratégica permite entender el consumo del servicio del ciudadano en el largo plazo.
- Umbral de riesgo tolerable por la organización.
- Capacidades y recursos disponibles.
- Prácticas de la industria.

7.2. Factores críticos de éxito

Los factores críticos de éxitos son tareas que ayudan a conseguir con éxito la implementación del PESI. Se puede mencionar, por ejemplo:

- El apoyo y compromiso de la presidencia y los directivos para la implementación, como así también la orientación y directrices para la implementación del plan
- Las metas en cascada permiten entender cómo pueden las distintas áreas de los departamentos apoyar el negocio y conseguir los objetivos
- Una comunicación efectiva de lo que se va a realizar y de los cambios propuestos, a fin de habilitar los cambios necesarios
- COBIT 5 [9], la serie ISO/IEC 27000 [4], el estándar de la ONTI [18] y otras buenas prácticas se pueden personalizar y ajustar al entorno de la organización.

- Enfocarse en las tareas que requieren poco esfuerzo y tienen resultados inmediatos, de esta forma se van a observar grandes cambios y el personal se va a mantener motivado.

7.3. Creando el Entorno Apropiado

El apoyo, soporte y dirección de la presidencia es primordial para conseguir los objetivos organizacionales. Es importante no centrarse en las tareas operativas sino en las actividades que van a dar resultados a largo plazo.

Los factores sensibles y temas actuales, por ejemplo, el contexto político, debe ser tenido en cuenta si éstos pueden llegar a afectar la implementación.

Es importante tener las condiciones necesarias para poder implementar el PESI. El personal de la organización debe estar capacitado y entrenado para realizar las tareas necesarias, desde las de gestión a las operativas.

Los recursos humanos de la organización que van a estar involucrados dentro del PESI tienen responsabilidades y tareas que realizan habitualmente. El costo de la dedicación de los recursos al PESI se debe tener en cuenta a la hora de elaborar el presupuesto. Se debe contar un presupuesto acorde a las tareas que se van a realizar y tener una previsión en caso de algún gasto imprevisto.

Se deben generar y mantener las estructuras y procesos para poder supervisar y orientar. Se deben poder ver resultados y deben estar alineados con las necesidades de las partes interesadas y la gestión del riesgo. El uso de métricas ayuda a generar estas estructuras.

Es importante establecer hitos en los cuales sea posible observar resultados, para establecer una línea del tiempo en el cual se va a conseguir el resultado deseado.

7.4. Reconociendo los Puntos débiles y eventos desencadenantes

La ejecución del PESI es un proyecto que tiene varios cambios estructurales aparejados. Es por esto que es muy probable que cuando el cambio comience a hacerse efectivo exista un rechazo al mismo. Para mejorar la aceptación es importante centrarse en las tareas con ganancias inmediatas. Además, es importante enfocarse en distintos eventos que puedan ayudar a extender el compromiso en la alta dirección y soportar los mencionados cambios.

Algunos eventos que pueden ayudar a generar el apoyo necesario son:

- Incidentes de seguridad relacionados con la infraestructura de TI, como pérdida de información y fallos en proyectos
- Problemas en los servicios internos y/o externos que brinda TI, como por ejemplo el fallo sistemático ante la necesidad de mantener los niveles de servicio acordados
- Incapacidad para cumplir con requisitos regulatorios o de entidades externas
- Hallazgos de auditorías que reflejen el bajo rendimiento de TI

- En el Apéndice se define los pasos a seguir para implementar un SGSI como parte de la ejecución de un PESI diseñado en base a COBIT 5.

8. Conclusiones

El presente trabajo trata sobre el diseño y armado de un PESI en una organización pública. Además, sugiere cómo abordar la implementación para conseguir resultados exitosos pero no se describe la experiencia en este proceso

El PESI diseñado contiene una serie de recomendaciones que le permiten estar alineado con el marco de trabajo COBIT 5 y otras normativas, como lo son la serie ISO/IEC 27000 [4], ANSI/TIA 942 [6].

Respecto a la experiencia con COBIT 5 se pudo observar que el marco de trabajo que se propone abarca toda la organización y el gobierno de TI. Esto representa una ventaja competitiva respecto a otros marcos de trabajos o normativas porque se puede alinear TI a la estrategia del negocio, maximizando el beneficio y minimizando el riesgo. Este marco puede ser utilizado en organizaciones donde el gobierno y la gestión están separados como este caso o se tiene la intención de separarlas.

Este marco normativo está elaborado para dar un soporte a alto nivel y que sirva para el gobierno o gestión de la organización. Para implementar procesos a un nivel más detallado hay que recurrir a normas específicas. Por ejemplo, en este trabajo se tuvo en cuenta también la serie de normas ISO/IEC 27000 para todo lo relacionado con seguridad de la información, ISO/IEC 20000 para la gestión de TI, PMI para la gestión de proyectos, ANSI/TIA 942 para la infraestructura de centros de cómputo, etc.

Como desventaja se pudo analizar la dificultad que tiene este marco de trabajo. Al ser una norma abarcativa y con tantos dominios, se requiere una gran experiencia en el área y un amplio conocimiento del negocio. Para lograr que el plan logre su propósito se debe establecer un alcance claro, de acuerdo a la cantidad de recursos disponibles y al presupuesto.

Se identificó durante el proceso algunos puntos en los cuales es necesario apoyarse para lograr implementar el PESI. Éstos son:

- Contar con el apoyo de la dirección es el factor fundamental para cumplir los objetivos
- Establecer metas acordes a la situación actual. Es difícil cumplir con objetivos que no están cerca de la realidad porque no se logra observar de manera clara el objetivo.
- Establecer una metodología acorde para el cumplimiento del plan. En este caso se eligió la metodología en cascada de PMI.
- Contar con el presupuesto, los recursos y el tiempo adecuado para cumplir las metas establecidas.
- Establecer hitos en los cuales se pueda observar los logros conseguidos.
- Definir un conjunto de métricas para determinar el cumplimiento del plan

Por otro lado, es posible que se tengan algunas dificultades para lograr el objetivo de implementar el plan:

- El rechazo al cambio por parte del personal [22] es un tema que debe ser abordado. Es necesario mantener una comunicación fluida entre las distintas partes, incluirlos en el proceso de cambio y realizar campañas de concientización para que entiendan que este cambio es necesario
- El presupuesto. Es posible que se tenga una determinada cantidad de dinero y luego por cambios en el proyecto o errores de diseño del plan, el presupuesto original no alcance. Se tiene que calcular un dinero extra para posibles imprevistos
- El contexto externo. Es importante tener en cuenta posibles cambios en el contexto externo para minimizar el riesgo. La inflación, devaluaciones, limitaciones en las exportaciones de diversos productos, cambios políticos, nuevos requerimientos externos son algunos ejemplos.
- La experiencia del personal y los recursos. Es posible tener grandes ideas pero es necesario saber cómo llevarlas a cabo. El personal debe estar capacitado, debe contar con las herramientas necesarias para realizar el

trabajo y un conocimiento de las metodologías que van a ser implementadas. Además, deben estar todos alineados con las metas empresariales y no ver sólo los intereses del sector involucrado

9. Apéndice

9.1. Plan de Implementación de un SGSI

9.1.1 Resumen

El presente trabajo tiene por objeto implementar un SGSI en una organización pública basado en la serie de normas ISO/IEC 27000 y encuadrado en el marco de un PESI desarrollado bajo el marco COBIT 5.

Define una serie de actividades para implementar un conjunto de políticas, procedimientos, mejores prácticas, herramientas y charlas de concientización relacionadas con la seguridad de la información.

Los objetivos del PESI están alineados con los de la organización por medio de las metas en cascada que relacionan las mismas con las de la Dirección de Informática.

9.1.1 Objetivo

Cambiar la cultura de la seguridad de la información en la organización concientizando, implementando mejores prácticas, creando políticas, así como implementando soluciones de software e infraestructura.

Implementar y mantener un SGSI en de la organización.

9.1.2. Alcance

El presente trabajo se desarrolla en base a la normativa COBIT 5 y la serie ISO/IEC 27000. No se encuentra dentro del alcance certificar ninguna de las normativas.

Se toma como foco del trabajo la Dirección de Informática de la organización, específicamente en temas relacionados con Seguridad de la Información.

Se definen los lineamientos para orientar el área de seguridad de la información hacia las mejores prácticas de COBIT 5 e ISO/IEC 27001.

9.1.3. Plan de Implementación

9.1.3.1. Inicio del Proyecto

Se definieron las siguientes tareas:

- Obtener el respaldo de la dirección para la creación e implementación del PESI
- Definición de los recursos que van a participar en el proyecto
- Identificar y definir los roles y funciones
- Creación de un Comité de Seguridad de la Información
- Acta de inicio del proyecto
- Elaborar una reunión de inicio de proyecto (Kick off Meeting)

Duración estimada de la actividad: 2 semanas

9.1.3.2. Planeamiento

- Asignar una oficina u oficial de seguridad de la información que se encargue de la operación y la implementación de los controles de seguridad de la información

El organigrama de la organización propuesto es el siguiente:

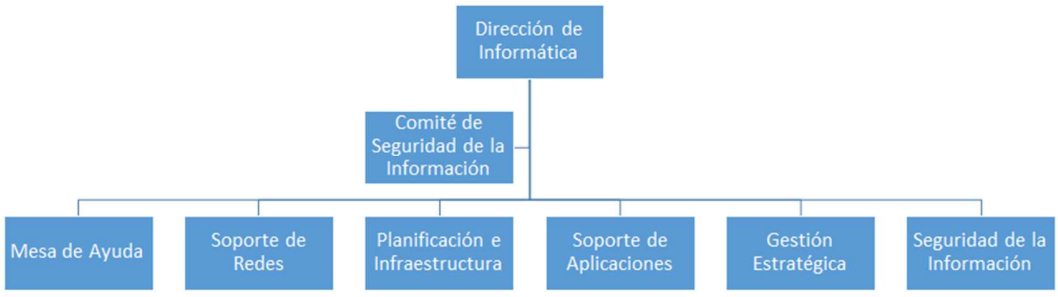

Figura 13- Organigrama Propuesto en el PESI

- Elaborar un plan de comunicaciones
- Roles y funciones de los recursos dentro del marco del PESI (Matriz RACI)

- Descomposición de las tareas de trabajo (EDT o WBS del inglés Work Breackdown Structure)[16] con los tiempos establecidos y los entregables de cada hito
- Revisión del proyecto, esto incluye:
  - Recursos requeridos
  - Costos del Proyecto
  - Riesgos del Proyecto
  - Revisión y entendimiento con el procedimiento de gestión de cambios
  - Establecer métricas
  - Planeamiento de las actividades previstas del proyecto

Duración estimada de la actividad: 5 Semanas

Criterio de Aceptación:

- Oficina de Seguridad de la información creada
- Organigrama modificado
- Recursos disponibles
- Plan detallado

9.1.3.3. Implementación

Fase 1

Documentos necesarios para un sistema de gestión de seguridad de la información (SGSI):

- Definir alcance del SGSI en función de las características de la organización
- Política de Seguridad de la información y Objetivos
- Metodología y Tratamiento de la Gestión del Riesgo dentro de la organización
- Informe sobre la evaluación de riesgos
- Definición de Roles y responsabilidades de la Seguridad de la información dentro de la organización

[16]La descomposición de las tareas de trabajo es una actividad dentro de un proyecto que consiste en una presentación simple y organizada de ver el trabajo requerido para completar un proyecto.

- Definir/modificar política de gestión de los activos
- Definir/modificar la política de clasificación de la información
- Crear y mantener un Inventario de Activos
- Política de Uso Aceptable de los Activos
- Política de Control de Acceso
- Procedimientos de Operación para gestión de TI
- Principios de Ingeniería de Sistemas seguros
- Política de Seguridad para proveedores
- Procedimiento para gestión de Incidentes
- Procedimientos de Continuidad del negocio
- Requerimientos legales, regulatorios y contractuales
- Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI
- Comunicar el enfoque de SGSI
- Procedimiento de comunicación de políticas

Se enuncian los documentos necesarios para el PESI con los distintos responsables en la siguiente matriz RACI:

Tabla 7- Documentos necesarios para establecer el SGSI y las responsabilidades en el PESI

Documentos	Presidente de la Institución	Comité de SI	Director de Sistemas	Dpto Soporte Tec.	Dpto Arq Tec.	Dpto Plan e Infra.	Dpto de Aplicaciones	Dpto de Seg Informática	Dpto Gestion Op y Tec.
Definir y elaborar un un PESI	I	R	I	C	C	C	C	A	C
Definir alcance del SGSI	I	R	I	C	C	C	C	A	C
Política de SI y Objetivos	I	R	I	C	C	C	C	A	C
Metodología y Tratamiento del Riesgo	I	R	I	C	C	C	C	A	C
Plan de Tratamiento del Riesgo	I	R	I	C	C	C	C	A	C
Informe sobre la evaluación de riesgos	I	R	I	C	C	C	C	A	C
Definición de Roles y responsabilidades de la Seguridad	I	R	I	C	C	C	C	A	C
Inventario de Activos	I	R	I	C	C	C	C	A	C
Uso Aceptable de los Activos	I	R	I	C	C	A	C	C	C
Política de Control de Acceso	I	R	I	C	C	A	C	C	C
Procedimientos de Operación para gestión de TI	I	R	I	C	C	C	C	C	A
Principios de Ingeniería de Sistemas seguros	I	R	I	C	C	A	C	C	C
Política de Seguridad para proovedores	I	R	I	C	C	A	C	C	C
Procedimiento para gestión de Incidentes	I	R	I	C	C	C	C	C	A
Procedimientos de Continuidad del negocio	I	R	I	C	C	C	C	A	C
Requerimientos legales, regulatorios y contractuales	I	R	I	C	C	C	C	A	C

Duración de la actividad: 6 semanas

Criterio de aceptación: Entrega de la documentación

Fase 2

La infraestructura de la red contempla las siguientes actividades para estar alineados con el PESI:

- Acondicionamiento de los centros de cómputos. Esto incluye control de acceso, refrigeración, sistemas contraincendios, UPS, generadores
- Redundancia en el equipamiento y en los servicios brindados.
- Plan de mantenimiento del equipamiento
- Gestión de la configuración de los equipos
- Configuración y optimización del sistema de resguardo

Se deben llevar a cabo las siguientes actividades en el departamento de aplicaciones:

- Todas las aplicaciones deben tener usuarios únicos y no deben ser compartidos.
- Implementar una política de contraseñas.
- Implementar un gestor centralizado de logs (SIEM).
- Cambiar todos los usuarios administradores por defecto por otros que sean difíciles de identificar como administrador.
- Implementar un gestor de contraseñas para los usuarios administradores.
- Implementar el principio de mínimo privilegio de las aplicaciones.
- Implementar distintos ambientes de trabajo, por ejemplo, Desarrollo, Testing, Producción y Capacitación.
- Implementar el concepto de segregación de funciones.

Las personas deben tener las competencias apropiadas para desempeñar el puesto de trabajo. Se propone lo siguiente:

- Revisar/Modificar/Crear una descripción detallada de las funciones y alcance de los departamentos
- Revisar/Modificar/Crear las responsabilidades de cada uno de los puestos de trabajo dentro de la estructura organizacional
- Revisar/Modificar/Crear una lista con toda la experiencia, profesiones según el puesto y cursos requeridos para cada posición
- Establecer un plan de capacitación a todos los empleados que deberían realizar según el tipo de función y rol dentro de la organización
- Establecer un plan de concientización de los empleados

Duración de la actividad: 12 Semanas
Criterio de Aceptación:

- Acondicionamiento de la infraestructura de centros de cómputos
- Redundancia en los servicios de red críticos
- Entrega de la documentación mantenimiento de los equipos y software
- Implementación del SIEM
- Creación de ambientes para el desarrollo de aplicaciones
- Planes de capacitación de los empleados

Fase 3

Se deben incluir al menos 10 métricas para poder gestionar la seguridad de la información, algunos ejemplos se mencionan a continuación:

- Complejidad de las contraseñas
- Cantidad de laptops que usan candados de seguridad
- Cantidad de documentos que tienen aplicadas las políticas de clasificación de la información
- Cantidad de personas que dejan la computadora/laptop desbloqueada
- Entrenamientos de seguridad de la información a los empleados encargados de la seguridad y la infraestructura de la organización

- Crear responsabilidad colectiva sobre la seguridad de la información con capacitaciones de concientización
- Registros de personas que asisten a capacitaciones sobre la seguridad de la información
- Políticas de clasificación de la información
- Clasificación y desclasificación de la información de la organización
- Archivo de la información (tanto digital como en papel) luego de un tiempo establecido
- Custodia de todos los documentos confidenciales que tienen que moverse físicamente
- Acciones relacionadas con el cuidado de la información que se maneja en escritorios (físicos o digitales) e impresoras.

Duración de la actividad: 3 semanas

Criterio de aceptación: 10 métricas de seguridad de la información implementadas.

Fase 4

- Realizar auditorías o revisiones periódicas
- Realizar revisiones periódicas del SGSI por la dirección para asegurar que el alcance sigue siendo el adecuado
- Diseñar proceso de evaluación y tratamiento de riesgos
- Realizar programas de capacitación y concientización

Duración de la Actividad: 5 Semanas

Criterio de Aceptación:

- Realizar una auditoría de seguridad
- Entrega de documentación

9.1.3.4. Cierre del Plan

- Reunión de cierre de proyecto.
- Entrega de toda la documentación relacionada al proyecto
- Lecciones aprendidas y oportunidades de mejora

Duración de la actividad: 1 semana

Criterio de Aceptación:

- Entrega de toda la documentación
- Documento de conformidad de las partes interesadas
- Acta de cierre de proyecto

9.1.4. Cronograma estimado

A continuación, se muestra el cronograma estimado para realizar las actividades:

Tabla 8- Cronograma de Actividades en el PESI

Cronograma																								
	Semanas	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Etapa	Fase																								
Inicio del Proyecto																									
Planeamiento																									
Implementación	Fase 1																								
	Fase 2																								
	Fase 3																								
	Fase 4																								
Cierre del Proyecto																									

10. Bibliografía

[1] Y. C. Josué, «Tipos de Organizaciones,» [En línea]. Available: https://es.slideshare.net/yezkas-yeye/tipos-de-organizaciones-13003927. [Último acceso: 17 11 2017].

[2] R. E. Rincón, «Diferencia entre Empresa Pública y Privada,» [En línea]. Available: https://es.slideshare.net/RobertoEnrique_Rincon/diferencias-entre-empresa-pblica-y-empresa-privada. [Último acceso: 17 11 2017].

[3] «Ley de Habeas Data. Ley 25.326,» [En línea]. Available: https://www.oas.org/juridico/PDFs/arg_ley25326.pdf. [Último acceso: 17 11 2017].

[4] International Organization for Standarization, «ISO/IEC 27000 Information Security,» [En línea]. Available: https://www.iso.org/isoiec-27001-information-security.html. [Último acceso: 17 11 2017].

[5] Ley de Delitos Informáticos. Ley 26.388, [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm. [Último acceso: 17 11 2017].

[6] TIA-942, «About Data Centers,» [En línea]. Available: http://www.tia-942.org/content/162/289/About_Data_Centers. [Último acceso: 22 11 2017].

[7] ISACA, «COBIT 2019 Publications & Resources,» ISACA, [En línea]. Available: http://www.isaca.org/COBIT/Pages/COBIT-2019-Publications-Resources.aspx. [Último acceso: 06 03 2019].

[8] P. Gonzalez, «COBIT 2019 - El nuevo modelo de gobierno empresarial para información y tecnología,» [En línea]. Available: https://medium.com/@ppglzr/cobit-2019-el-nuevo-modelo-de-gobierno-empresarial-para-informaci%C3%B3n-y-tecnolog%C3%ADa-a7bf92b7288b. [Último acceso: 06 03 2019].

[9] ISACA, COBIT 5 - Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa, 2012.

[10] ISACA, COBIT 5 for Information Security, 2012.

[11] C. I. Panamá, «COBIT 5 Introduction,» ISACA, [En línea]. Available: https://www.isaca.org/COBIT/Documents/COBIT5-Introduction-Spanish.ppt. [Último

acceso: 06 03 2019].

[12] ISACA, COBIT 5: Procesos Catalizadores, IL, EE.UU.: ISACA, 2012.

[13] G. Braga, «Cómo COBIT 5 mejora la capacidad de procesos de trabajo de auditores, profesionales de aseguramiento y evaluadores,» ISACA, 2016. [En línea]. Available: https://www.isaca.org/Journal/archives/2016/Volume-1/Documents/How-COBIT-5-Improves-the-Work-Process-Capability-of-Auditors-Assurance-Professionals-and-Assessors_joa_Spa_0116.pdf. [Último acceso: 06 03 2019].

[14] E. Celi, «Evaluación del nivel de capacidad de los procesos de TI, mediante el marco de referencia COBIT PAM,» [En línea]. Available: https://www.researchgate.net/publication/317558763_Evaluacion_del_nivel_de_capacidad_de_los_procesos_de_TI_mediante_el_marco_de_referencia_COBIT_PAM. [Último acceso: 6 3 2019].

[15] G. Kulkarni, «Applying the Goals Cascade to the COBIT 5 Principle Meeting Stakeholder Needs,» ISACA, 24 04 2017. [En línea]. Available: http://www.isaca.org/COBIT/focus/Pages/applying-the-goals-cascade-to-the-cobit-5-principle-meeting-stakeholder-needs.aspx. [Último acceso: 06 03 2019].

[16] Ley de Propiedad Intelectual. Ley 11.723, [En línea]. Available: http://www.oas.org/juridico/PDFs/arg_ley11723.pdf. [Último acceso: 17 11 2017].

[17] Buenos Aires Ciudad, «Agencia de Sistemas de Información,» [En línea]. Available: http://www.buenosaires.gob.ar/jefaturadegabinete/agenciadesistemas. [Último acceso: 22 11 2017].

[18] ONTI, «Oficina Nacional de Tecnologías de la Información,» [En línea]. Available: https://www.argentina.gob.ar/onti. [Último acceso: 06 03 2019].

[19] D. Kosutic, «Lista de documentos obligatorios exigidos por la norma ISO 27001 (revisión 2013),» 27001 Academy - Advisera, [En línea]. Available: https://advisera.com/27001academy/es/knowledgebase/lista-de-documentos-obligatorios-exigidos-por-la-norma-iso-27001-revision-2013/. [Último acceso: 06 03 2019].

[20] SGSI - Blog especializado en Sistemas de Gestión de Seguridad de la Información, «ISO 27001: Aspectos organizativos para la Seguridad de la Información,» 8 4 2015. [En línea]. Available: https://www.pmg-ssi.com/2015/04/iso-27001-aspectos-organizativos-para-la-seguridad-de-la-informacion/. [Último acceso: 6 3 2019].

[21] M. Gil García, «La Administración Pública de la Provincia de Buenos Aires como ámbito laboral,» [En línea]. Available: http://www.memoria.fahce.unlp.edu.ar/trab_eventos/ev.4694/ev.4694.pdf. [Último acceso: 6 3 2019].

[22] S. P. R. &. T. A. Judge, Comportamiento Organizacional - Decimotercera Edición, México: Pearson Educación, 2009.