Universidad de Buenos Aires
Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Trabajo Final de Maestría

Tema

Aplicación de COBIT® 2019 para la protección de las infraestructuras virtuales de una organización

Título

Desarrollo de un Plan para la gestión de la seguridad de la información de la infraestructura tecnológica virtual y sistemas convergentes en la Universidad Estatal a Distancia de la República de Costa Rica

Autor:
Pablo Roberto Sandoval Barrantes

Directora de Trabajo Final de Maestría:
Mg. Patricia Prandini

Año de presentación: 2021
Cohorte: 2018

Declaración Jurada

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.

FIRMADO

Pablo Roberto Sandoval Barrantes

DNI: 95853656, Pasaporte Costarricense: 401940201

Resumen

La presente investigación estudia de forma particular la situación de la seguridad de la información de las infraestructuras tecnológicas virtuales de la organización. Para este fin, hace una reseña del avance tecnológico en que han estado inmersas las diferentes compañías e instituciones en los últimos años e invita a reflexionar sobre meditar cómo enfrentar profesionalmente lo que encontraremos en un futuro próximo en materia de seguridad de la información.

Para la comprensión del tema y el desarrollo investigativo, se recurre al caso real de la Universidad Estatal a Distancia en Costa Rica, institución que ha ido evolucionando tecnológicamente a través de diversos procesos en la última década, transformándose en un caso ejemplar en materia de educación a distancia con cobertura a nivel nacional y sustentada en tecnologías de la información.

Por lo anterior, esta investigación realiza un estudio consciente y profesional de la seguridad de la información de las plataformas tecnológicas virtuales, sustentando la veracidad de los hechos y resultados en la bibliografía existente y el aporte profesional del autor a partir de los saberes obtenidos en la Maestría en Seguridad Informática de la Universidad de Buenos Aires y su propia experiencia laboral. Para lograr el cometido, se recurre a la consulta de normativas en el campo de la seguridad informática, se profundiza en el análisis y la aplicación del marco de trabajo COBIT® 2019 como el ingrediente innovador que aporta las características necesarias para establecer las pautas en seguridad de la información que brinden respuestas a las necesidades de la organización en estudio. Ofrece finalmente conclusiones, buscando aportar valor en su interpretación y estimulo de nuevas investigaciones alrededor de esta temática de actualidad.

Palabras claves: Seguridad de la información, seguridad informática, UNED Costa Rica, COBIT® 2019, ISACA, Infraestructura tecnológica virtual.

Tabla de contenido

Índice de figuras

Índice de tablas

Agradecimientos

A Dios, mi esposa, mis padres, familiares y amigos, que en todo momento me brindaron el apoyo incondicional para cumplir la meta.

A la Universidad Estatal a Distancia (UNED) en la República de Costa Rica, Institución Benemérita de la Patria, que me patrocinó durante toda la carrera y además confió en mi persona la gran responsabilidad de formarme como Máster en Seguridad Informática en la República Argentina.

A todo el personal del Acuerdo de Mejoramiento Institucional (AMI), a la Unidad Coordinadora del Proyecto Institucional (UCPI) y el legado de su Directora Heidy Rosales Sánchez quien con un gran equipo de trabajo realizaron una admirable labor con las iniciativas que fortalecerán el modelo de educación a distancia en la UNED perdurando en el tiempo.

Al Consejo de Becas Institucional (COBI), por su labor en seguimiento durante el proceso de beca.

A todo el personal de la Dirección de Tecnología de Información y Comunicaciones (DTIC), liderados por el Mag. Francisco Durán Montoya, que me abrieron las puertas para ser parte del equipo y han depositado su confianza en este proceso.

A la Unidad de Infraestructura Tecnológica (UIT), liderados por el Mag. Rolando Rojas Coto, quienes me han brindado palabras de aliento y acompañamiento durante este proceso.

A todo el personal administrativo y docente de la carrera de Maestría de la Universidad de Buenos Aires en Seguridad Informática, que durante todo el proceso me acompañaron, me instruyeron, me guiaron y me brindaron todo el apoyo que necesité.

A la Mag. Patricia Prandini, por sus palabras de apoyo y guía profesional como directora del presente trabajo final de maestría.

Al Dr. Juan Pedro Hecht, Dr. Raúl H. Saroka y al Ing. Hugo A. Pagola, por su compromiso como tutores, su trayectoria científica y su entrega a la carrera.

A la República Argentina, a todas sus personas que me brindaron calor humano durante mi estadía en la Ciudad de Buenos Aires y que se convirtieron en mi familia argentina, me hicieron parte de esta gran Nación.

Nómina de abreviaturas

APO: Dominio de gestión de COBIT para Alinear, Planificar y Organizar

AWS®: *Amazon Web Services*. Plataforma de computación en la nube del fabricante Amazon Inc.

BAI: Dominio de gestión de COBIT para Construir, Adquirir e Implementar

BCP: *Business Continuity Plan* o Plan de Continuidad del Negocio

BIA: *Business Impact Analysis* o Análisis de Impacto al Negocio

CEN: Comité Europeo de Normalización.

CGR: Contraloría General de la República

CIS: Center for Internet Security

CMMI: *Capability Maturity Model Integration* o Integración de Modelo de Madurez de Capacidades

COBIT: *Control Objectives for Information and related Technology* u Objetivos de Control para Tecnologías de Información o Relacionadas

CONARE: Consejo Nacional de Rectores de las universidades públicas de Costa Rica.

CSIRT: *Computer Security Incident Response Team* o Equipo de Respuesta ante Incidencias de Seguridad Informáticas

CSIRT: *Computer Security Incident Response Team* o Equipo de Respuesta ante Incidencias de Seguridad Informáticas

CSIRT-CR: El CSIRT del gobierno de Costa Rica

CSIRT-UNED: El CSIRT de la UNED que coordina hacia el CSIRT-CR

DRP: *Disaster Recovery Plan* o Plan para la Recuperación de Desastres

DSS: Dominio de gestión de COBIT para Entrega, Servicio y Soporte

DTIC: Dirección de Tecnología de Información y Comunicaciones

EDM: Dominio de gobierno de COBIT para Evaluar, Orientar y Supervisar

EDT: Estructura Desagregada de Trabajo

EPE: Empresas de Propiedad Estatal

e-CF: *e-Competence Framework.* Describe habilidades técnicas en TI.

GETI: Gobierno Empresarial de Tecnologías de la Información

HITRUST®: *Health Information Trust Alliance*

ISACA: *Information Systems Audit and Control Association* o Asociación de Auditoría y Control de Sistemas de Información (ADACSI)

ISF: *Information Security Forum* o Foro de Seguridad de la Información

ISO/IEC: Organización Internacional para la Estandarización y la Comisión Electrotécnica Internacional

ITIL®: *Information Technology Infrastructure Library*

MEA: Dominio de gestión de COBIT para Supervisar, Evaluar y Valorar

MICITT: Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones

NIST: *National Institute of Standards and Technology* o Instituto Nacional de Estándares y Tecnología

NOC: *Network Operation Center* o Centro de Operaciones de Red

PDS: Plan Director de Seguridad

PMBOK®: *Project Management Book of Knowledge*

SEVRI: Sistema Específico de Valoración del Riesgo Institucional de la UNED

SGSI: Sistema de Gestión de la Seguridad de la Información

SI: Seguridad de la información

SIEM: *Security Information and Event Management* o Sistema de Gestión de Información y Eventos de Seguridad

SOC: *Security Operation Center* o Centro de Operaciones de Seguridad

SOGP: *Standard of Good Practice for information security* o Estándar de Buenas Prácticas para la seguridad de la información

TFM: Trabajo Final de Maestría

TI: Tecnologías de Información. También puede referirse al departamento responsable de las tecnologías de información.

TIC: Tecnologías de Información y Comunicaciones

T&I: Las tecnologías y la información.

UIT: Unidad de Infraestructura Tecnológica perteneciente a la DTIC

UNED: Universidad Estatal a Distancia de Costa Rica.

USD: Unidad de Seguridad Digital perteneciente a la DTIC

VMWare: *VMware Corporation*

VPN: *Virtual Private Network* o Red Privada Virtual

VxBlock: modelo de la unidad convergente del fabricante VCE

CAPITULO 1: INTRODUCCIÓN

El presente Trabajo Final de Maestría expone la importancia y particularidad de la seguridad de la información en las organizaciones educativas modernas, y como éstas deben apoyarse en las normativas que les sean aplicables o bien que desarrollen, para sobreponerse al constante avance tecnológico y los obstáculos que se presentan en el ámbito de la seguridad de la información.

Si bien el campo tecnológico de cada organización puede ser muy amplio y específico, resulta relevante estudiar las plataformas tecnológicas virtuales, donde comúnmente se delegan los servicios críticos de la empresa, y es además el foco de interés ante los incidentes que puedan comprometer la seguridad de su información.

También se incluye contenido referente a normativas relacionadas al campo de la seguridad de la información, descripciones útiles de las mismas, y como éstas pueden ser un valioso aporte para abordar los distintos casos que puedan presentarse en las organizaciones. Para esto último se profundizará en el análisis del marco de trabajo COBIT® 2019.

Como aplicación práctica, se aborda el caso real la Universidad Estatal a Distancia (UNED) en la República de Costa Rica, considerando el antecedente de esta institución, su tamaño y estructura como organización, las normativas que le son aplicables, el estado actual de la seguridad informática en torno a su infraestructura virtual con servicios en la nube y la aplicabilidad del marco de trabajo COBIT® 2019 como alternativa flexible para el gobierno y la gestión de la seguridad de la información en el tiempo.

1.1 Antecedentes

Los constantes avances tecnológicos alcanzan a la mayoría de las organizaciones alrededor del mundo. Estos avances adquieren cada vez mayor vertiginosidad y particularmente durante la última década, esto se ha convertido en un tema notable para toda entidad, al punto que el negocio y sus procesos caminan de la mano con la tecnología y su correcto uso.

Pero también con este acelerado avance, aparece la seguridad de la información como un asunto muy propio o particular de cada institución y se

vuelve clave proteger la información y los recursos involucrados. La Universidad Estatal a Distancia no escapa de esta realidad.

Por otra parte, los esfuerzos en normativa, regulaciones y cumplimiento han llevado a diferentes organizaciones a utilizar herramientas y metodologías a su alcance para abordar la seguridad de la información. En este sentido, COBIT® 2019 se presenta como un marco de trabajo para el gobierno y la gestión de la Tecnología y la Información, con la capacidad de responder a las exigencias modernas que marcan el ritmo de las organizaciones. A continuación, se presentan en forma más detallada algunos aspectos de la investigación realizada para este caso.

1.1.1 La idea de investigación

El planteo central del Trabajo Final de Maestría gira alrededor de la importancia que reviste la seguridad de la información en una infraestructura tecnológica virtual y sistemas convergentes que soportan los procesos tecnológicos críticos en la UNED. La idea de investigación es abordar la situación de la mencionada entidad como institución pública del sector educación superior, enfocándose en su actual situación tecnológica, la cual está estrechamente ligada al valor estratégico del negocio que es en esencia, entregar servicios de calidad a sus estudiantes en un modelo de educación a distancia.

Como lógica consecuencia de lo anterior, la UNED actualmente afronta una serie de necesidades en materia de seguridad de la información e incluso en temas de cumplimiento normativo ante entes superiores o reguladores del Gobierno de Costa Rica. Como ejemplo, pueden citarse los que surgen de las Normas Técnicas para la gestión y el control de las Tecnologías de Información, las Normas de control interno para el sector público, el Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021 y la Estrategia Nacional de Ciberseguridad Costa Rica, entre otras.

Considerando la situación de la UNED, su Dirección de Tecnología viene realizando importantes esfuerzos en materia de seguridad de la información. Sin embargo, no ha desarrollado aún un Plan Director que contemple la gestión de la seguridad en los equipos adquiridos recientemente para implementar la plataforma virtual que brinda servicios

centrales para la casa de estudios. Para lograrlo, lo que propone el presente documento es utilizar un marco de trabajo reconocido y flexible, que permita potenciar las tecnologías de información de la institución y sus políticas, gestionar la seguridad de la información y desarrollar de este modo un plan para una gestión de la seguridad que resulte sustentable en el tiempo.

A estos fines, se ha determinado que COBIT® 2019 es el marco que constituye una base adecuada por su enfoque empresarial, basado en procesos. Por lo tanto, se trabajará aplicándolo en el caso de la UNED, para así indagar y comprender aspectos vinculados a la gestión de la seguridad de la información en equipos y servicios virtuales, de manera que se utilice dicho marco para establecer una metodología de trabajo innovadora para el ambiente antes descripto.

1.1.2 Contexto y evolución de la infraestructura tecnológica de la UNED

Si bien existe registro de tecnología de virtualización desde la década de 1960, el auge mundial más significativo se presentó después de la aparición del hipervisor como componente clave perfeccionado por VMware Inc. en el año 2006, dando origen al concepto que se conoce actualmente como Infraestructura Virtual.

La Universidad Estatal a Distancia en Costa Rica también debió adaptarse a la evolución tecnológica, ya que hasta el año 2002 su Oficina de Sistemas era la que se encargaba de procesos genéricos relacionados a servicios básicos de tecnología. A partir de ese momento, la administración de la Institución decidió sustituirla o potenciarla creando la Dirección de Tecnología de Información y Comunicaciones (**DTIC**), con la intención de darle un rol estratégico para los procesos de la Universidad.

Casi paralelamente, para finales de la década del 2000, surge una gran demanda de servicios tecnológicos en red para las diferentes organizaciones en el mundo y la tecnología virtual se consolida en el ámbito empresarial. Efectivamente, los centros de datos tradicionales se transforman en infraestructuras cada vez más complejas. Lo anterior ocasionó que la recién creada DTIC, tuviera que hacer frente a las exigencias descritas, a través de sus unidades estratégicas. Sin embargo, el

presupuesto asignado se tornó en una limitación, que sumado a infraestructura obsoleta en servidores físicos alojados en un centro de datos que no estaba acondicionado para albergarlos, generó una situación crítica que apenas pudo moderarse a través de la aplicación de buenas prácticas para la gestión de la tecnología.

Para el año 2010 en la UNED se había logrado establecer una granja de servidores físicos, reemplazar algunos equipos obsoletos y realizar mejoras en los equipos de red y cómputo en general, permitiendo mantener un centro de datos operativo. Al mismo tiempo, se observaba una mayor demanda de servicios en red, lo que ocasionó una cascada de dificultades tecnológicas y presupuestarias. Debido a la falta de recursos para hacer frente a los nuevos y numerosos servicios, se instalaron una serie de servidores "satélites" administrados por dependencias ajenas a TI, pero consumiendo espacio y energía en un centro de datos obsoleto en su diseño.

Es entonces que la DTIC a través de su Unidad de Infraestructura Tecnológica (**UIT**), inicia con sus primeros proyectos de virtualización en busca de una mejora u optimización de espacio y del recurso tecnológico, enfocándose principalmente en eliminar modelos anteriores de servidores físicos y servicios "uno a uno".

La etapa más reciente y la más drástica en avance tecnológico para la UNED y la DTIC sucede desde el año 2014 hasta la actualidad, en la que se dedica un importante esfuerzo en la gestión de TI para optimizar la infraestructura virtual mediante pruebas de concepto, junto a su análisis económico. Se suma a esto una fuerte inversión económica por parte del Gobierno de Costa Rica, destinada a instituciones públicas de educación superior, permitiendo la construcción de un nuevo centro de datos para la UNED, diseñado con las condiciones y normas adecuadas. Además, la UNED modernizó casi la totalidad de su parque tecnológico, sus redes de comunicaciones y equipos de cómputo, así como la infraestructura de sus más de 40 centros universitarios. Incluso se construyó un centro de datos alterno para soportar los servicios críticos del centro de datos principal, en caso de algún evento de desastre.

Todo lo anterior muestra como la infraestructura tecnológica de la UNED en un período relativamente breve para una institución pública de tal envergadura, pasó del anonimato a un rol estratégico para la organización a través de la DTIC. Sin embargo, en forma paralela se registró una serie de nuevas necesidades, alrededor del nuevo entorno tecnológico ya que, si bien muchos servicios críticos y dinámicos están soportados por la nueva infraestructura virtual en el centro de datos, esto no resulta suficiente para garantizar el cumplimiento de las normativas tanto de legislación nacional, como las internas para la UNED. Resulta entonces más relevante la situación de la seguridad de la información procesada en los sistemas informáticos de la UNED, incluyendo los datos de sus más de 30.000 estudiantes y 2.000 funcionarios, de gran valor estratégico para la universidad, por mencionar solo un caso puntual.

A partir de lo referido, resulta importante no perder de vista cómo las organizaciones crecen acelerada y dinámicamente con la tecnología y las demandas de los usuarios y el personal también lo hacen. Ante esto, las diferentes metodologías, normativas, regulaciones y marcos de trabajo, también se transforman y se presentan como herramientas y actores claves para solventar las necesidades específicas de cada organización. Es este el caso puntual de COBIT® 2019, renovado y actualizado para las exigencias actuales, y como se verá más adelante en este documento, proveyendo una serie de pautas claves para abordar la situación descrita dentro de la UNED en materia de seguridad de la información.

1.1.3 Enfoque de la investigación

Para la presente investigación se utilizará un enfoque mayormente cuantitativo, a partir de lo descrito en el caso de estudio de la seguridad de la información en la UNED ya que se expondrán datos reales. El enfoque a utilizar “usa la recolección de datos para probar hipótesis, con base en la medición numérica y el análisis estadístico para establecer patrones de comportamiento y probar teorías [1]”. Efectivamente y desde los resultados, se pretende obtener un estudio exploratorio el cual “Se realiza cuando el objetivo consiste en examinar un tema poco estudiado [1]” como lo es el marco de trabajo COBIT® 2019 de reciente aparición en su versión actual y

aplicarlo a la realidad dentro de la UNED con el fin de trabajar sobre la seguridad de la información de esta organización en particular.

1.2 Planteamiento de la problemática

Considerando el antecedente definido previamente, a continuación, se profundiza con más detalle el problema.

1.2.1 Problemática de la organización y su tecnología

La UNED ha logrado adquirir diversos recursos de vanguardia gracias al compromiso e inversión de la administración, sumado a una gestión adecuada de la DTIC. Esto trae consigo una responsabilidad considerable sobre los nuevos equipos virtuales, los cuales soportan muchos servicios críticos de la institución.

En el periodo comprendido entre los años 2014 y 2019, se logró adquirir y modernizar la actual infraestructura de tecnología informática de la Institución. Puntualmente se adquirieron los equipos principales que soportan la red y el centro de datos, este último con la adquisición de una unidad o sistema convergente modelo Dell EMC VxBlock System 340, debidamente configurado en julio del 2017, y destinado a soportar 98 servidores virtuales con los servicios de nivel más alto de criticidad identificados por la DTIC. Adicionalmente a este equipo convergente, se cuenta con 2 clústeres de servidores físicos para virtualización que alojan 46 servidores virtuales para atender servicios de nivel medio y bajo de criticidad.

La infraestructura tecnológica virtual descrita en el párrafo anterior ha demostrado un alto y exitoso desempeño en sus primeros años. Esto también se logró en base a una adecuada gestión por parte de la DTIC, de cara a un mantenimiento viable para los próximos años, que además debe estar alineado a los objetivos institucionales y coyunturales. Esto requirió trabajar aspectos tecnológicos y de seguridad de la información en conjunto con las áreas de administración, incluyendo aspectos del negocio vinculados al servicio de educación a distancia.

Lo anterior denota la problemática que han traído estos equipos virtuales, ya que más allá del esfuerzo por adquirirlos y administrarlos, estos

contienen la mayor parte de la información valiosa para la institución y sus usuarios, por lo que se requieren recursos humanos especializados para llevar adelante un arduo trabajo en seguridad de la información para poder darles una adecuada protección.

1.2.2 Problemática por resolver en seguridad de la información

Por lo mencionado, la UNED enfrenta el desafío de atender nuevas amenazas tecnológicas, específicamente a través de la DTIC, particularmente en los equipos de infraestructura virtual que soportan la mayor parte de la operación.

Si bien, se realizan esfuerzos para manejar de manera tradicional algunos aspectos de seguridad y se trabaja en la gestión de algunos riesgos de TI anualmente, lo cierto es que la seguridad de la información presenta un atraso importante en presupuesto, recursos humanos y gestión.

Para el 2019, con la infraestructura virtual funcionando en producción y soportando plena operación, la administración de la UNED le asigna a la DTIC una persona adicional para trabajar en la protección de la información, completando así apenas 2 recursos humanos destacados en la Unidad de Seguridad Digital (USD) para atender el tema.

Dentro de estos esfuerzos, en julio del 2019 se plantean las primeras reuniones para analizar, entre otros temas, cómo establecer una dinámica de trabajo entre el personal de infraestructura y el de seguridad digital. En esta línea, se envió a la administración de la UNED una solicitud sobre la conformación del CSIRT institucional lo cual fue aprobado con urgencia, se asignó apoyo adicional a seguridad por parte del recurso humano del área de analistas desarrolladores, se enfatizó en la necesidad de capacitaciones y formación en seguridad informática de todo el personal involucrado, se revisó la inversión en herramientas tecnológicas actuales y por adquirir, se abordaron temas de privilegios y accesos en los equipos críticos así como en las plataformas utilizadas por los usuarios finales y en términos más generales, se planteó la necesidad de revisar a mediano plazo temas de monitoreo (NOC-SOC, SIEM), antivirus, inversiones anuales, protocolo de reportes de incidentes y control de privilegios de acceso (centralizados en infraestructura).

Lo anterior evidencia el interés institucional por trabajar en el aseguramiento de los equipos virtuales y de los servicios que éstos soportan. En este sentido, si bien se tiene conocimiento general de lo que se necesita, se observa la brecha de seguridad de la información existente en la UNED causada por una inversión importante en tecnología que trajo consigo una carga de nuevas acciones a realizar en materia de seguridad de la información. Urge, por lo tanto, asignar una mayor inversión y recursos de gestión, a fin de enfrentar las constantes amenazas en ciberseguridad.

Adicionalmente, se tiene mandato de entes gubernamentales superiores para mejorar o implementar aspectos de tecnología y seguridad en la institución. Esto se aprecia por ejemplo en lo establecido por la Contraloría General de la República en su documento sobre “Normas Técnicas para la gestión y el control de las Tecnologías de Información”, en el “Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021” y en la Estrategia Nacional de Ciberseguridad de Costa Rica, siendo estos dos últimos promovidos por el Ministerio de Ciencia y Tecnología del Poder Ejecutivo.

Las situaciones mencionadas colocan a la UNED en una situación que requiere acciones concretas. Por una parte, si mantiene su estado actual de seguridad de la información se incrementará la probabilidad de sufrir el impacto de nuevas amenazas. Como contraparte, en caso se asignen los recursos necesarios, surge la oportunidad de negocio de atender adecuadamente el problema de la seguridad de la información no solo para salvaguardarla, sino para generar valor para sus usuarios mientras que al mismo tiempo se da cumplimiento a las regulaciones estatales, aportándole solidez y calidad a la educación y al país en general.

1.2.3 Diagrama situacional

A continuación, se muestra el diagrama con los principales actores en torno a la infraestructura virtual que soporta la mayor parte de la operación en la UNED. Se observa que tanto los factores gubernamentales externos como la administración interna de la UNED, se relacionan con la gestión de TI a través de la DTIC y sus unidades estratégicas. Esto condiciona el funcionamiento de la infraestructura virtual y los servicios que se brindan, por

lo que la protección de estos equipos toma un rol fundamental para la institución y se convierte en objeto de estudio.

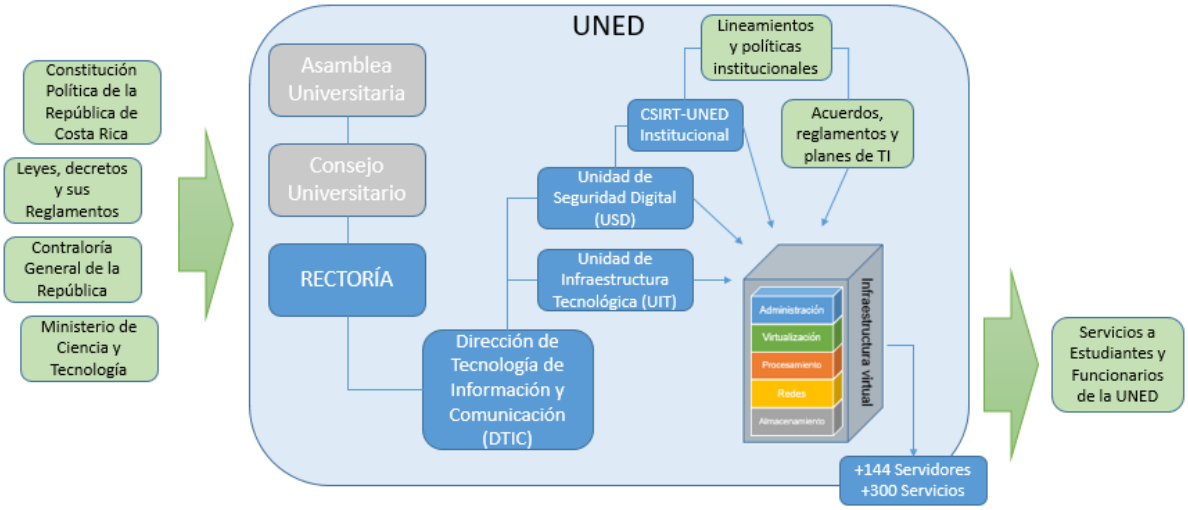


Ilustración 1: La infraestructura virtual soporta la operación de los principales servicios de la UNED, la cual es influenciada por factores internos y externos que requieren revisión en seguridad informática.

Fuente: Elaboración propia.

1.2.4 Preguntas de investigación

Teniendo en consideración lo descrito en los anteriores apartados, resulta útil plantear una serie de preguntas para analizar la situación actual de la UNED, su infraestructura virtual, en nivel de protección de ésta y la necesidad de un abordaje de este tema por parte de la organización:

¿Existe un antecedente relacionado a la seguridad de la información que recibe tratamiento en los equipos críticos de la UNED?

¿Se cuenta con información precisa de la infraestructura virtual de la UNED, identificando los activos de información que la componen?

¿La UNED tiene claramente definidos los procesos y servicios críticos soportados por los equipos virtuales que administra la DTIC?

¿Cuenta la UNED con un sistema de gestión de la seguridad de la información adecuado?

¿Se considera o se trabaja con un marco de trabajo sólido y reconocido para la gestión de la seguridad de la información que, además, sea sustentable en el tiempo?

1.3 Justificación

1.3.1 Importancia de la investigación

Como ya se mencionó, la UNED está atravesando una etapa de transformación, con importantes inversiones en tecnología y requerimientos altos de recursos humanos especializados, con el fin de implementar un modelo de negocio que permita brindar servicios de educación superior a distancia a lo largo y ancho del país. Ese rol para el cual fue creada la UNED, ha tomado gran relevancia en la actualidad, por su alcance nacional y una importante cantidad de estudiantes inscritos anualmente en las diferentes carreras universitarias que ofrece.

Dentro de los diferentes procesos de la UNED, que dependen cada vez más de la tecnología al alcance de la institución, se encuentran los procesos administrativos de diversas oficinas, como el área financiera, de recursos humanos, comunicación, audiovisuales, centros universitarios regionales y otras dependientes de las vicerrectorías ejecutiva y planificación. También se involucran procesos de las vicerrectorías de investigación y académica, con una importante cantidad de información del ambiente académico conformado por investigadores, profesores y estudiantes. Esto último se ha convertido en los últimos años en un foco importante para las amenazas en seguridad, pasando de procesos caracterizados por la presencia física desde la década de 1970, a un ámbito totalmente digital en la actualidad.

Considerando la situación de la UNED, con el fin de dar continuidad al trabajo que viene realizando tanto su área administrativa como la DTIC, así como aprovechar la inversión tecnológica realizada y el recurso humano comprometido con el interés institucional, se buscará mediante este trabajo investigativo hacer un aporte en seguridad de la información que promueva o mejore la situación presente y futura de los procesos críticos, soportados en la infraestructura virtual a cargo de la DTIC.

Además, surge la oportunidad de realizar una investigación que permita intervenir la situación de la seguridad de la información de la UNED con la metodología de trabajo COBIT® 2019, y consolidar un Plan Director

para la gestión de la seguridad de la información, que le aportará valor a la gestión.

1.3.2 Beneficios

Dentro de los beneficios más relevantes que se identifican al promover la presente investigación, se puede mencionar la respuesta fundada al interés institucional de abordar de manera profesional la seguridad de la información en los procesos críticos que tienen lugar en la infraestructura virtual de la DTIC y en los servicios brindados. Con los resultados obtenidos las autoridades tendrán una visión más precisa del nivel de protección de la información, lo cual les permitirá tomar mejores decisiones a mediano y largo plazo.

Se producirá un documento que además de presentar la situación, ofrecerá una serie de pautas adaptadas a la institución para la gestión de su seguridad informática, no invasivo en los procesos y funciones ya establecidos por las partes involucradas, sino a manera de aporte flexible basado en el marco de trabajo COBIT® 2019. Esto le permitirá orientar y sostener en el tiempo la gestión de la seguridad de la información.

Se espera también que, a partir del presente Trabajo Final de Maestría, los servicios tecnológicos muestren una mejora en la calidad, contribuyendo a optimizar el manejo de la información personal y a mejorar su nivel de disponibilidad en todo momento.

Además de lo mencionado, se conseguirá una mejora en la protección de la reputación institucional ante las partes involucradas, incluyendo la población estudiantil y la sociedad en general, el reconocimiento de la universidad estatal como proveedora de servicios académicos de alta calidad y el cumplimiento de las leyes y reglamentos destinados a la modernización en temas de seguridad de la información de las instituciones públicas.

1.3.3 Beneficiarios

Considerando que la presente investigación permite proteger la infraestructura computacional de la UNED, compuesta por ambientes virtuales, además de entregar un plan director para la implementación del sistema de gestión de la seguridad de la información a la DTIC, sustentado

sobre COBIT® 2019 como marco de trabajo sólido, los principales beneficiarios son:

-La Universidad Estatal a Distancia como Institución Benemérita de la Patria, ya que se fortalecerá su reputación en la sociedad costarricense a través de servicios de calidad y ejemplo en la vanguardia en seguridad de la información.

-La DTIC y sus dependencias como ente director de TI responsable de la seguridad de la información, ya que contará con un plan director para abordar adecuadamente la protección de la información, con capacidad de toma de decisiones en la materia y planificación a corto y largo plazo.

-Las instituciones gubernamentales superiores con interés en la mejora tecnológica de la UNED, que obtendrán resultados más concretos en el cumplimiento de leyes y reglamentos.

-Los estudiantes de la UNED, como usuarios finales que confían su información en los servicios que la UNED brinda, al contar con servicios de calidad que salvaguardarán sus datos personales con herramientas a la altura de las actuales exigencias en ciberseguridad.

-Los funcionarios de la UNED, quienes como usuarios de los sistemas de la UNED son responsables de la información de estudiantes y terceros a la que tienen acceso y a su propia información, y serán respaldados en sus funciones a través de una correcta gestión de la seguridad de la información.

1.4 Objetivos

1.4.1 Objetivo general

Evidenciar la importancia de proteger la infraestructura tecnológica de la UNED, compuesta por ambientes virtuales y sistemas convergentes e hiperconvergentes, y generar sobre esa base, un Plan Director para la implementación del sistema de gestión de la seguridad de la información, sobre la base de un marco reconocido internacionalmente.

1.4.2 Objetivos específicos

Analizar la infraestructura convergente, hiperconvergente, y servicios en la nube existente en la UNED, desde la perspectiva de la protección de los activos que la componen.

Determinar los procesos y servicios críticos brindados a través de la infraestructura tecnológica de virtualización en la UNED.

Evaluar, mediante la aplicación de COBIT® 2019 como marco de trabajo para el gobierno y la gestión de las Tecnologías y la Información, la seguridad de la información, particularmente en lo que respecta a los equipos físicos y virtuales y los servicios ofrecidos a través de la infraestructura tecnológica de virtualización en la UNED.

Generar un plan director para la gestión de la seguridad informática de los equipos físicos, virtuales, y para los servicios ofrecidos a través de la infraestructura tecnológica antes mencionada.

CAPÍTULO 2: MARCO TEÓRICO

El presente capítulo recopila el sustento teórico necesario para comprender los aspectos de seguridad relacionados con los procesos tecnológicos de la UNED involucrados en la investigación. Además, presenta alternativas para enfrentar la problemática y destaca el valor que tiene para la institución trabajar con el marco de trabajo COBIT® 2019.

2.1 La UNED, educación a distancia en Costa Rica

La UNED es la única universidad estatal que provee el servicio de educación superior en modalidad a distancia en Costa Rica, tarea que viene realizando desde hace más de cuatro décadas, desde su creación en el año 1977.

Para comprender qué implica estudiar a distancia dentro del contexto costarricense y siendo la UNED la institución pionera en el campo, esta define en su portal web “que la persona que estudia con nosotros debe organizar su tiempo de manera que, sin tener que desatender sustantivamente otras responsabilidades como la familia, el trabajo, o verse obligado a realizar largos y costosos desplazamientos, pueda cumplir con el estudio al desarrollar las unidades académicas que le propone cada curso o asignatura. [2]”

Para lograr el objetivo descrito anteriormente, la UNED evolucionó en el tiempo pasando de utilizar antiguos canales como entrega por correspondencia física, documentación impresa y telecomunicaciones analógicas, para llegar a canales informáticos en los cuales se apoya hoy día a través de recursos tecnológicos diversos. Efectivamente, indistintamente del canal utilizado, “el fundamento filosófico de la UNED coloca al estudiante como el centro del proceso [3]”. Por lo tanto le brinda a la población estudiantil el acceso a una estructura que contiene entre sus principales componentes digitales: un portal web, tutoría virtual, el repositorio con acceso libre a materiales académicos, la plataforma para la enseñanza-aprendizaje (“medio virtual por el cual los estudiantes acceden a materiales y actividades organizados por un tutor [3]”), el entorno estudiantil para gestiones administrativas, el servicio de audiovisuales o conjunto de

recursos digitales, el servicio de videoconferencia, la biblioteca en línea con "grandes e importantes bases de datos que ofrecen libros, revistas o artículos digitales [3]" y las redes sociales con cuentas institucionales en Facebook y Twitter, entre otros.

En cuanto a su alcance geográfico y demográfico, la UNED es una institución inclusiva, que pretende alcanzar a toda la población con la misión de "ofrecer educación superior a todos los sectores de la población, especialmente a aquellos que, por razones económicas, sociales, geográficas, culturales, etarias, de discapacidad o de género, requieren oportunidades para una inserción real y equitativa en la sociedad. Para ello, hace uso de diversos medios tecnológicos… [4]". Lo dicho obliga a la UNED a mantener una importante infraestructura de telecomunicaciones que soporta la operación a nivel nacional, conectando más de 40 Centros Universitarios a los cuales les entrega diversos servicios digitales alcanzando a más de 30 mil [1]estudiantes activos anualmente.

A continuación, se presenta el detalle de la distribución geográfica de los diferentes Centros Universitarios interconectados que permiten a la UNED brindar sus servicios a las diferentes regiones del país.

Ilustración 2: Distribución geográfica de los Centros Universitarios de la UNED en Costa Rica.

Fuente: https://www.uned.ac.cr/index.php/centros-universitarios. Web UNED Costa Rica.

[1] Fuente: Centro de Investigación y Evaluación Institucional de la UNED, Anuario estadístico 2018 disponible en: https://www.uned.ac.cr/viplan/images/ciei/018_Anuario_2018_07-08-2019.pdf (pag24)

2.2 Seguridad de la Información

Como ya se mencionó, la seguridad de la información es un concepto que viene tomando relevancia en la última década. Efectivamente, “las personas están exponiendo su privacidad, volcando datos públicos y privados en entornos tecnológicos, en muchas ocasiones por desconocimiento o por la necesidad de utilizar un servicio bajo ciertas condiciones del proveedor [5]”.

Entonces, resulta importante traer a la luz tanto el concepto de seguridad de información como el de seguridad informática. El primero implica “asegurar la identificación, valoración y gestión de los activos de información y sus riesgos, en función del impacto que representan para una organización [6]”, entendiendo que “no se centra en la protección de las TIC sino de todos los activos de información que son de un alto valor para la institución [6]” contemplando incluso la información que pudiese estar contenida en medios físicos no tecnológicos. En contraparte, el concepto de seguridad informática es definido como “la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable [7]”. En otras palabras, “se entiende que mantener un sistema seguro y fiable, es garantizar tres aspectos: su confidencialidad, integridad y disponibilidad. [8]” pudiéndose incluso ampliar a más propiedades como la autenticidad, la responsabilidad, la fiabilidad y el no repudio, pero siempre aplicado a un medio electrónico.

Los conceptos anteriores toman más sentido si lo denotamos en cualquier entorno cotidiano personal o empresarial. Efectivamente, es difícil pensar en las sociedades globalizadas sin relacionarlas estrechamente con servicios tecnológicos virtuales y en la nube, desde acciones tan simples como revisar el correo electrónico, enviar un mensaje instantáneo por aplicaciones móviles, o al realizar acciones más críticas como trámites bancarios o utilizar servicios gubernamentales obligatorios para renovar documentación o pagos de impuestos, por solo dar ejemplos básicos. Todo eso solo incrementa la necesidad de acudir a la seguridad de la información

como medida obligatoria para no exponerse a las amenazas constantes en el campo tecnológico y no terminar pagando un alto costo en recursos.

Además, el constante avance tecnológico desemboca en nuevas y constantes tecnologías emergentes, las cuales se orientan a las modernas infraestructuras virtuales y de cómputo en la nube, pero también abren nuevas brechas en ciberseguridad, habilitando nuevas amenazas y vulnerabilidades que afectan tanto a los usuarios como a las organizaciones. Esto eleva la urgencia de trabajar en la concientización en seguridad de la información, formar profesionales en seguridad informática e implementar una adecuada gestión de la seguridad de la información, acorde a la necesidad de los usuarios y empresas modernas.

2.3 Seguridad de la información en Infraestructuras virtuales

Las organizaciones modernas tienen un acceso cada vez mayor a servicios virtuales enfocados a internet, tanto por los implementados en infraestructura virtuales en sus propios establecimientos, como los que puedan contratar a un tercero. Esto plantea una serie de aspectos que se deben considerar en torno a la seguridad de los sistemas y de la información procesada en estos ambientes.

Dentro de las características principales a considerar se puede mencionar la seguridad física de los equipos que soportan la operación, la seguridad de los equipos virtualizados, la identificación de vulnerabilidades en estas plataformas, el diseño seguro de la red informática, el uso de modelos seguros en programación, la separación de entornos para los servicios y la revisión de acuerdos de servicio y seguridad por parte de terceros, así como una correcta gestión de la seguridad informática que contemple además de los aspectos antes mencionados, otras cuestiones propias de la organización.

Lo anterior ha vuelto más importante los conceptos de gobierno y gestión en la organización. En este sentido, ISACA lo ha venido acuñando en torno a la tecnología de información desde hace varios años y en forma más explícita menciona:

> “El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que

se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas [9]".

Y continúa con el concepto de gestión indicando:

"La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales [9]".

Entonces los servicios tecnológicos virtuales con los que cuente una organización son parte de los distintos procesos que se ven alcanzados por el Gobierno y Gestión de la empresa, y por consiguiente deben ser considerados, estudiados, e incluidos en las políticas, normas y procedimientos de la institución.

En este marco, estos servicios y equipos virtuales se ven particularmente afectados por las decisiones de las autoridades y son gestionados por la gerencia de tecnología de la información. Sin embargo, la seguridad de la información ha tenido un avance significativo respecto a la visión de su gobierno y gestión. Incluso COBIT® 2019 se ha presentado como un marco de trabajo que cubre la tecnología de la información de extremo a extremo, e incluye aspectos muy puntuales respecto a la seguridad de la misma. Surge de lo anterior, la oportunidad de aprovechar la metodología de COBIT® 2019 para analizar el caso de la seguridad de la información de los equipos y servicios virtuales de la UNED, aplicando conceptos sólidos de gobierno y gestión, sobre la base de políticas institucionales existentes y revisando normativas aplicables, que se describirán a continuación.

2.4 Gobierno y gestión en seguridad de la información.

En la actualidad, para comprender el gobierno y establecer el contexto para una adecuada gestión de la seguridad de la información, hay que entender de antemano que las empresas vienen incorporando durante la última década el concepto del Gobierno Corporativo, "definido ampliamente como la correcta asignación de poderes y responsabilidades entre el directorio, la administración y los propietarios de una empresa [10]". A partir

de lo señalado, las entidades buscan fortalecer “los órganos de dirección y control de las empresas (asamblea de accionistas o propietario, directorio y gerencia), al tiempo que definen reglas claras de juego entre los actores, e incrementan el nivel de transparencia y rendición de cuentas frente a grupos de interés [10]”. Más recientemente las empresas de propiedad estatal (EPE) también están viéndose envueltas en este concepto con el fin de implementar “mejores principios y prácticas de Gobierno Corporativo como mecanismo para fortalecer sus capacidades, tanto institucionales como gerenciales, y promover la transparencia y efectividad de su gestión [10]”.

También resulta conveniente traer a foco los conceptos de Gestión de Riesgo y Cumplimiento, siendo el primero “el proceso de identificar, analizar y responder a factores de riesgo a lo largo de la vida de un proyecto y en beneficio de sus objetivos [11]”, mientras que el segundo “consiste en establecer las políticas y procedimientos adecuados y suficientes para garantizar que una empresa desarrolle sus actividades y negocios conforme a la normativa vigente y a las políticas y procedimientos internos, promoviendo una cultura de cumplimiento entre sus empleados, directivos y agentes vinculados [12]”. De manera que, promoviendo el concepto de Gobierno Corporativo junto con la Gestión del Riesgo y el Cumplimiento, podemos hablar de GRC como “un modelo de gestión que integra las actividades y funciones de gobierno corporativo, la gestión del desempeño, la administración de riesgos y las responsabilidades de cumplimiento, mejorando con esto la capacidad de las empresas para lograr sus objetivos de negocio [13]”.

Entonces, de las definiciones anteriores se puede obtener un panorama más claro del modo en que las organizaciones modernas pueden desarrollar modelos de gestión capaces de integrar las distintas áreas de la empresa en consecución de los objetivos del negocio. Las tecnologías informáticas y las cuestiones vinculadas a la seguridad de la información no escapan a esta situación y pueden vislumbrarse como áreas beneficiarias de estos modelos al permitirles generar valor al tiempo que toman un rol más protagónico ante las autoridades.

Por lo tanto, ante un panorama empresarial como el descrito, el área encargada de seguridad de la información debe responder a la altura,

alineando su Gobierno de la Seguridad de la Información con el Gobierno Corporativo, y para esto debe recurrir a una estrategia que le permita integrar a todos los involucrados y responder en tiempo y forma a los requerimientos de las autoridades. En este punto, entra en juego una correcta Gestión de la Seguridad de la Información por parte del área de seguridad de la información, con capacidad de administrar los recursos y producir resultados, en base al nivel de riesgo de seguridad, fortaleciendo la disponibilidad, integridad y confidencialidad de la información.

Para abordar los conceptos antes mencionados y brindar a los distintos actores de la organización las herramientas con que enfrentar las exigencias en materia de protección de la información, se tiene como posible punto de partida a las normas publicadas por ISO/IEC. Una de las primeras normas a considerar es la ISO/IEC 27014:2013 que es una guía de conceptos y principios aplicables al Gobierno de Seguridad de la Información. En esta norma se menciona cómo involucrar a las partes interesadas y generar valor. Pero, por otra parte, se tiene disponible el marco de trabajo COBIT® 2019, como base para el correcto Gobierno y Gestión de Tecnología y la Información de toda la organización, pudiéndose utilizar para establecer la Gestión de la SI. Esto abarca los procesos de gestión y los de gobierno mediante el ciclo PDCA para su mejora continua en el tiempo y convive con normas existentes, por ejemplo, ISO/IEC 27001 sobre el Sistema de Gestión de la Seguridad de la Información (SGSI), e ISO/IEC 27002 (Buenas prácticas de Seguridad de la Información), entre otras. Estos estándares se revisarán con mayor detalle más adelante.

2.5 Regulaciones, políticas, normativa, reglamentos y estándares en seguridad de la información existentes en la UNED.

La UNED es una institución estatal que cuenta con autonomía organizativa, administrativa y de gobierno corporativo, pero también responde por objetivos ante instancias superiores del Estado costarricense, dado que se encuentra regulada por una serie de normativas, tanto internas como externas.

Por su parte, la DTIC tiene entre sus objetivos

"Elaborar el Marco Jurídico que contenga el compendio de leyes, reglamentos, acuerdos, pronunciamientos, contratos y otras normas aplicables a las Tecnologías de la Información y Comunicación, utilizadas por la Universidad Estatal a Distancia, esto con el fin de establecer las regulaciones legales, gubernamentales, técnicas, contractuales, de seguridad, confidencialidad y sensibilidad de la información en los equipos tecnológicos y en la red institucional, como en los procesos de transferencia electrónica de datos interna y externa a la UNED [14]".

Si bien este Marco Jurídico actualmente está compuesto por más de 42 documentos normativos de diverso origen, se listan a continuación los más relevantes para la Seguridad de la Información como objeto de estudio del presente trabajo:

Leyes y decretos (aplica a todas las instituciones estatales):

- Ley Nº 8454 de Certificados, Firmas y Documentos Electrónicos, 2005.
- Ley Nº 8642 General de Telecomunicaciones, 2008.
- Ley Nº 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales, 2011.
- Ley Nº 9048 de Delitos Informáticos y Conexos, 2012.
- Decreto Ejecutivo Nº 37052 Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) con sede en las instalaciones del Ministerio de Ciencia y Tecnología (Micitt), 2012.

Reglamentos nacionales:

- Reglamento a la Ley Nº 8454 de Certificados, Firmas y Documentos Electrónicos, 2006
- Reglamento a la Ley Nº 8642 General de Telecomunicaciones, 2008
- Reglamento a la Ley Nº 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales, 2013

Normas nacionales:

- Normas Técnicas para la gestión y el control de las Tecnologías de Información, 2007

- Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021, publicado en 2008.
- Estrategia Nacional de Ciberseguridad Costa Rica (Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), 2017.

Normativa Interna (aplica solamente dentro de la UNED):

- Reglamento para Uso de Equipos de Cómputo e Internet de la Universidad Estatal a Distancia, 2014.

Lineamientos y política institucional:

- Acuerdo CU-575-2002, Políticas para el Uso y Seguridad de internet. 2002.
- Políticas para el Uso y Desarrollo de Tecnologías de la Información y la Comunicación de la UNED, 2015.
- Prioridades Institucionales en Tecnologías de la Información y la Comunicación (TIC) que deberá atender la Dirección de Tecnologías de Información y Comunicación (DTIC), 2016.
- Conformación del Equipo de Respuesta a Incidentes de Seguridad Informática de la Universidad Estatal a Distancia vinculada a la Unidad de Seguridad Digital de la DTIC, 2019.
- Establecimiento y funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI), 2014.

Manuales elaborados por la UNED

- Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones de la Universidad Estatal a Distancia, 2017.
- Instructivos para la Gestión de Usuarios en la UNED. 2017

A partir del listado anterior, se puede comprender que la UNED a través de la DTIC ha venido trabajando durante la última década en cumplir normativas de acatamiento obligatorio. Además, ha elaborado una serie de documentos de manera interna que le permiten gestionar algunos aspectos en TI y en SI. Si bien son un insumo positivo y una oportunidad de mejora para la seguridad de la información de la institución, no resultan suficientes para resaltar la importancia de establecer una correcta gestión de la seguridad, que tome el aporte generado por la DTIC y lo revalorice dentro de

un Plan Director adecuado a las exigencias de actualidad, cuestión que resulta compatible con un marco de trabajo como COBIT® 2019, como se expondrá en la siguiente sección.

2.6 COBIT® 2019

Se presenta a continuación el rol que tiene COBIT® 2019 para las organizaciones y la justificación por la cual se considera pertinente justificar su utilización para abordar el caso de la UNED desde una perspectiva profesional y actualizada.

La primera versión de COBIT® fue publicada por primera vez en el año 1996 por ISACA bajo la denominación “Objetivos de Control para Tecnologías de Información o Relacionadas” (COBIT, por los términos en inglés). Esta sigla en la actualidad se utiliza como acrónimo. En su versión más actual, que es la 2019, establece como su principal objetivo ser el marco de negocios para el gobierno y la gestión de las tecnologías y la información empresariales.

En su primera versión, el enfoque de ISACA fue dirigirse a la auditoría de las tecnologías de información. En las siguientes versiones COBIT 2 del año 1998 y COBIT 3 del año 2000, se amplía el alcance dirigiéndolo a la auditoría, el control y la gestión. Pero es en la versión 4 del año 2005 y su extensión 4.1 del 2007, que por primera vez el alcance de COBIT incorpora el concepto de Gobierno. Para el año 2012 se consolida el Gobierno Corporativo en COBIT 5, siendo esta penúltima versión ampliamente utilizada hasta la fecha. Con la aparición de la versión más reciente, ISACA marca un hito importante en la historia de COBIT. Efectivamente, más allá de haber cambiado el criterio con el que se publican las versiones al denominarla COBIT® 2019, esta versión viene a mejorar la forma en que se aborda el Gobierno Corporativo comprendiendo que vivimos una transformación digital que merece prestar particular foco de atención en la información y tecnología (T&I).

COBIT® 5 ha sido ampliamente acogida por las organizaciones durante la última década, extendiendo su uso y reputación, mientras COBIT® 2019 viene incorporando cambios relevantes a considerar. Por eso

que a continuación se presenta una descripción más detallada de esas dos versiones de COBIT®:

2.6.1 COBIT® 5:

Haciendo un breve repaso de lo que ofrece y vuelve sólido a COBIT5, podemos afirmar que es un "marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas [9]". Esto se traduce en crear valor para el negocio, y optimizar el riesgo y los recursos. Para lograr lo anterior, COBIT 5 propone que las TI sean "gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin… [9]". Considera las partes interesadas internas y externas y "es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público [9]".

Para lograr su cometido, COBIT 5 se fundamenta en 5 principios a saber:

Ilustración 3: Los 5 principios en los que se fundamenta COBIT 5.

Fuente: COBIT 5 Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. [9]

2.6.2 COBIT® 2019:

En COBIT® 2019, ISACA explica cómo “la información y la tecnología (I&T) se han convertido en algo fundamental para el soporte, la sostenibilidad y el crecimiento de las empresas [15]”. Y es que “dada la importancia de la I&T para la gestión del riesgo empresarial y la generación de valor, en las últimas tres décadas se ha prestado una atención especial al gobierno empresarial de tecnologías de la información (GETI) [15]“. Lo anterior hace que el alcance de COBIT® 2019 se extienda al tiempo que se adapta a la necesidad actual al incluir en sus alcances al **Gobierno Corporativo de T&I**[2].

Para lograr lo propuesto, COBIT® 2019 se reinventa en sus principios, los cuales ya no son los 5 con los que tradicionalmente se venía trabajando, sino que propone 2 series de principios. El primer grupo “describe los requisitos fundamentales de un **sistema de gobierno para la Información y la Tecnología** de la empresa [16]”, mientras que el segundo, resulta “un **marco de gobierno que pueda usarse para crear un sistema de gobierno** para la empresa [16]”. Los principios se muestran en la siguiente imagen:

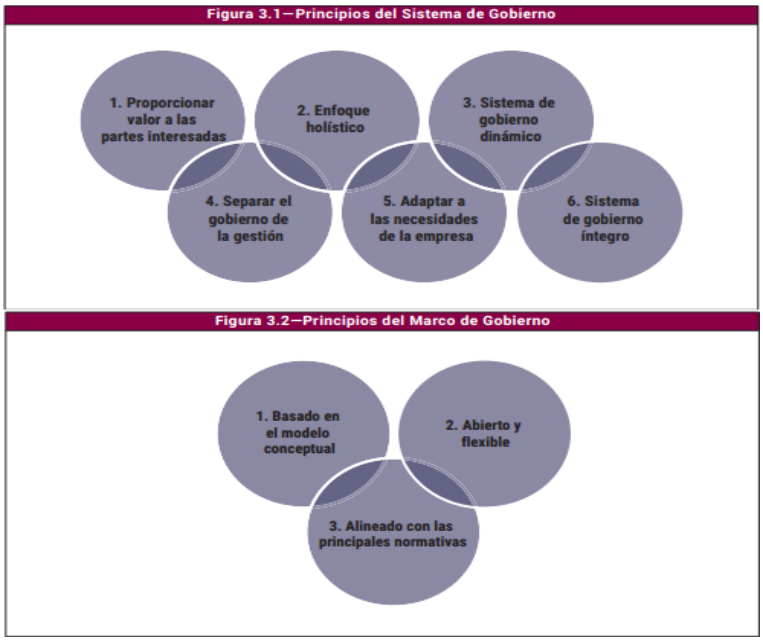


Ilustración 4: Los dos grupos de principios en los que COBIT® 2019 se fundamenta. Fuente: COBIT® 2019 Marco de referencia, Introducción y metodología [16].

[2] **TI:** Departamento de la organización responsable de la tecnología.
T&I: “Toda la **información** que la empresa genera, procesa y utiliza para lograr sus objetivos, y la **tecnología** que da soporte en toda la empresa. [16]”

Los principios de COBIT son la base para trabajar con su metodología. Además, COBIT® 2019 establece una serie de objetivos para el gobierno y para la gestión, de manera que cada objetivo corresponde a un proceso específico (objetivo de gobierno a proceso de gobierno y objetivo de gestión a proceso de gestión). En ambos casos se trabaja con una serie de componentes con el fin de lograr la consecución del objetivo, conformando así 40 objetivos en su modelo de referencia y sumando así 3 nuevos objetivos de gestión respecto a la versión anterior de COBIT, a saber:

APO014 Gestionar los datos.

BAI11 Gestionar los proyectos.

MEA04 Gestionar el aseguramiento.

A continuación, se presenta el modelo de referencia de los 40 objetivos de COBIT® 2019, que además se agrupan en cinco dominios; 1 dominio de Gobierno y 4 dominios de Gestión, que incluyen los 3 nuevos objetivos antes mencionados:

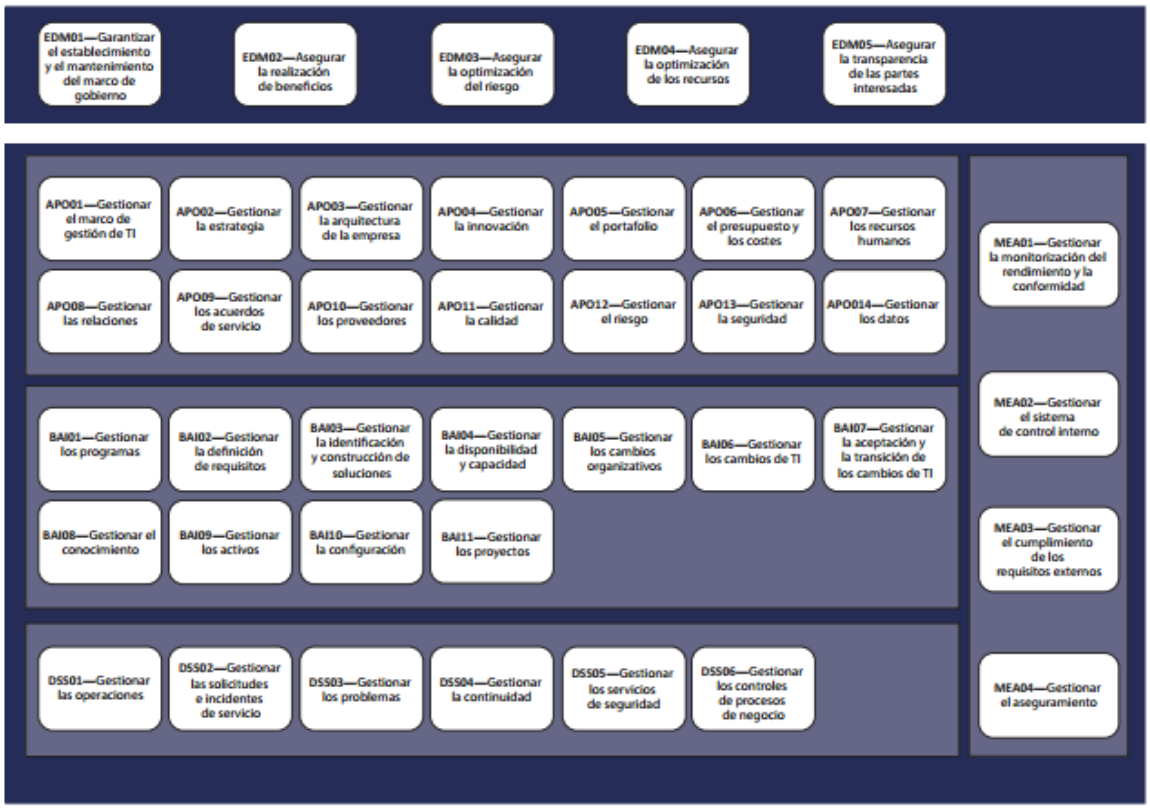


Ilustración 5: Modelo de procesos, Core del COBIT® 2019.

Fuente: Marco De Referencia COBIT® 2019: Introducción Y Metodología [17]

Además, dentro de las mejoras realizadas en la versión COBIT® 2019, ISACA indica en el documento de “Introducción y Metodología” que

procura dar mayor flexibilidad al marco de trabajo permitiendo “incorporar nuevas áreas prioritarias o modificar las actuales, sin implicaciones directas para la estructura y el contenido del modelo esencial de COBIT [18]” (esferas de interés). También se actualiza y adapta en el tema normativo de manera que “COBIT apoya las referencias y alineamiento con conceptos que surgen de otras fuentes (p. ej. los últimos estándares y regulaciones de cumplimiento de TI) [18]”.

Ante la adquisición del reconocido Instituto que produce el modelo de madurez de capacidades de procesos (CMMI)[3] por parte de ISACA en el año 2016, en COBIT “los conceptos de madurez y capacidad se introducen para lograr un mayor alineamiento con CMMI [18]”. Con esto último, COBIT® 2019 “asigna niveles de capacidad a todas las actividades del proceso, permitiendo una clara definición de los procesos y las actividades requeridas para alcanzar los distintos niveles de capacidad [19]“.

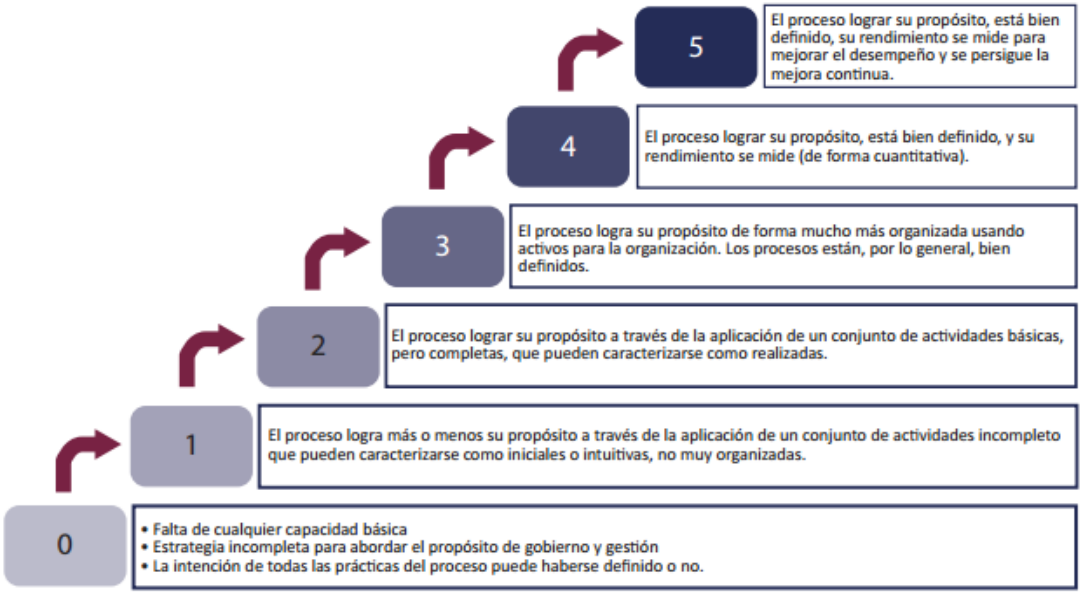


Ilustración 6: Capacidad de procesos según CMMI. Los niveles de capacidad, de 0 a 5 para cada objetivo de gobierno y gestión.

Fuente: Marco De Referencia COBIT® 2019: Introducción Y Metodología [19].

Si bien la descripción anterior de COBIT® 2019 no pretende incluir la totalidad del marco de trabajo, permite establecer su carácter de marco para Gobierno y Gestión de las tecnologías y la información de toda la empresa, surgiendo como la alternativa metodológica para abordar el caso de la

[3] ISACA Adquiere al Instituto CMMI®, Líder de Madurez de Capacidades Globales, nota de Bussiness Wire enlace: https://www.businesswire.com/news/home/20160303006772/es/

UNED debido a las características descritas. Efectivamente, es posible trabajar con los procesos existentes relacionados a la seguridad de la información, contemplando las normativas existentes en la UNED, de manera que se aborde este caso de estudio para el análisis de brechas en seguridad de la información, considerar alternativas, proponer soluciones y obtener insumos valiosos para generar el plan director para la implementación del sistema de gestión de la seguridad de la información en la UNED.

2.7 ISO/IEC 27014:2013, guía de conceptos y principios aplicables al gobierno de SI

Cuando se aborda el tema de seguridad de la información, resulta importante traer a consideración normas reconocidas que aporten aspectos puntuales o incluso técnicos para afrontar la situación particular de la organización En este sentido, la norma ISO/IEC 27014:2013 cuenta con características que pueden incorporarse en conjunto con el marco de trabajo COBIT® 2019 para atender el caso de la seguridad de la información de la UNED, descrito anteriormente.

La norma antes citada constituye una guía de conceptos y principios aplicables al Gobierno de Seguridad de la Información. Con ella “las organizaciones podrán dirigir, comunicar, evaluar y controlar la seguridad de la información que está relacionada con las actividades de la organización. Su ámbito de aplicación es para todas las clases y tamaños de organizaciones [20]”.

Resulta relevante mencionar que la norma hace una estricta separación entre el Gobierno de Seguridad de la Información y el Gobierno de Tecnología de Información. Si bien ambos se alinean e integran al Gobierno Corporativo, su interacción directa solo debe ser a través de aspectos de seguridad de TI, lo cual se puede representar mediante la siguiente figura:

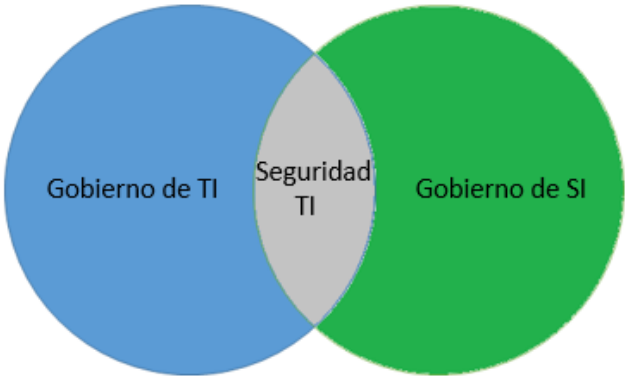


Ilustración 7: ISO/IEC 27014, separación de Gobierno de TI del Gobierno de SI, ambos interactúan a través de la Seguridad de TI.

Fuente: Elaboración propia.

2.8 ISO/IEC 27001:2013, Sistemas de gestión de la seguridad de la información (SGSI)

La norma ISO/IEC 27001 es un estándar ampliamente reconocido que establece los requisitos de un Sistema de Gestión de Seguridad de la Información (SGSI) en la organización. La primera versión fue publicada en 2005 y su versión más actualizada es de 2013. Brinda los requisitos para establecer, implementar, mantener y dar mejora continua al sistema de gestión de la seguridad de la información. La estructura de la norma incluye 10 cláusulas más un Anexo, que se describen a continuación:

Las primeras 3 secciones son:

1- Objeto y campo de aplicación
2- Referencias normativas
3- Términos y definiciones

Las sesiones 4 a la 10 corresponden a la información de interés para los requisitos del SGSI y se detallan a continuación, agregando una breve descripción:

4- **Contexto de la organización**: De extremo a extremo y con un alcance definido para el SGSI.
5- **Liderazgo**: Compromiso de las autoridades con el SGSI y los recursos necesarios.
6- **Planificación**: Basada en gestión de riesgos con objetivos claros.
7- **Soporte**: Determinación de recursos, competencia del personal, conciencia de los interesados, comunicación y documentación.

8- **Operación**: Planificación y control operacional.

9- **Evaluación de desempeño**: Sustento del ciclo PDCA (Planificar, Hacer, Verificar, Actuar) mediante seguimiento, medición, análisis y evaluación del SGSI.

10- **Mejora continua:** Acciones correctivas y de mejora continua

La última sección es un Anexo que provee una lista con objetivos de control y controles de referencia, que son abordados en mayor detalle en la ISO/IEC 27002:2013.

Dentro de las características generales de la norma ISO/IEC 27001:2013, se encuentra la forma de trabajar con objetivos de seguridad de la información que deben ser definidos por cada organización de acuerdo con sus exigencias de confidencialidad, integridad y disponibilidad, promoviendo que la seguridad y los procesos de la empresa se integren.

Para ello, COBIT® 2019 tiene ampliamente desarrollada una estructura de principios y un modelo de procesos, de manera que el uso de ISO/IEC 27001:2013 junto a COBIT® 2019 es compatible para abordar el caso de la UNED.

2.9 ISO/IEC 27002:2013, Código de prácticas para los controles de seguridad de la información

Si bien la norma ISO/IEC 27001:2013, en su versión más reciente del año 2013, aporta los requisitos necesarios para un SGSI en la organización, es necesario complementarlo con la norma ISO/IEC 27002:2013. Se trata de “una guía de buenas prácticas que describe los objetivos de control y controles recomendables y comúnmente aceptados en la seguridad de la información y que, de hecho, son los que se encuentran en el Anexo A dentro de la norma ISO/IEC 27001 [21]”. A continuación, se presenta una figura que muestra en forma simplificada la correspondencia entre las normas ISO/IEC 27001:2013 y la ISO/IEC 27002:2013.

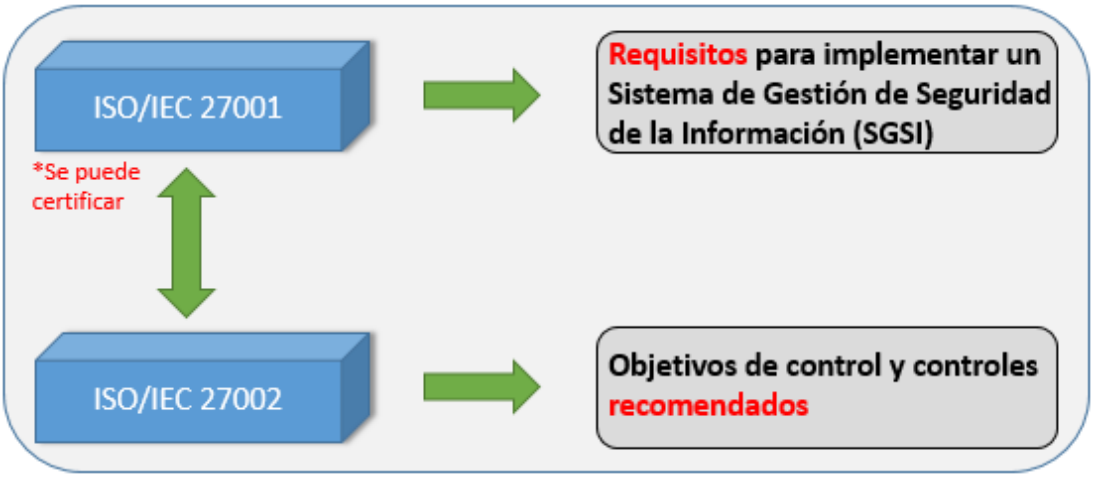


Ilustración 8: La norma ISO/IEC 27001 establece requisitos para implementar el SGSI, y hace referencia a los objetivos de control y controles que se detallan en la norma ISO/IEC 27002.

Fuente: Elaboración propia.

La estructura de la norma ISO/IEC 27002:2013 incluye 14 categorías principales de seguridad que a su vez contienen un total de 35 Objetivos de control y estos a su vez totalizan114 controles.

A continuación, se agrega una breve descripción de las 14 secciones:

1- **Políticas de Seguridad de la Información:** que deben ser aprobadas por las autoridades, de conocimiento de todo el personal de la organización, revisadas y actualizadas frecuentemente.

2- **Organización de la Seguridad de la Información:** Controles aplicados a través de roles, asignación de responsabilidades, comunicación con las autoridades. Además, indica aspectos de dispositivos móviles y teletrabajo.

3- **Seguridad de recursos humanos:** Considera el factor humano en seguridad de la información, destacando la necesidad de concientizar y capacitar al personal interno y externo. Establece también los roles y la consideración de los recursos humanos antes de iniciar su trabajo en el puesto, durante sus labores y cuando se desvincula de la organización.

4- **Gestión de activos:** Contempla activos de información y medidas adecuadas para protegerlos, responsables, propietarios, entrega, uso, devolución y eliminación, entre otros.

5- **Control de acceso a la información:** Incluye políticas de acceso a información, redes y servicios, el registro, la entrega y cancelación de usuarios, su nivel de privilegio y aspectos vinculados a los programas autorizados y al código fuente.
6- **Criptografía:** Establece la necesidad de un control criptográfico para asegurar la autenticidad, confidencialidad e integridad de la información.
7- **Seguridad física y ambiental:** Contribuye a asegurar el perímetro de la infraestructura física, los equipos informáticos y su mantenimiento.
8- **Seguridad de las operaciones:** Establece aspectos mayormente técnicos sobre malware, respaldos, control de software operacional, gestión de vulnerabilidad, monitoreo y auditoria.
9- **Seguridad en las comunicaciones:** Indica controles para la gestión de la seguridad de la red, su segmentación, transmisión, mensajería, acuerdos de confidencialidad.
10- **Adquisiciones, desarrollo y mantenimiento de sistemas de información:** Incorpora aspectos de seguridad de los sistemas, su desarrollo y soporte, datos de prueba uso y eliminación.
11- **Relación con los proveedores:** Brinda lineamientos para la seguridad de los activos en que intervienen terceros, acuerdos del servicio, gestión de servicios de proveedores.
12- **Gestión de incidentes de seguridad de la información:** Establece responsables y procedimientos para una respuesta adecuada a los incidentes de seguridad de la información.
13- **Aspectos de la seguridad de la información en la gestión de la continuidad de la operación:** Apunta a prevenir la continuidad de la seguridad de la operación y gestionar la redundancia.
14- **Cumplimiento:** Establece la necesidad de un acatamiento de requisitos legales y contractuales y la revisión del cumplimiento de políticas organizacionales.

Los 114 controles involucrados, reunidos en las 14 categorías principales de seguridad antes mencionadas no son necesariamente obligatorios en cuanto a su implementación y pueden complementar lo

indicado en el marco COBIT® 2019 al establecer los controles necesarios y adecuados para una adecuada gestión de la seguridad de la información en la organización.

2.10 Otros estándares para considerar

En los apartados anteriores se describieron tres normas ampliamente utilizadas en seguridad de la información, las cuales pertenecen a la familia de normas ISO/IEC 27000. Se trata de estándares de seguridad de la información creados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). Dichos estándares se enfocan principalmente a implementar y mantener los Sistemas de Gestión de la Seguridad de la Información (SGSI) en una organización y con el pasar de los años han consolidado su uso extensivo y liderazgo en el campo a nivel mundial.

Sin embargo, existen otras normas y/o estándares en el campo de la informática que también merecen mención, por lo que a continuación se brinda una breve descripción:

1- El estándar de buenas prácticas para la seguridad de la información 2016 (SOGP) desarrollado por el Foro de Seguridad de la Información (ISF), “busca proveer en varios ámbitos una guía de buenas prácticas en el manejo de la información, pero siempre de tal forma que tenga aplicabilidad directa. Este estándar, basado en las experiencias de los diferentes actores que se ven implicados en el manejo de la información a nivel empresarial, ha sido desarrollado con la meta de mitigar el riesgo relacionado con la fuga de información [22]”. Es una guía para la seguridad de la información del negocio, organizada alrededor de 4 categorías (gobierno de la seguridad, requisitos de seguridad, marco de control y seguimiento y mejora de la seguridad). Se enfoca en el establecimiento de una estrategia de seguridad, en la gestión de incidentes y en la continuidad del negocio y recuperación.

2- NIST SP 800: se trata de una alternativa a la norma ISO/IEC 27002:2013 en cuanto a objetivos de control y a la posible implementación de estos ante requerimientos particulares de la organización. Se presenta como “un conjunto de documentos de libre

descarga que se facilita desde el gobierno federal de los Estados Unidos, que describe las políticas de protección de la información, los procedimientos y las directrices. Son publicadas por el Instituto Nacional de Estándares y Tecnología [23]".

3- ISO/IEC 20000-1:2018: Es una norma creada para gestionar la calidad de los servicios de tecnología de información, que tiene por objetivo una "implementación efectiva y un planteamiento estructurado para desarrollar servicios de tecnología de la información fiables en lo referente a la gestión de servicios de TI [24]".

4- Estándares y directrices utilizadas o compatibles con COBIT® 2019:

A continuación, se listan los estándares y directrices que son referenciados o utilizados en COBIT® 2019 en lo que hace a la seguridad de la información:

- CIS Center for Internet Security, The CIS Critical Security Controls for Effective Cyber Defense,
- Cloud standards and good practices:

  Amazon Web Services (AWS®)

  Security Considerations for Cloud Computing, ISACA

  Controls and Assurance in the Cloud: Using COBIT® 5, ISACA:
- CMMI Cybermaturity Platform, 2018
- CMMI Data Management Maturity (DMM)SM model, 2014
- Comité de Organizaciones Patrocinadoras (COSO) Enterprise Risk Management (ERM) Framework, junio 2017
- HITRUST® Common Security Framework, version 9, September 2017
- Information Security Forum (ISF), The Standard of Good Practice for Information Security 2016
- Normativa de la Organización Internacional de Normalización / Comisión Electrotécnica Internacional (ISO/CEI)
- ISO/CIE 27001:2013/Cor.2:2015(E)
- ISO/CIE 27002:2013/Cor.2:2015(E)
- ISO/CIE 27004:2016(E)

- ISO/CIE 38500:2015(E)
- ISO/CIE 38502:2017(E)
- Information Technology Infrastructure Library (ITIL®) v3, 2011
- Normativa del Instituto de Estándares y Tecnología de Estados Unidos (NIST)
- Framework for Improving Critical Infrastructure Cybersecurity V1.1, abril 2018
- Special Publication 800-37, Revisión 2 (Borrador), mayo 2018
- Special Publication 800-53, Revisión 5 (Borrador), agosto 2017
- A Guide to the Project Management Book of Knowledge: PMBOK® Guide, 6.ª Edición, 2017
- Skills Framework for the Information Age (SFIA®) V6, 2015

CAPITULO 3: MARCO METODOLÓGICO

En el presente capítulo se describe la metodología de la investigación empleada en el presente TFM, el enfoque metodológico utilizado, así como el alcance definido y directamente vinculado a la gestión de la seguridad de la información en equipos y servicios virtuales de la UNED con la respectiva aplicación del marco de trabajo COBIT® 2019 en los entregables que se desarrollarán.

3.1 Tipo de investigación

Para la presente investigación se requiere de un enfoque metodológico cuantitativo el cual, en términos de Hernández, Fernández y Baptista tiene lugar cuando “los planteamientos que se van a investigar son específicos y delimitados desde el inicio de un estudio [1]” Este enfoque metodológico por la naturaleza del caso de estudio, tiene un alcance exploratorio. Según Hernández, Fernández y Baptista (2006) este tipo de estudio “se emplea cuando el objetivo consiste en examinar un tema poco estudiado o novedoso. [1]” Esto resulta útil considerando lo que se pretende describir, ya que se busca aplicar un Marco de Trabajo novedoso como es COBIT® 2019 a un aspecto crítico de actualidad como lo es la gestión de seguridad de la información.

3.2 Entregables

En esta sección se incluyen los entregables, tomando en cuenta la seguridad de la información involucrada en su infraestructura virtual con servicios en la nube y la aplicabilidad del marco de trabajo COBIT® 2019, siempre considerando la metodología previamente indicada en este documento y alineado a los objetivos planteados.

3.2.1 Entregables por objetivo específico con su descripción

Tabla 1: Entregable para alcanzar el objetivo: Analizar la infraestructura convergente, hiperconvergente, y servicios en la nube existente en la UNED, desde la perspectiva de la protección de los activos que la componen

Entregable	Descripción de alcance
A1-Modelo de plataforma tecnológica.	- Detalle del modelo de plataforma tecnológica utilizada por la UNED, con descripción de la infraestructura virtual que administra la UIT y las observaciones relacionadas a la protección de activos de información en este modelo. -Este entregable se presenta y analiza en la sección 4.1.1 de este TFM, a partir de la información que se obtiene del Coordinador de la UIT.

Fuente: Elaboración propia.

Tabla 2: Entregable para alcanzar el objetivo: Determinar los procesos y servicios críticos brindados a través de la infraestructura tecnológica de virtualización en la UNED.

Entregable	Descripción de alcance
B1-Activos de información de la infraestructura virtual	- Presentación de un extracto de los activos de información relevantes para la investigación. Incluye detalles de la prioridad de procesos y servicios tecnológicos institucionales. - Este documento se elabora como parte de este TFM, a partir de la información que se obtiene del Coordinador de la UIT.
B2-COBIT 2019: Definición del caso	- Informe Ejecutivo del caso de estudio, considerando las recomendaciones del Marco de Trabajo COBIT® 2019 para su definición, desarrollo y solución propuesta. Este documento va dirigido a definir o resumir (en términos de COBIT® 2019) el caso de estudio de la UNED considerando la gestión de la seguridad de la información de la infraestructura tecnológica virtual y sistemas convergentes en la UIT. Se excluyen los aspectos que no son relevantes para los objetivos planteados o para el alcance. - Este documento se elabora basándose en la guía de Introducción y Metodología de COBIT® 2019 disponible y

	las normas que pueden aplicar al caso de estudio.

Fuente: Elaboración propia.

Tabla 3: Entregable para alcanzar el objetivo: Evaluar, mediante la aplicación de COBIT® 2019 como marco de trabajo para el gobierno y la gestión de las Tecnologías y la Información, la seguridad informática aplicable a los equipos físicos y virtuales y los servicios ofrecidos a través de la infraestructura tecnológica de virtualización en la UNED.

Entregable	**Descripción de alcance**
C1-COBIT 2019: Guía de diseño del alcance inicial del Sistema de Gobierno, factores de diseño y resultados.	- Documento detallado que surge a partir de aplicar la Guía de Diseño COBIT® 2019 al caso de estudio mediante la herramienta de diseño COBIT® 2019 que provee ISACA para este fin. El documento resultante provee los resultados consolidados del alcance del sistema de Gobierno inicial, entrega mejoras a dicho alcance y consolida los resultados para su interpretación, facilitando el análisis de los objetivos COBIT® 2019 de gestión de la seguridad de la información. - Este documento se elabora basándose en la documentación de COBIT® 2019 disponible y su herramienta de diseño.

Fuente: Elaboración propia.

Tabla 4: Entregable para alcanzar el objetivo: Generar un plan director para la gestión de la seguridad informática de los equipos físicos, virtuales, y para los servicios ofrecidos a través de la infraestructura tecnológica de virtualización en la UNED

Entregable	**Descripción de alcance**
D1-Plan Director propuesto para la gestión de la seguridad informática.	- Documento con el Plan Director para la Gestión de la Seguridad Informática de los equipos físicos, virtuales, y para los servicios ofrecidos a través de la infraestructura tecnológica de virtualización en la UNED. - Este documento se elabora basándose en los resultados obtenidos de la aplicación de COBIT® 2019 a la gestión de la seguridad de la información de la infraestructura tecnológica virtual y sistemas convergentes en la UNED en la presente investigación. Surge a partir de los entregables previos donde se establece el caso de estudio y se aplica la Guía de Diseño.

Fuente: Elaboración propia.

3.2.2 Estructura Desagregada de Trabajo (EDT)

A continuación, se presenta la figura de la estructura desagregada del trabajo, cuyo fin es descomponer y apreciar de mejor manera los entregables necesarios para lograr los objetivos planteados. Más adelante se detallarán las actividades establecidas para cada entregable.

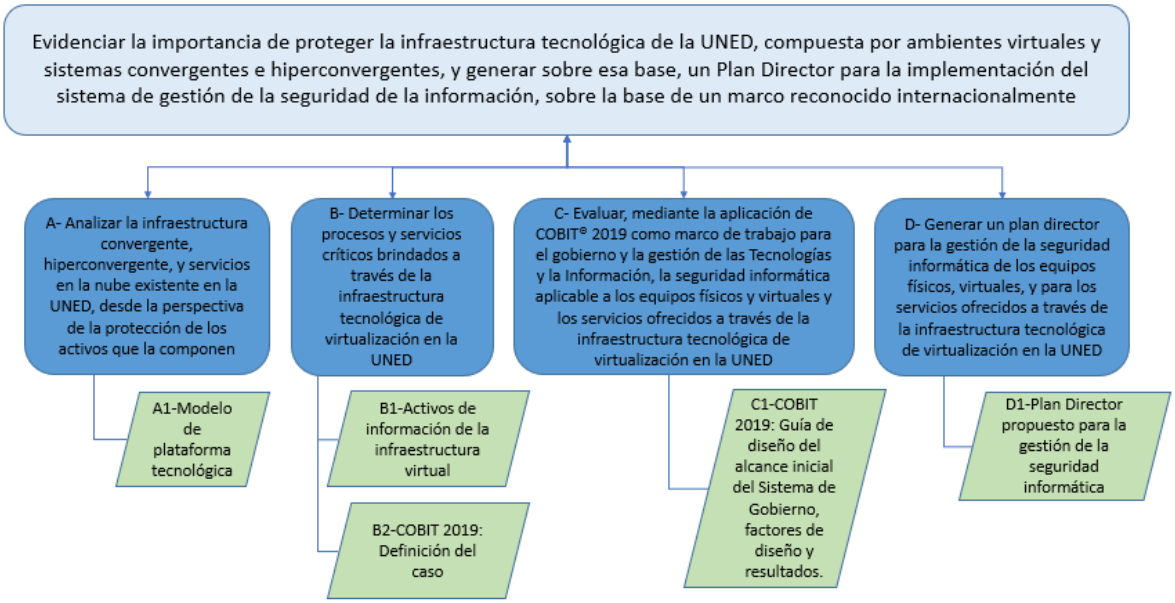


Ilustración 9: Estructura Desagregada del trabajo investigativo planteado, se indican los entregables para lograr los objetivos definidos.

Fuente: Elaboración propia.

3.3 Planteamiento de investigación

3.3.1 Conceptualización

A continuación, se describen conceptualmente los procesos que serán utilizados para medir la aplicación del Marco de Trabajo COBIT® 2019 en la protección de las infraestructuras virtuales de la UNED como base para la gestión de la seguridad de la información de la infraestructura tecnológica virtual y sistemas convergentes en la UNED.

Se definen procesos para dos de los objetivos específicos del trabajo investigativo, siendo estos seleccionados en base en la información útil medible que puede extraerse de ellos. A su vez se les aplicarán métricas a los procesos por cada objetivo.

Tabla 5: Descripción conceptual de los procesos del objetivo específico relacionado a los activos de información indicado en la sección 1.4.2

Objetivo específico: Determinar los procesos y servicios críticos brindados a través de la infraestructura tecnológica de virtualización en la UNED.		
Proceso	**Definición conceptual**	**Atributo**
Gestión de activos	Identificar los activos de la organización y definir las responsabilidades para la apropiada protección. (ISO/IEC 27002:2013). La organización debe tener la documentación respectiva y actualizada.	- Inventario de activos. - Propiedad de los activos. - Uso aceptable de los activos. - Devolución de activos.
Clasificación de la información	La información recibe un nivel de protección apropiado, de acuerdo con su importancia para la organización. (ISO/IEC 27002:2013). La organización debe tener la documentación respectiva y actualizada.	- Clasificación de la información. - Etiquetado de la Información. - Manejo de los activos.
Manejo de los medios	Prevenir la divulgación, modificación, remoción o destrucción indebida de la información (ISO/IEC 27001:2013).	-Gestión, eliminación y traslado de medios

Fuente: Elaboración propia.

Tabla 6: Descripción conceptual de los procesos del objetivo específico de aplicación de COBIT® 2019 al caso de la UNED indicado en la sección 1.4.2

Objetivo específico: Evaluar, mediante la aplicación de COBIT® 2019 la seguridad de los equipos físicos y virtuales y de los servicios ofrecidos a través de la infraestructura tecnológica de virtualización en la UNED.		
Proceso	**Definición conceptual**	**Atributo**
Diseño de un sistema de Gobierno	- Definir la importancia de los objetivos de gobierno y gestión para el caso de estudio, mediante	- Alcance inicial del sistema de Gobierno.

	la medición de la influencia de factores de diseño sobre los objetivos de gobierno o gestión de COBIT® 2019.	

Fuente: Elaboración propia.

3.3.2 Descripción instrumental y operacional por procesos

A partir de la información conceptual establecida para los procesos, se describen los instrumentos y procedimientos utilizados para el análisis y la generación de métricas o resultados esperados de dichos procesos.

A continuación, se desglosa instrumental y operacionalmente los atributos de los procesos propuestos.

Tabla 7: Descripción instrumental y operacional de los procesos del objetivo específico relacionado a los activos de información indicado en la sección 1.4.2

Proceso	**Atributo**	**Descripción instrumental y operacional**
Gestión de activos	- Inventario de activos. - Propiedad de los activos. - Uso aceptable de los activos. - Devolución de activos. - Gestión, eliminación y traslado de medios	- Extracto de activos de información de la organización relacionados directamente a infraestructura tecnológica de virtualización en la UNED, identificación de sus responsables y de las medidas de protección adoptadas para éstos. - Se recolectará la información existente relacionada con los activos de la infraestructura tecnológica de virtualización en la UNED. - Se tabularán los datos haciendo referencia a la norma ISO/IEC 27002: 2013, sección “Gestión de Activos” y se presentarán los resultados.
Clasificación de la información.	- Clasificación de la	- Clasificación de la lista de los activos de la organización relacionados directamente

	información. - Etiquetado de la Información. - Manejo de los activos.	con la infraestructura tecnológica de virtualización en la UNED. - Se clasificará la lista previa de activos de la infraestructura tecnológica de virtualización en la UNED, sobre la base de la norma ISO/IEC 27002:2013. sección "Clasificación de la información", por requisitos de valor para la UNED. - Se tabularán los datos haciendo referencia a la norma ISO/IEC 27002:2013, sección "Clasificación de la información", considerando la forma en que se etiquetan, describen o se manejan los activos en la UNED y se presentarán los resultados.

Fuente: Elaboración propia.

Tabla 8: Descripción instrumental y operacional de los procesos del objetivo específico relacionado a la aplicación de COBIT® 2019 al caso de estudio, indicado en la sección 1.4.2

Procesos	**Atributo**	**Descripción instrumental y operacional**
Diseño de sistema de Gobierno	- Alcance inicial del Sistema de Gobierno.	- Medición de la influencia de factores de diseño sobre los objetivos de gobierno o gestión de COBIT® 2019, con el fin de determinar el alcance inicial del Sistema de Gobierno para el caso. - Partiendo de la información previa de la gestión de activos y la clasificación de la información, de la infraestructura tecnológica de virtualización en la UNED, sumado al caso de estudio planteado en términos de COBIT® 2019, se procede a aplicar la Guía de Diseño COBIT® 2019 al caso de estudio mediante la herramienta de diseño COBIT® 2019 que provee ISACA

		para este fin. - Se ingresarán los datos a la herramienta de diseño COBIT® 2019 y se presentarán los resultados del alcance inicial obtenido.

Fuente: Elaboración propia.

3.3.3 Resumen de entregables

En el siguiente cuadro se presenta la relación entre los objetivos específicos de la investigación, los procesos planteados y los entregables que sustentan los resultados. Esto se realiza con el fin de resumir y asistir en la comprensión de la metodología descrita en el presente capítulo:

Tabla 9: Lista de entregables esperados según la metodología planteada y en consecución de los objetivos específicos de la investigación.

Objetivo	Entregable	Proceso
Analizar la infraestructura convergente, hiperconvergente, y servicios en la nube existente en la UNED, desde la perspectiva de la protección de los activos que la componen.	A1-Modelo de plataforma tecnológica.	NA.
Determinar los procesos y servicios críticos brindados a través de la infraestructura tecnológica de virtualización en la UNED.	B1-Activos de información de la infraestructura virtual. B2-COBIT 2019: Definición del caso.	- Gestión de activos. - Clasificación de la información.
Evaluar mediante la aplicación de COBIT® 2019 como marco de trabajo para el gobierno y la gestión de las Tecnologías y la Información, la seguridad de los equipos	C1-COBIT 2019: Guía de diseño del alcance inicial del Sistema de Gobierno, factores de diseño y resultados.	- Diseño de sistema de Gobierno.

físicos y virtuales y los servicios ofrecidos a través de la infraestructura tecnológica de virtualización en la UNED.		
Generar un Plan Director para la gestión de la seguridad de la información de los equipos físicos y virtuales y para los servicios ofrecidos a través de la infraestructura tecnológica de virtualización en la UNED.	D1-Plan Director propuesto para la gestión de la seguridad de la información.	NA.

Fuente: Elaboración propia.

CAPÍTULO 4: PRESENTACIÓN Y ANALISIS DE RESULTADOS JUNTO CON LA PROPUESTA PARA LA GESTIÓN DE LA SEGURIDAD

El presente capítulo resume el resultado del trabajo realizado, según lo planteado en el marco metodológico descripto en el capítulo anterior.

A continuación, se presentan los entregables previamente definidos, incluyendo la valoración de hallazgos relevantes para la definición del caso de estudio, junto con la aplicación del marco de trabajo COBIT® 2019.Se incluye el análisis de resultados y la presentación de la propuesta del Plan Director de Seguridad.

4.1 Presentación de datos y análisis de los resultados

4.1.1 Entregable A1-Modelo de plataforma tecnológica.

La UNED tiene un modelo de plataforma tecnológica orientado a la virtualización de equipos y uso de redes de datos, brindando sus servicios a través de Internet. A continuación, se presenta el diagrama del modelo de plataforma vigente:

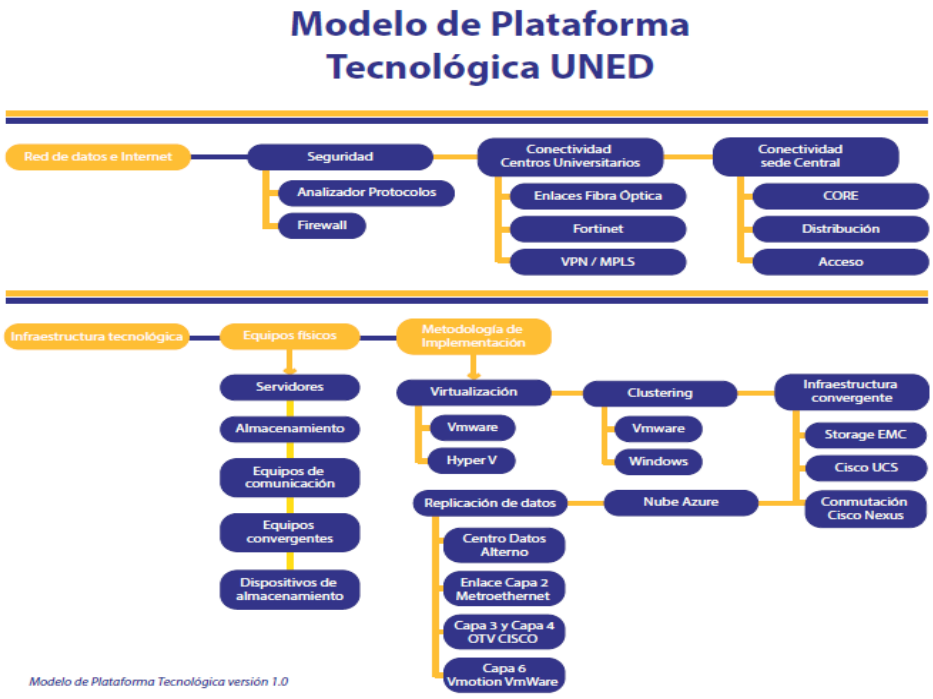


Ilustración 10: Diagrama del Modelo de Plataforma Tecnológica vigente en la UNED.
Fuente: Elaborado por el Coordinador de la UIT de la UNED.

En la figura anterior se observan los componentes de la Infraestructura tecnológica, desde una perspectiva técnica, se hace relevancia en los equipos virtuales y en la red de cómputo.

En el bloque superior denota el uso intensivo de redes de datos en servicios a nivel interno y de Internet para proveer servicios a los usuarios externos del país. Además, se tiene una primera capa de red interna en la sede central en San José, una segunda capa de red hacia los Centros Universitarios en las diferentes regiones (continúa siendo conexión interna a través de medios asegurados por VPN y firewall, entre otros) y finalmente, una capa externa exponiendo los diferentes servicios a los usuarios por internet.

En el bloque inferior se muestran los equipos físicos, incluyendo los servidores, unidades de almacenamiento empresarial, dispositivos de red y equipos convergentes de última generación. Lo anterior resulta ser la capa inferior que provee la infraestructura física de cómputo que brinda soporte para todo lo referente a la virtualización y equipos convergentes.

Lo anterior muestra como la seguridad de la información se encuentra estrechamente ligada a los servicios relacionados a los equipos virtuales, convergentes y en la nube. En otras palabras y más allá del aseguramiento tradicional de equipos físicos en el centro de datos, surge la importancia en proteger los activos de información de esta capa virtual de la infraestructura tecnológica.

4.1.2 Entregable B1-Activos de información de la infraestructura virtual.

En el presente apartado se determina la situación actual de la UNED en cuanto a inventario de activos de información, como punto de partida necesario para establecer las medidas de seguridad a adoptar.

Dentro de los hallazgos más relevantes, se comprobó que la UNED maneja un inventario de activos de información (reflejado en varios documentos) que contempla los equipos físicos y virtuales de la infraestructura. Sin embargo, dicha documentación no se revisa periódicamente, por lo que se tienen detalles desactualizados de algunos

equipos que no se revisan desde el año 2017, conviviendo con información registrada más recientes en el año 2020.

A continuación, se muestra un extracto del inventario utilizado en el año 2017 para el centro de datos principal:

Consec	Equipo	Responsable	Usuario/Unidad Fin	Servidor o Rol	Uso	Detalle aplicaciones
395	CD00LVVIPP01	Pablo Sandoval	DTIC	Central VoIP	P	FreePBX, Asterisk 11.12.0
406	CD00LVWEBD01	Pablo Sandoval	Arias	Servidor Web Linux de Desarrollo-Pruebas	D	Apache2, php5, MySQL 5.6
415	CD00LVMDBP04	Pablo Sandoval	Arias	Servidor MySQL 5.6 de Producción	P	MySQL 5.6 Server
448	CD00LVLBAP07	Pablo Sandoval	DTIC	Servidor proxy balanceo de HTTP-HTTPS para matricula	P	HaProxy 1.6
452	CD00WVWEBP01	Pablo Sandoval	DTIC	Equipo para Desarrollo de proyectos de Estudiantes ,	P	IIS8, MSSQL, .NET, php, MySQL 5, no

Ilustración 11: Activos identificados en el inventario. Contempla equipos físicos y virtuales de la infraestructura tecnológica.

A partir del 2018 con la inversión en nuevos equipos, principalmente la modernización del centro de datos y compra de unidades convergentes, surge una nueva clasificación general de activos. A continuación, se presenta un extracto de la categorización que se origina a partir de la criticidad de los servicios alojados en la infraestructura:

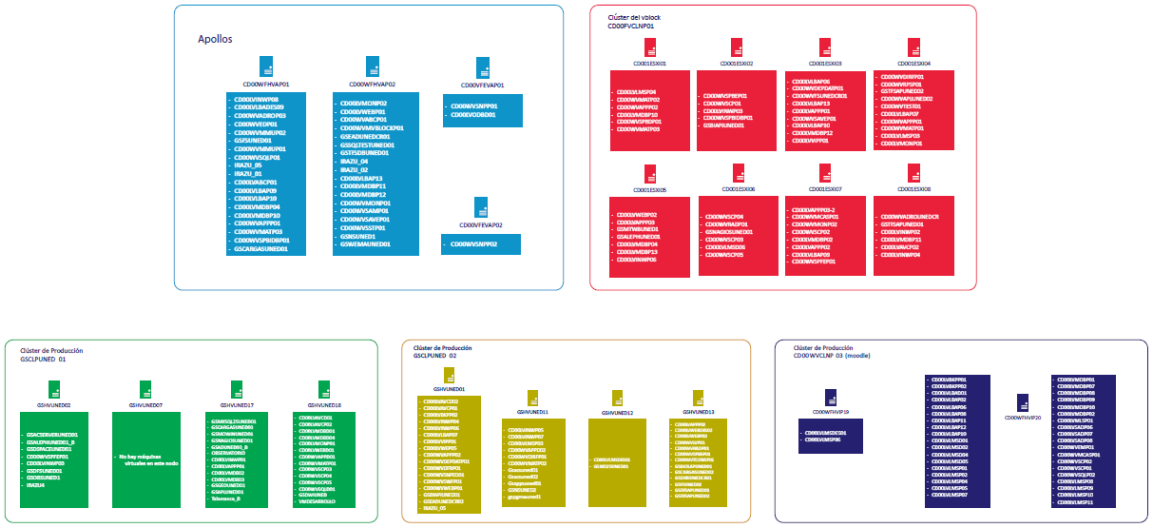


Ilustración 12: Distribución del nuevo modelo a partir de la inversión en el nuevo centro de datos. Se redistribuyen los equipos virtuales según la criticidad de los servicios. (Las etiquetas son difuminadas intencionalmente en la imagen para preservar la privacidad del diseño).

Fuente: Elaborado por la Unidad de Infraestructura Tecnológica, UNED 2019.

La imagen anterior muestra el reordenamiento de los diferentes equipos en el inventario, de manera que los equipos virtuales y los servicios alojados en éstos, se distribuyeron en la infraestructura tecnológica física en el centro de datos, dotando de mejores recursos a los servicios más críticos de la UNED.

Finalmente, para el año 2020, ante el crecimiento de la plataforma tecnológica, se define un esquema simplificado en tres niveles de criticidad,

cuya distribución se detalla a continuación. Esta distribución permanece vigente a la fecha.

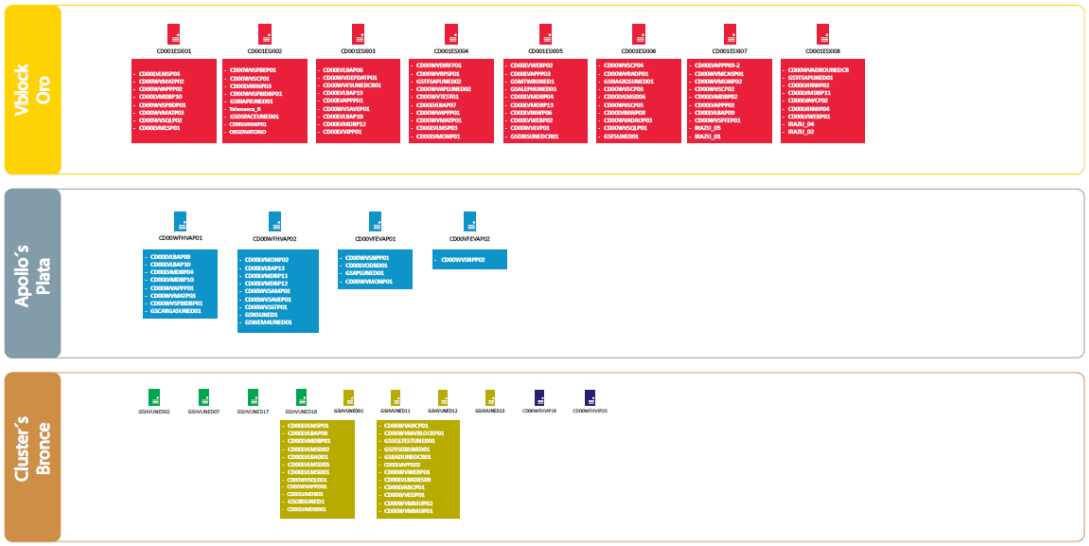


Ilustración 13: Distribución de los equipos virtuales que conforman la plataforma tecnológica actual en la UNED. (Las etiquetas son difuminadas intencionalmente en la imagen para preservar la privacidad del diseño).

Fuente: Elaborado por la Unidad de Infraestructura Tecnológica, UNED 2020.

En la imagen anterior, se aprecia como ante la creciente complejidad de la plataforma tecnológica en los últimos 3 años, resulta necesario emplear un modelo viable, donde se pueda atender toda la infraestructura tecnológica virtual que soporta los diferentes activos de información. Es entonces que para junio del año 2020 las autoridades aprueban el portafolio actualizado de servicios brindados por la DTIC, que se listan por prioridad. A continuación, se presenta un extracto de dicho documento (vigente a la fecha):

Prioridad según acuerdo de Prioridades Ref: CR.2016.124	Líder de Servicio	Suprasistema	Sistema	Aplicación	Nombre	Descripción	Unidad Patrocinadora
Alta	S. Saborío (Oficina de Registro y Administración Estudiantil)	SAE	Admisión y Matricula	Admisión Web	**Admisión Web**	Sistemas de Admisión vía Web	Oficina de Registro y Administración Estudiantil

Ilustración 14: Muestra de un servicio dentro del portafolio de servicios institucionales soportados en la infraestructura tecnológica virtual por la DTIC.

Fuente: Elaborado por la DTIC, UNED, ratificado por las autoridades (rectoría) de la Universidad.

Considerando la información anterior y haciendo referencia a la norma ISO/IEC 27002:2013, se realizó el siguiente cuadro resumen de la gestión actual del inventario de activos de la infraestructura tecnológica virtual de la UNED:

Tabla 10: Valoración de la gestión de activos y responsabilidades de la infraestructura tecnológica virtual de la UNED

Gestión de activos y responsabilidades					
Descripción del instrumento: Con los activos identificados en la infraestructura tecnológica virtual de la UNED, se valora el estado actual de la gestión y las responsabilidades, para la apropiada protección de los activos de información.					
			Valoración obtenida		
Referencia a norma ISO/IEC 27002	Item a valorar	Valor de referencia esperado	No existe o No es gestionado	Existe o es parcialmente gestionado	Existe y es debidamente gestionado
A.8.1.1	Inventario de activos	Los activos de información son identificados y se mantiene un inventario de esos activos.		Se cuenta con inventario, pero carece de un mantenimiento periódico y esta desactualizado.	
A.8.1.2	Propiedad de los activos	Los activos del inventario tienen un propietario asignado.			Se tiene propietario en cada activo identificado.
A.8.1.3	Uso aceptable de los activos	Se tienen las reglas para el uso aceptable de los activos de información.		Se tienen reglas generales de uso, sin controles específicos.	
A.8.1.4	Devolución de activos	Todos los funcionarios, o terceros deben devolver los activos de la organización al finalizar su relación o acuerdo.			Se tiene respaldo contractual en todos los casos de devolución de activos.

Fuente: Elaboración propia a partir del análisis de plataforma tecnológica, inventario de activos y las buenas prácticas definidas en la norma ISO/IEC 27001/27002

Tabla 11: Valoración de la clasificación de activos de la infraestructura tecnológica virtual de la UNED

Clasificación de la información					
Descripción del instrumento: Con los activos identificados en la infraestructura tecnológica virtual de la UNED, se valora si estos cuentan con un nivel de protección apropiado, de acuerdo con su importancia para la organización.					
			Valoración obtenida		
Referencia a norma ISO/IEC 27002	Item a valorar	Valor de referencia esperado	No existe o No es gestionado	Existe o es parcialmente gestionado	Existe y es debidamente gestionado
A.8.2.1	Clasificación de la información	La información es clasificada por requisitos legales, valor, criticidad y sensibilidad.			La UNED cuenta con documento de prioridades de activos, incluye servicios prioritarios en acuerdo ratificado por las autoridades.
A.8.2.2	Etiquetado de la información	Existe conjunto apropiado de procedimientos para el etiquetado de la información según la clasificación de la organización.			Se incluye la etiqueta en cada activo, tanto en equipos físicos y virtuales. Se utilizan etiquetas de 5 dígitos grabadas directamente en los equipos físicos y se utilizan etiquetas digitales de 12 dígitos para inventariar equipos virtuales.
A.8.2.3	Manejo de los activos	Se tienen procedimientos para el manejo de los activos según la clasificación de la organización.		Existen procedimientos de trasiego y descargo de activos físicos, sin especificaciones en el manejo de equipos virtuales e información sensible.	

Fuente: Elaboración propia a partir del análisis de plataforma tecnológica, inventario de activos y las buenas prácticas definidas en la norma ISO/IEC 27001/27002.

Con las valoraciones de las tablas anteriores, se puede concluir que existe una plataforma tecnológica robusta en la UNED, con un diseño que responde a las necesidades de la organización, representa una inversión importante y es debidamente gestionada en términos de infraestructura tecnológica. Sin embargo, surge del análisis a la luz de las normas ISO/IEC 27001/27002:2013, la necesidad de mejora en cuanto a buenas prácticas e incluso controles específicos en materia de seguridad de la información, principalmente en los procedimientos del manejo de equipos virtuales. Estos hallazgos dan lugar a las evaluaciones y diagnósticos que se detallan en los siguientes apartados.

4.1.3 Entregable B2-COBIT 2019: Definición del caso.

En concordancia con el modelo de plataforma tecnológica y los activos de información expuestos en los puntos anteriores, se construye el caso de negocio en estudio, permitiendo sintetizar una perspectiva cualitativa con la ayuda de COBIT® 2019.

El caso en específico se presenta como sigue a continuación:

- Resumen:

  La UNED es una institución educativa compuesta por áreas internas tradicionales comunes a toda institución de carácter similar. Sin embargo, en los últimos años se ha visto forzada a modernizarse, creando nuevas áreas de negocios basados en Internet y tecnologías relacionadas a la educación a distancia. Por otra parte, dado que su expansión es a nivel nacional, encuentra algunas diferencias culturales y económicas locales. La institución contempla directrices propias de una institución pública desde su creación. Existe una buena adopción de infraestructura virtual para mejorar el valor generado; que, sin embargo, ha mostrado un incipiente desarrollo de los aspectos de seguridad de la información mediante controles o reglas internas. Adicionalmente, estos aspectos no están guiados formalmente por metodologías o marcos de trabajo que faciliten su gestión y no obedecen a una estrategia de gobierno de la seguridad de la información.

- Antecedentes:

  Si bien, como se ha repasado exhaustivamente en capítulos anteriores, la UNED cuenta con la DTIC como ente responsable de las tecnologías de información y comunicación, la seguridad de la información está guiada por una unidad estratégica dentro de la DTIC. Esta unidad a su vez se encarga de generar controles o reglas de seguridad, teniendo como insumos las directrices de la jefatura, los documentos de la plataforma tecnológica e inventario y los informes de riesgos que puedan generarse por iniciativas propias o por auditorías internas o externas.

- Desafíos:

  El principal desafío en el caso de la UNED en temas de seguridad de la información es comprender el entorno tecnológico existente que brinda servicio al modelo negocio de educación a distancia a través de internet, y protegerlo adecuadamente. Este entorno se base en una infraestructura tecnológica virtual. Se busca aplicar un marco de trabajo que le permita proteger correctamente los activos, y generar un Plan Director de Seguridad que permita darle seguimiento.

- Análisis de brechas y meta:

  Existe una brecha significativa en la seguridad de la información, la cual es gestionada mediante limitados controles internos y escasos recursos lo cual repercute en riesgos potenciales y reales a los que se expone.

  Por otra parte, trabajar la seguridad de la información bajo un marco o metodología adecuada, puede traducirse en valor para la institución, sin afectar los procesos propios del negocio. Se puede, además, mitigar los riesgos y anticipar mejores prácticas, mejorando la cultura organizacional respecto a la seguridad de la información.

- Alternativas consideradas:

  Si bien, como se ha expuesto en capítulos anteriores, existen diferentes metodologías o marcos de trabajo para tecnologías de información que comprenden aspectos de seguridad de la

información, lo cierto es que COBIT® 2019 es muy flexible en su implementación debido a que no se requiere implementar de manera total y se puede enfocar en áreas específicas.

- Solución propuesta:

  Una vez analizado el caso, a continuación, se esboza una breve descripción de las etapas de la propuesta del presente estudio:

  - Planificación:

    Se toma como punto de partida la revisión de la plataforma tecnológica existente y la gestión de activos de información descritos en el presente documento, se identifican aspectos de relevancia de estos y el caso de negocio establecido. Se aplica la Guía de Diseño COBIT® 2019 al caso de estudio mediante la herramienta de diseño COBIT® 2019 que provee ISACA para comprender el alcance inicial a partir de la influencia de factores de diseño sobre los objetivos de gobierno o gestión de COBIT® 2019. Como resultado adicional, se presenta una propuesta de Plan Director de Seguridad para el caso.

  - Alcance:

    Lograr un mapeo inicial de los objetivos de gobierno y gestión a priorizar en relación con la seguridad de la información de la infraestructura tecnológica virtual y servicios ofrecidos a partir de ella.

  - Metodología y alineamiento:

    Completar la herramienta de diseño COBIT® 2019 con el área de tecnología encargada de la gestión de la infraestructura tecnológica virtual, enfocándose en los riesgos de seguridad de la información.

  - Entregables:

    Presentación de los resultados de la herramienta de diseño COBIT® 2019 con el respectivo análisis enfocado en la seguridad de la información.

    Propuesta de Plan Director de Seguridad.

    Conclusiones y recomendaciones en la presente investigación.

- Riesgo:

  Considerando que es una investigación académica relacionada a la seguridad de la información con un alcance delimitado, no hay riesgo para la organización en este caso.
- Partes Interesadas:

  La DTIC, sus unidades UIT, USD, así como su jefatura, las autoridades de la UNED y el autor del presente trabajo final, quien también se desempeña en la UNED, con interés en los hallazgos y las conclusiones o recomendaciones finales de la investigación.
- Costo-Beneficio:

  Considerando que es una investigación académica relacionada a la seguridad de la información con un alcance delimitado, no hay costo significativo, más si un beneficio potencial de las conclusiones de la investigación, que pueden ser utilizadas por la UNED para el fortalecimiento de la seguridad de la información en la Institución.

4.1.4 Entregable C1-COBIT 2019: Guía de diseño del alcance inicial del Sistema de Gobierno, factores de diseño y resultados.

El presente apartado presenta los resultados de aplicar la Guía de Diseño COBIT® 2019 al caso de estudio. Esta Guía propone el diseño e implementación de un sistema de gobierno personalizado para la organización. Para el caso del presente trabajo, el interés se centra en los resultados obtenidos hasta el **alcance inicial** del sistema de gobierno, siendo mediante la interpretación de estos resultados que se obtiene el detalle de los objetivos de gobierno y gestión COBIT® 2019 prioritarios para la seguridad de la información de la UNED.

Para lograr resultados aptos de interpretación, se recurrió a la herramienta de diseño COBIT® 2019 que provee ISACA junto a la Guía de Diseño. La herramienta fue aplicada a los hallazgos del caso de estudio, específicamente con la información con que se cuenta en la Unidad de Infraestructura Tecnológica (UIT) de la DTIC. De esta manera se buscó esclarecer los objetivos COBIT® 2019 de gobierno y gestión prioritarios,

relacionados a la seguridad de la información de la infraestructura tecnológica virtual existente en la UNED.

La herramienta de diseño COBIT® 2019, consiste en un grupo de tablas parametrizables en las cuales, partiendo del contexto empresarial (**Paso 1**), se le asigna un valor a cada uno de los factores de diseño con el fin de tener un alcance inicial de sistema de gobierno. La herramienta toma los valores descriptivos de cada factor y los correlaciona con los 40 objetivos de gobierno y gestión existentes en COBIT® 2019, consolidando así los resultados para su interpretación.

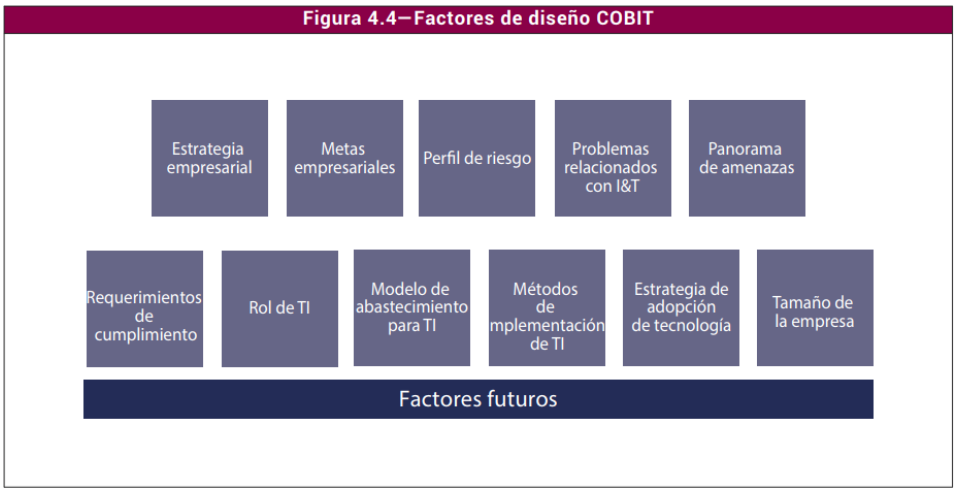


Ilustración 15: Factores de diseño COBIT® 2019

Fuente: Marco De Referencia COBIT® 2019: Introducción Y Metodología [25]

La importancia de haber establecido previamente el contexto y conocer a fondo la realidad del caso, permite utilizar la herramienta de diseño COBIT® 2019 de forma óptima y así poder interpretar los resultados para evaluar y determinar las prioridades en la seguridad de la información de la infraestructura tecnológica de virtualización en la UNED.

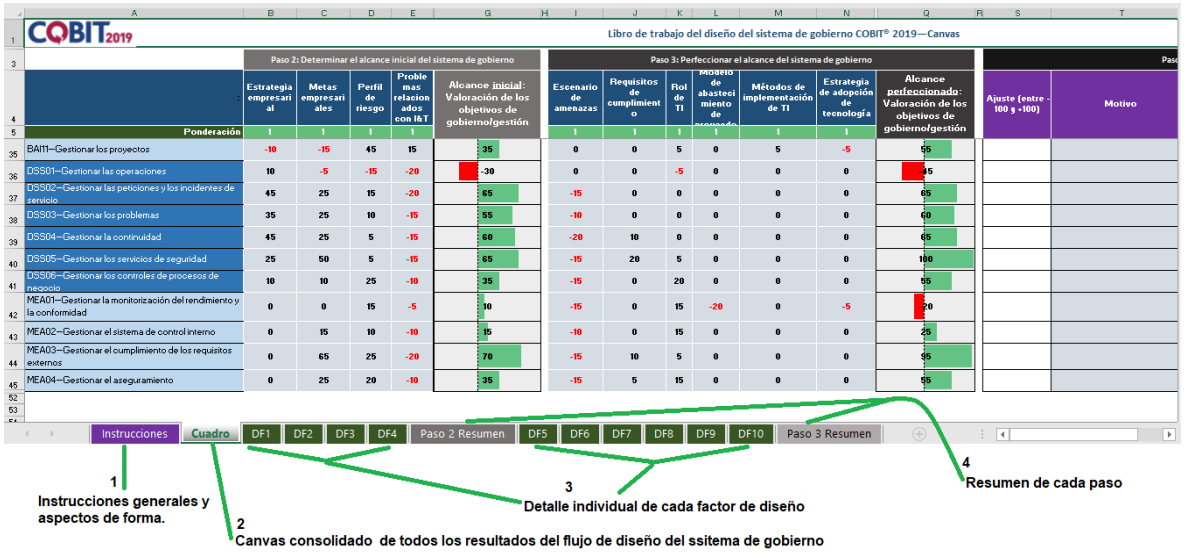


Ilustración 16: Visualización de las partes de la herramienta de diseño con los datos detallados y los consolidados. (Numeradas de 1 a 4 las principales partes que componen la herramienta).

Fuente: Elaboración propia a partir de captura de pantalla de la herramienta de diseño COBIT® 2019, ISACA.

En la imagen anterior se muestra una vista de la herramienta de diseño COBIT® 2019 con valores detallados. Además, se indican las 4 principales interfaces que permiten elaborar el flujo de trabajo para obtener un diseño de sistema de gobierno personalizado. La primera pestaña corresponde a instrucciones generales de llenado de información y uso de la herramienta, la segunda pestaña es el cuadro consolidado a interpretar. Las pestañas DF1-10 corresponden a los 10 factores de diseño específicos que se trabajan a partir del contexto previamente analizado, y las pestañas de resumen corresponden al **Paso 2** de valores obtenidos y el **Paso 3** para refinamiento de todos los valores. Es importante aclarar que el factor de diseño 11, que corresponde a "tamaño de la empresa únicamente indica si debe usarse la guía del área prioritaria de pequeñas y medianas empresas, en lugar de la guía Core de COBIT. El tamaño de una empresa no tiene impacto en la prioridad y los niveles de capacidad objetivo de los objetivos de gobierno y gestión [26]".

A continuación, se presentan los hallazgos más relevantes obtenidos después de aplicar la guía de diseño al caso (para más detalle ver Anexo #1: Resultados de herramienta de diseño COBIT® 2019), con su respectivo análisis.

- **Factores de diseño 1 al 4 y resumen de resultados del Paso 2**:
  En el paso 2 del diseño, se contemplan 4 factores de diseño a saber:
  FD1: Estrategia empresarial.
  FD2: Metas empresariales.
  FD3: Perfil del riesgo.
  FD4: Problemas relacionados con **I&T**.

Si bien todos los factores de diseño evaluados son relevantes, para la investigación, es útil analizar los valores obtenidos del factor de diseño 4: problemas relacionados con I&T. Este factor puede influenciar negativamente en la operación por frustración entre áreas (el usuario con TI) debido a iniciativas fallidas, además de un gasto en TI por áreas al margen de los mecanismos institucionales de inversión y los presupuestos aprobados en la UNED. Esto puede estar relacionado a insuficientes recursos de TI, personal desgastado o no calificado, así como al fracaso en implementaciones de iniciativas e innovaciones condicionadas por la arquitectura y sistemas de TI vigentes.

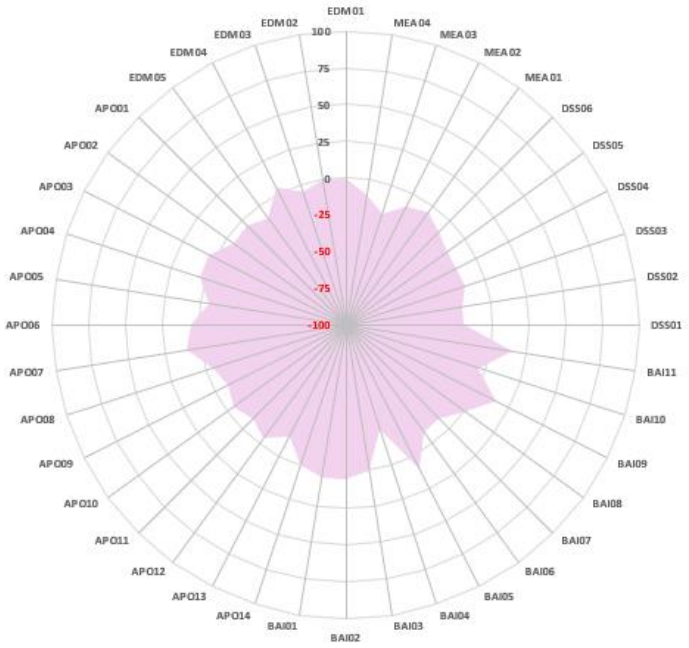


Ilustración 17: Objetivos de gobierno y gestión COBIT® 2019 relevantes para el factor de diseño 4.

Fuente: Elaboración propia a partir de los valores ingresados en la herramienta de diseño COBIT® 2019.

Siguiendo con el análisis del factor de diseño 4, como se aprecia en la figura anterior, existen objetivos de gobierno y gestión que presentan una

importancia limitada o relativa, como son los casos de APO3, APO4, APO6, APO7, BAI5, BAI9, BAI11 o EDM04. Estos objetivos se relacionan a la gestión de la arquitectura, la innovación, el presupuesto, los recursos humanos, los cambios organizativos, los activos, los proyectos y el gobierno en cuanto a la optimización de los recursos. En principio se puede considerar que estos aspectos tienen poca relevancia para la seguridad de la información. Sin embargo, al brindar indicadores para procesos relacionados a la infraestructura tecnológica de la organización, resultan fundamentales para identificar tanto debilidades como fortalezas en seguridad de la información. Efectivamente, son relevantes los valores relacionados a la arquitectura actual que causa fraccionamiento y se crea tecnología descentralizada en otras áreas que no son competentes en materia tecnológica. A manera de ejemplo, la infraestructura virtual puede ser una solución si se hacen ajustes en la arquitectura actual. De lo contrario continuarán apareciendo nuevas implementaciones tecnológicas al margen de la DTIC que crearán una brecha peligrosa en seguridad de la información.

Continuando con el análisis de los factores de diseño del **Paso 2**, específicamente en el factor de diseño 2: Metas Empresariales, podemos indicar que la UNED, siendo una institución pública con servicio de educación a distancia y enfocada en el estudiante, presenta un grado de importancia en sus metas empresariales de gestión de riesgo del negocio, cumplimiento de leyes y normativas externas y una cultura de servicio al cliente. Esto se corresponde con metas aún más críticas como lo es la continuidad y disponibilidad del servicio del negocio y el cumplimiento con las políticas internas. Las metas antes descritas, por lo tanto, hacen que la gestión de la seguridad de la información tenga mayor relevancia para la organización.

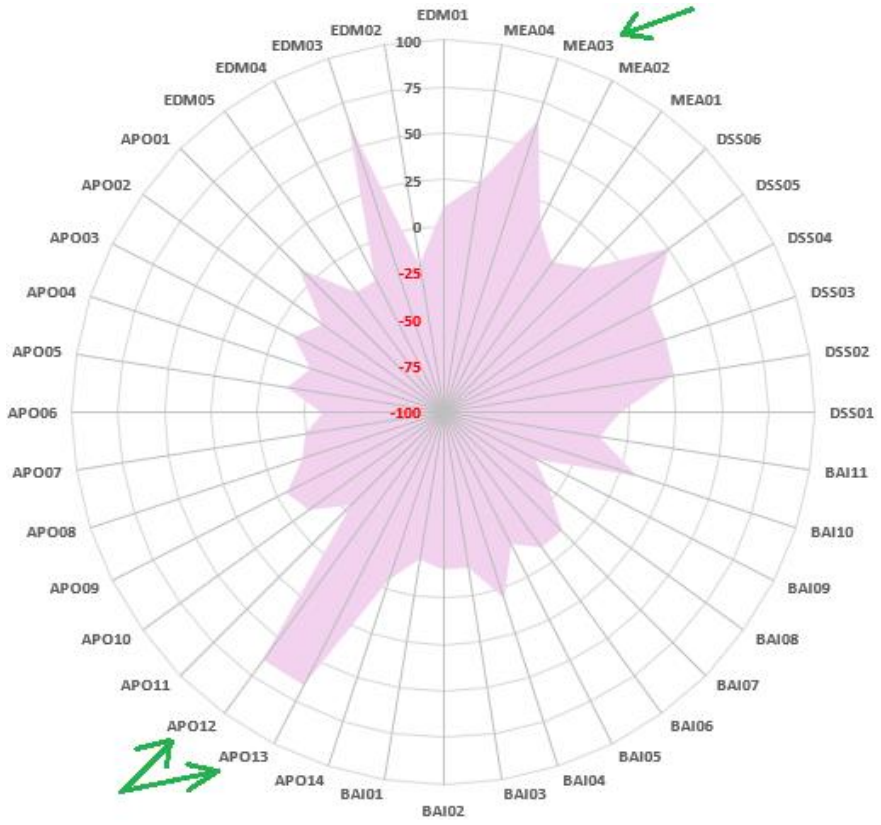


Ilustración 18: Objetivos de gobierno y gestión COBIT® 2019 relevantes para el factor de diseño 2.

Fuente: Elaboración propia a partir de los valores ingresados en la herramienta de diseño COBIT® 2019.

Como se aprecia en la figura anterior, resulta muy relevante para el estudio de la seguridad de la información, los resultados obtenidos por el factor de diseño 2: Metas Empresariales. Esto se debe a que hay valores altos en los objetivos de gestión COBIT® 2019 APO12-Gestionar el riesgo, APO13-Gestionar la seguridad y MEA03-Gestionar el cumplimiento de los requisitos externos.

Lo anterior nos arroja información valiosa para el objeto del presente estudio, debido a que hay objetivos de gestión COBIT® 2019 claramente prioritarios para la seguridad de la información, que se relacionan directamente a la infraestructura tecnológica virtual existente. Una primera observación indica que, si bien es suficiente para brindar los diferentes servicios, no se alcanza el cumplimiento de los objetivos de gestión del riesgo y de la seguridad de la información. Esto pone en relevancia el hecho de que es probable que la UNED le haya estado dando mucha importancia a los temas de cumplimiento, descuidando objetivos de riesgo y seguridad, al no darles la importancia o el alcance que les corresponde.

Para los factores de diseño 1: Estrategia Empresarial y 3: Perfil del Riesgo, ambos evaluados en el paso 2, si bien se obtuvieron valores que superan los 25 puntos de 100 en importancia relativa, están muy distantes de ser objetivos de gobierno o gestión COBIT® 2019 prioritarios para el caso de estudio. Por otra parte, dentro de los valores más significativos, se tiene la gestión de proyectos, de los acuerdos de servicio, de la disponibilidad y capacidad, de la calidad, de las solicitudes e incidentes de servicio, y de la continuidad. Sus resultados pueden interpretarse como fortalezas de la UNED por su tipo de negocio y por tratarse de una institución pública.

En el final del paso 2, la herramienta de diseño COBIT® 2019 nos brinda un primer resumen (**alcance inicial** del sistema de gobierno) a partir de los factores de diseño 1 al 4, donde se consolidan los resultados obtenidos y los principales objetivos COBIT® 2019 de gobierno y gestión, es decir los objetivos prioritarios para el caso de estudio:

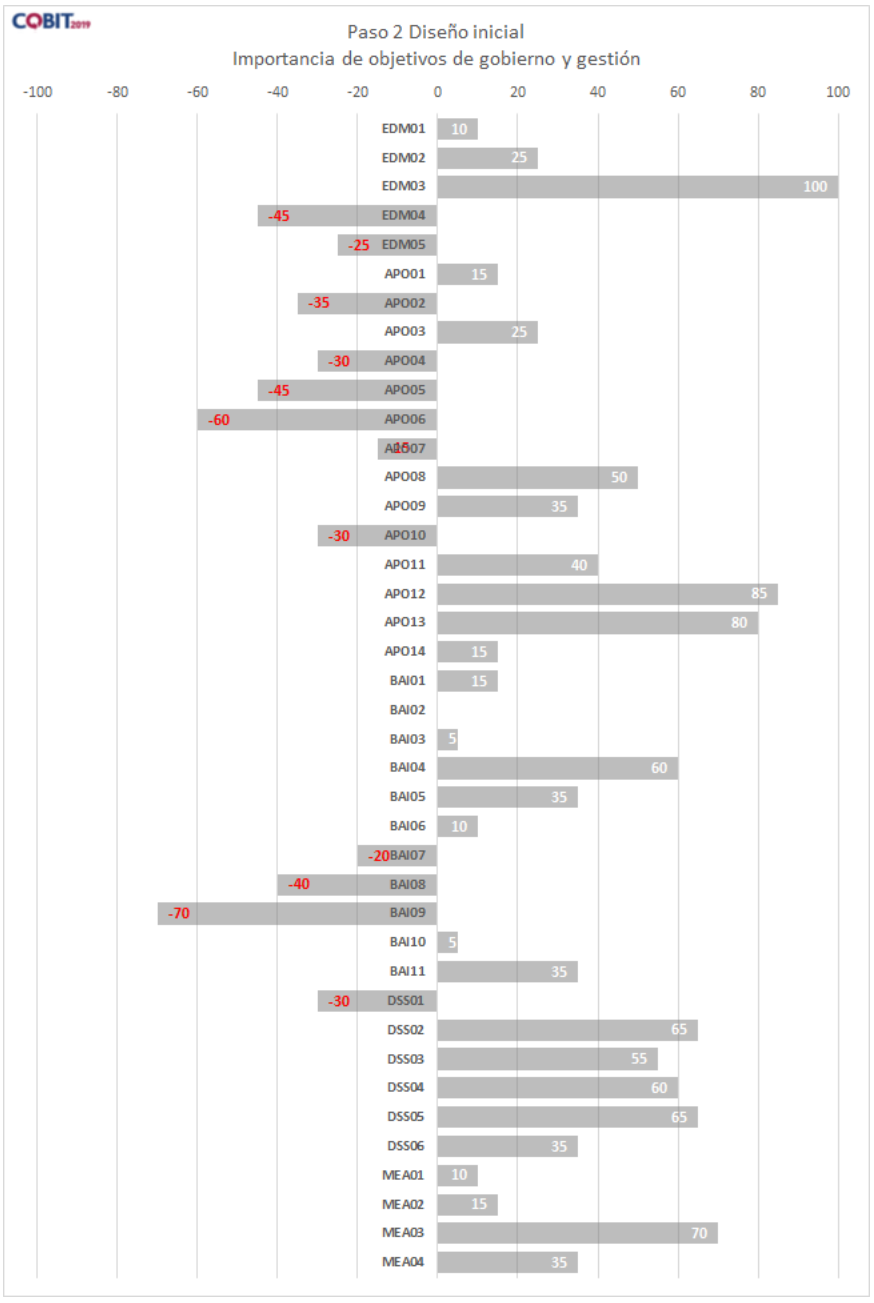


Ilustración 19: Resumen de objetivos de gobierno y gestión COBIT® 2019 relevantes para el paso 2 (Factores de diseño 1 al 4).

Fuente: Elaboración propia a partir de los valores ingresados en la herramienta de diseño COBIT® 2019.

Como se ilustra en la figura anterior, el resumen muestra la relevancia al objetivo de gobierno EDM03-Asegurar la optimización del riesgo, así como de los objetivos de gestión APO12-Gestionar el Riesgo y APO13-Gestionar la Seguridad. Esto es consecuente con lo analizado anteriormente para los factores de diseño 1 al 4, y puede considerarse un insumo valioso para fundamentar posteriores conclusiones y recomendaciones al respecto.

- **Factores de diseño 5 al 10 y resumen de resultados del Paso 3**: En el paso 3 del diseño, se contemplan 6 Factores de Diseño a saber:

  FD5: Importancia del escenario de amenazas.

  FD6: Importancia de los requisitos de cumplimiento.

  FD7: Importancia del rol de TI.

  FD8: Importancia modelo de abastecimiento de proveedores de TI.

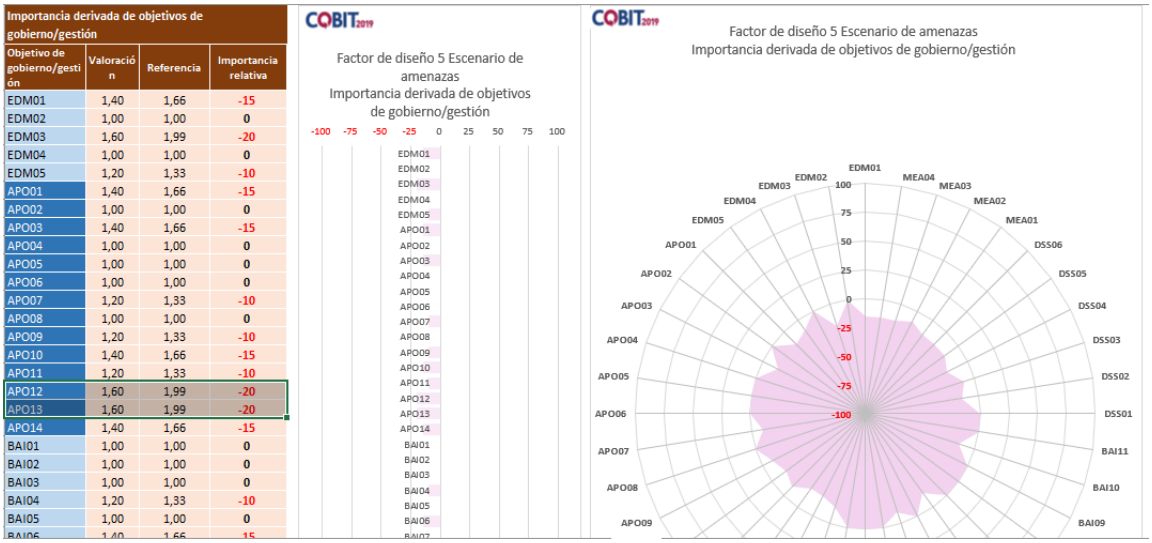
  FD9: Importancia de los métodos de implementación de TI.

  FD10: Importancia de la estrategia de adopción de tecnología.

  FD11: Tamaño de la empresa. Como se indicó previamente en este documento, este factor no tiene impacto en los objetivos de gobierno y gestión, por lo que la herramienta de diseño COBIT® 2019 no lo contempla.

A diferencia de los 4 primeros factores de diseño evaluados en el paso anterior cuyo fin era obtener un alcance inicial del sistema de gobierno, los factores 5 al 10 corresponden al **Paso 3** y son para mejorar ese sistema de gobierno. Si bien los factores de diseño de este paso tienen una perspectiva más cualitativa, al asignárseles un valor cuantificable, pueden asistir a la hora de perfeccionar los valores finales y obtener un resumen más completo de todo el flujo de trabajo. A continuación, se presentan los resultados más relevantes con su respectivo análisis.

Para el factor de diseño 5: Importancia de Escenario de Amenazas, se muestra un hallazgo relevante, ya que a la infraestructura tecnológica virtual se le brinda una atención considerada “normal” en función de las necesidades. Efectivamente, se parte de la base de que se le da mayor importancia a tener servicios funcionales con los recursos disponibles, y una importancia relativa a posibles amenazas. Lo anterior no implica un accionar necesariamente incorrecto, sino demuestra que las prioridades actualmente responden a una necesidad especifica de la organización. Como resultado, los valores de importancia de los objetivos de gobierno y gestión COBIT® 2019 son ajustados a valores más precisos. Cabe acotar que la herramienta de diseño COBIT® 2019 le resta puntos de importancia relativa a objetivos de gestión relacionados a la seguridad de la información como APO12-Gestionar el riesgo y APO13-Gestionar la seguridad.



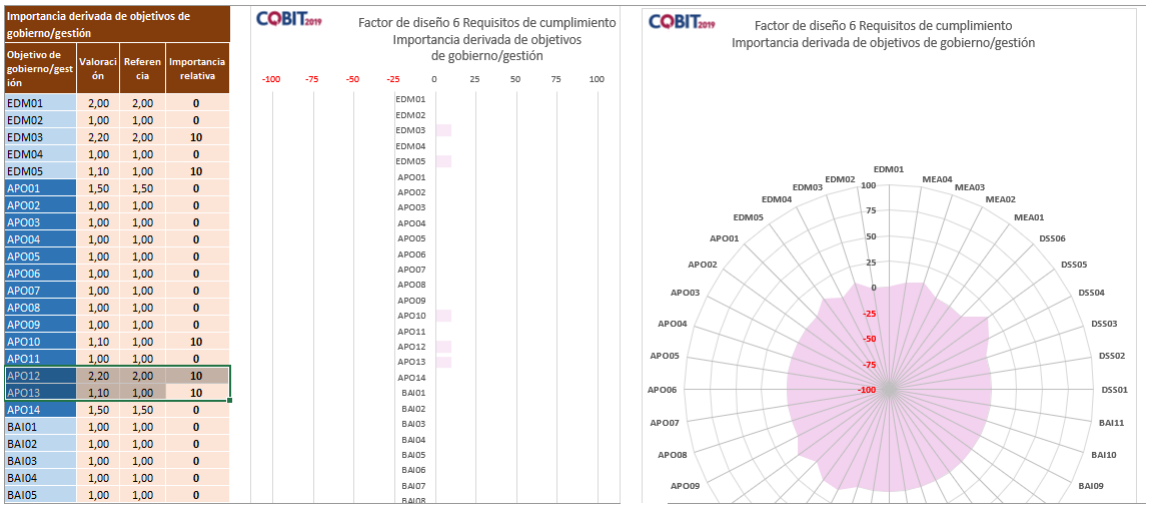
Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	Valoración	Referencia	Importancia relativa
EDM01	1,40	1,66	-15
EDM02	1,00	1,00	0
EDM03	1,60	1,99	-20
EDM04	1,00	1,00	0
EDM05	1,20	1,33	-10
APO01	1,40	1,66	-15
APO02	1,00	1,00	0
APO03	1,40	1,66	-15
APO04	1,00	1,00	0
APO05	1,00	1,00	0
APO06	1,00	1,00	0
APO07	1,20	1,33	-10
APO08	1,00	1,00	0
APO09	1,20	1,33	-10
APO10	1,40	1,66	-15
APO11	1,20	1,33	-10
APO12	1,60	1,99	-20
APO13	1,60	1,99	-20
APO14	1,40	1,66	-15
BAI01	1,00	1,00	0
BAI02	1,00	1,00	0
BAI03	1,00	1,00	0
BAI04	1,20	1,33	-10
BAI05	1,00	1,00	0
BAI06	1,40	1,66	-15

Ilustración 20: Resultado ajustados a partir del factor de diseño 5: Importancia del Escenario de Amenazas. Los objetivos de gobierno y gestión COBIT® 2019 varían levemente.

Fuente: Elaboración propia a partir de los valores ingresados en la herramienta de diseño COBIT® 2019.

En la imagen anterior se aprecia como la mayoría de los objetivos de gobierno y gestión COBIT® 2019 tienen una variación o ajuste mínimo de importancia relativa en el factor de diseño 5. Este comportamiento es de interés para el trabajo ya que el ajuste tiende a negativo para objetivos relacionados a seguridad de la información: APO12-Gestionar el riesgo y APO13-Gestionar la seguridad, lo cual indica que la organización muestra poco interés al escenario de amenazas y enfoca sus recursos a otros objetivos de gobierno y gestión.

Siguiendo con el análisis de los resultados, se puede apreciar que para el factor de diseño 6: Importancia de los requisitos de cumplimiento, la situación es opuesta a lo visto en el factor de diseño 5. Esto es debido a que la organización, al pertenecer al sector público, se encuentra sometida a una serie de regulaciones internas y externas que hacen del cumplimiento un factor relevante.



Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	Valoración	Referencia	Importancia relativa
EDM01	2,00	2,00	0
EDM02	1,00	1,00	0
EDM03	2,20	2,00	10
EDM04	1,00	1,00	0
EDM05	1,10	1,00	10
APO01	1,50	1,50	0
APO02	1,00	1,00	0
APO03	1,00	1,00	0
APO04	1,00	1,00	0
APO05	1,00	1,00	0
APO06	1,00	1,00	0
APO07	1,00	1,00	0
APO08	1,00	1,00	0
APO09	1,00	1,00	0
APO10	1,10	1,00	10
APO11	1,00	1,00	0
APO12	2,20	2,00	10
APO13	1,10	1,00	10
APO14	1,50	1,50	0
BAI01	1,00	1,00	0
BAI02	1,00	1,00	0
BAI03	1,00	1,00	0
BAI04	1,00	1,00	0
BAI05	1,00	1,00	0

Ilustración 21: Resultado ajustados a partir del factor de diseño 6: Requisitos de cumplimiento. Los objetivos de gobierno y gestión COBIT® 2019 varían levemente con valores al alza.

Fuente: Elaboración propia a partir de los valores ingresados en la herramienta de diseño COBIT® 2019.

En la imagen anterior nuevamente los objetivos de gobierno y gestión COBIT® 2019 tienen una variación o ajuste mínimo en este factor de diseño, pero el ajuste que sobresale en este caso en particular es positivo, es decir que suman puntos de importancia relativa para objetivos relacionados a seguridad de la información. De esto se puede interpretar que la seguridad de la información resulta relevante para alcanzar valores de cumplimiento adecuados.

Para el factor de diseño 7: Importancia del rol de TI, se observa un leve aumento en la importancia relativa, pero con la particularidad de que es un incremento uniforme en la mayoría de los objetivos de gobierno y gestión COBIT® 2019, como se aprecia en la siguiente imagen:

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	Valoración	Referencia	Importancia relativa
EDM01	29,0	25,5	15
EDM02	25,0	22,5	10
EDM03	24,0	24,0	0
EDM04	17,0	15,0	15
EDM05	17,0	15,0	15
APO01	21,0	19,5	10
APO02	26,0	24,0	10
APO03	19,0	18,0	5
APO04	30,0	27,0	10
APO05	25,0	22,5	10
APO06	17,0	15,0	15
APO07	14,5	13,5	5
APO08	21,5	19,5	10
APO09	19,0	19,5	-5
APO10	19,5	21,0	-5
APO11	18,5	18,0	5
APO12	23,5	22,5	5
APO13	24,0	22,5	5
APO14	21,0	19,5	10
BAI01	21,5	19,5	10
BAI02	26,0	24,0	10
BAI03	26,0	24,0	10
BAI04	19,5	21,0	-5
BAI05	17,0	15,0	15
BAI06	18,5	19,5	-5
BAI07	19,0	18,0	5
BAI08	17,0	15,0	15
BAI09	17,0	15,0	15
BAI10	17,5	16,5	5
BAI11	19,0	18,0	5
DSS01	24,5	25,5	-5
DSS02	25,0	25,5	0
DSS03	27,5	27,0	0
DSS04	27,5	27,0	0
DSS05	29,0	27,0	5
DSS06	19,5	16,5	20
MEA01	17,0	15,0	15
MEA02	17,0	15,0	15
MEA03	14,5	13,5	5
MEA04	17,0	15,0	15

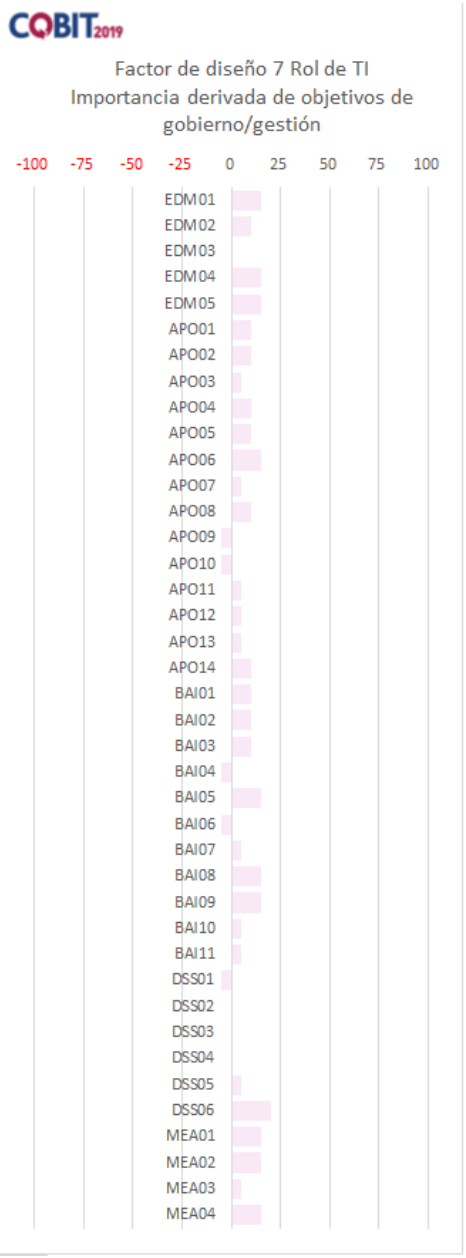


Ilustración 22: Incremento general de la importancia relativa a partir del factor de diseño 7: Importancia del Rol de TI. Los objetivos de gobierno y gestión COBIT® 2019 tienden al alza.

Fuente: Elaboración propia a partir de los valores ingresados en la herramienta de diseño COBIT® 2019.

De la anterior ilustración, se interpreta que la organización le asigna una importancia relativamente elevada en cuanto al rol que tiene la tecnología en sus diferentes áreas. En otras palabras, TI es parte de las prioridades institucionales. Está claro que los objetivos relacionados a la seguridad de la información son parte de los valores que también tienden al aumentar al considerar el rol de TI, como los objetivos de gestión APO12-Gestionar el riesgo, APO13-Gestionar la seguridad o APO14-Gestionar los datos, por citar algunos.

Para el factor de diseño 8: Importancia modelo de abastecimiento de proveedores para TI, así como para el factor de diseño 9: Importancia de los métodos de implementación de TI, los valores se mantienen invariables en casi la totalidad de objetivos de gobierno y gestión COBIT® 2019. Ahora bien, es de resaltar que esto obedece a una realidad actual, en la que la UNED viene trabajando con infraestructura mayormente alojada en los centros de datos en sus instalaciones físicas y los modelos de desarrollo son casi totalmente internos y se encuentran implementados mediante metodologías tradicionales. Con la tendencia que se viene mostrando a futuro y considerando algunas iniciativas de las autoridades, se estima que se acudirá a algunos servicios en la nube o de terceros y a orientarse a la adopción de metodologías agiles de desarrollo. Lo dicho constituye un importante foco de interés para la seguridad de la información, pues si bien es algo no concretado hoy día y que escapa de esta investigación, si se logra a mediano o largo plazo, la revisión de estos factores de diseño puede aportar mayor variabilidad en la importancia relativa de las tecnologías y la seguridad de la información.

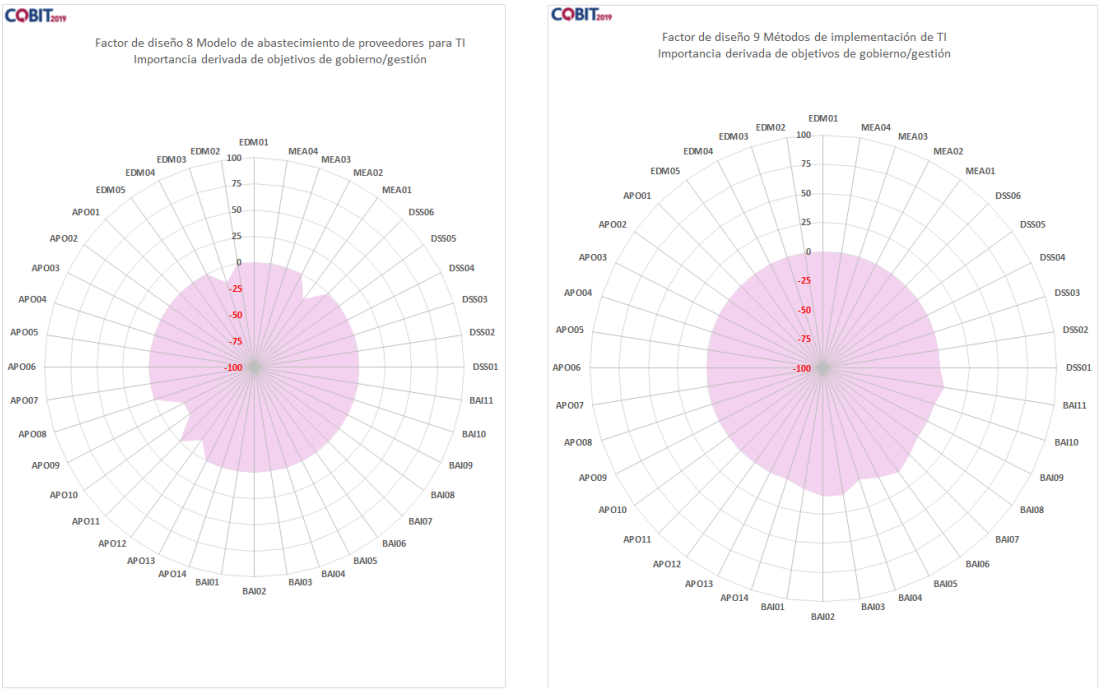


Ilustración 23: La importancia relativa de los objetivos de gobierno y gestión COBIT® 2019 es casi invariable a partir de los resultados obtenidos en el factor de diseño 8 y el factor de diseño 9.

Fuente: Elaboración propia a partir de los valores ingresados en la herramienta de diseño COBIT® 2019.

El último factor de diseño evaluado en la herramienta de diseño COBIT® 2019 es el 10: Importancia de la estrategia de adopción de tecnología. Por los resultados obtenidos, presenta valores levemente a la baja, lo cual es consecuente con la realidad de la UNED, para la cual la infraestructura tecnológica adquirida responde mayormente a las tendencias del mercado o en menor medida, a una adopción lenta de tecnología por su característica de entidad pública con limitaciones burocráticas. Esto impacta en la seguridad de la información ya que se corre menor riesgo al no ser una organización que reacciona primero en la adopción de tecnologías nuevas o poco probadas. Por ende, hay una leve disminución en la importancia relativa de los objetivos de gobierno y gestión COBIT® 2019.

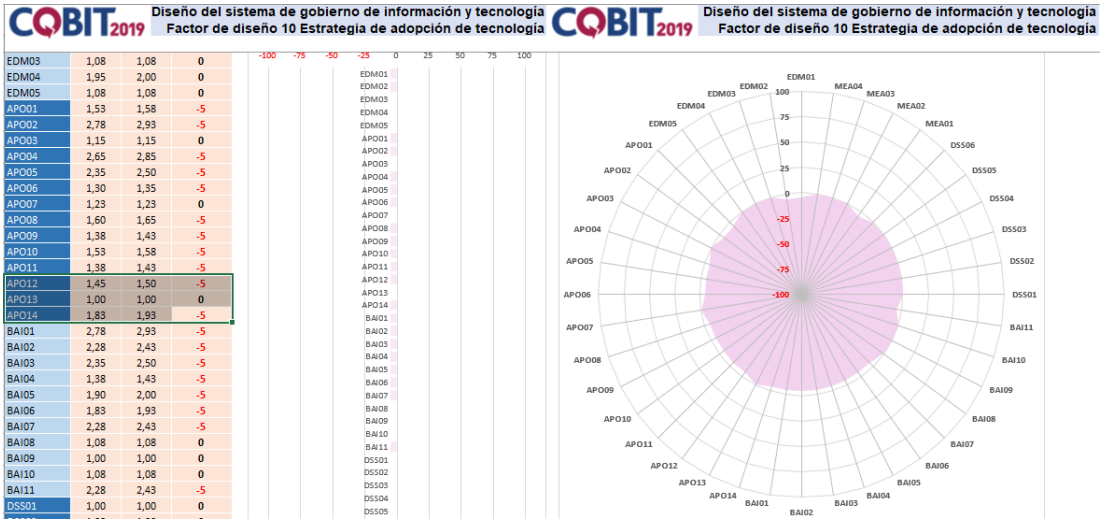


Ilustración 24: La importancia relativa de los objetivos de gobierno y gestión COBIT® 2019 es levemente a la baja a partir de la estrategia de adopción de tecnología de la UNED.

Fuente: Elaboración propia a partir de los valores ingresados en la herramienta de diseño COBIT® 2019.

Finalmente, para el paso 3, la herramienta de diseño COBIT® 2019 brinda un segundo resumen (**Perfeccionar** el alcance inicial del sistema de gobierno) a partir de los factores de diseño 5 al 10. En este resumen se observa cómo se consolidan y se refinan los resultados obtenidos y los principales objetivos COBIT® 2019 de gobierno y gestión, es decir los objetivos de gobierno y gestión prioritarios para el caso de estudio:

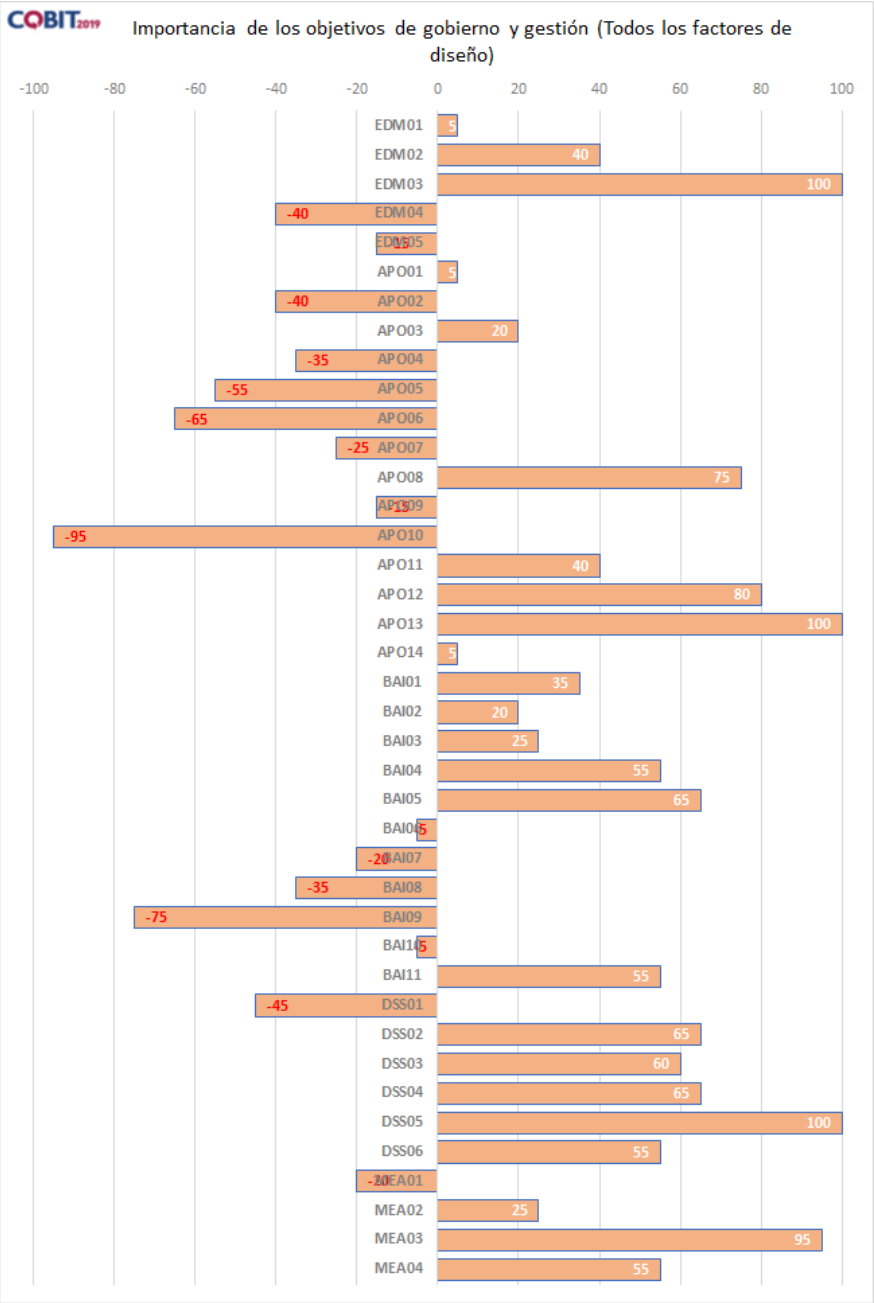


Ilustración 25: Resumen de objetivos de gobierno y gestión COBIT® 2019 relevantes para el paso 3 (Factores de diseño 5 al 10).

Fuente: Elaboración propia a partir de los valores ingresados en la herramienta de diseño COBIT® 2019.

La figura anterior corresponde al resultado del Paso 3, el cual muestra los valores perfeccionados para el caso de estudio. Es destacable el incremento hacia una importancia alta en el objetivo de gobierno EDM03-Asegurar la optimización del riesgo, así como para los objetivos de gestión APO12-Gestionar el riesgo, APO13-Gestionar la seguridad, DSS05-Gestionar los servicios de seguridad y MEA03-Gestionar el cumplimiento de los requisitos externos, entre otros.

Los anteriores objetivos y sus respectivos resultados de importancia o prioridad para la UNED reflejan la situación de la seguridad de la información de la infraestructura tecnológica virtual de esta institución, siendo el análisis previo un insumo importante para la UIT y la DTIC en sus funciones como áreas directoras de tecnologías de la información. Estas unidades vienen tomando buenas decisiones en gestión e inversión por citar dos ejemplos, pero existe también una oportunidad de mejora en aspectos vinculados a la seguridad de la información, evidenciada a la luz del marco de trabajo COBIT® 2019 aplicado al caso real de la UNED.

La información obtenida en este apartado será el insumo para el siguiente, cuyo fin será establecer una propuesta de Plan Director de Seguridad, para luego cerrar con las conclusiones o recomendaciones al respecto.

4.1.5 Entregable D1-Plan director propuesto para la gestión de la seguridad informática.

El siguiente apartado constituye el punto final del presente capítulo, y consta de la presentación de la propuesta de un Plan Director de Seguridad para la UNED, específicamente para las áreas involucradas en la infraestructura tecnológica virtual a cargo de la DTIC.

Esta propuesta de Plan Director de Seguridad tiene su fundamento en la investigación realizada en la infraestructura tecnológica virtual existente en la institución, la cual fue sometida a evaluación mediante normas de seguridad y al marco de trabajo COBIT® 2019 en los apartados anteriores, cuyos resultados permitieron su elaboración.

Dentro del ámbito de los profesionales en seguridad de la información un “Plan Director de Seguridad consiste en la definición y priorización de un conjunto de proyectos en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial [27]”. Lo anterior resulta adecuado para el caso de estudio planteado y los resultados analizados previamente, que mediante la aplicación de COBIT® 2019 no solo brinda una situación inicial, sino que detalla objetivos relacionados a la seguridad de la información con valores de importancia cuantificados, con

los que podemos establecer prioridades en seguridad de información para la infraestructura tecnológica virtual de la UNED.

Plan director para la gestión de la seguridad informática de los equipos físicos, virtuales, y para los servicios ofrecidos a través de la infraestructura tecnológica de virtualización en la UNED

1- Definiciones del Plan Director de Seguridad propuesto:

A- Alcance del Plan Director de Seguridad propuesto

El presente apartado tiene un alcance delimitado por la plataforma tecnológica conformada por los equipos físicos y virtuales, así como los servicios contenidos en estos, los cuales son administrados por la UIT dentro de la DTIC.

B- Activos de Información

- Procesos relacionados a los equipos físicos y virtuales de la plataforma tecnológica administrada por la UIT dentro de la DTIC.
- Personas con información relevante para la gestión de equipos físicos y virtuales de la plataforma tecnológica administrada por la UIT dentro de la DTIC.
- Centro de datos principal y alterno que alojan los equipos físicos y virtuales de la plataforma tecnológica administrada por la UIT dentro de la DTIC.
- Software o ficheros con información de la organización, los cuales conforman los diferentes servicios contenidos en los equipos físicos y virtuales de la plataforma tecnológica administrada por la UIT dentro de la DTIC.

C- Responsable de activos

Todo aquel personal técnico o administrativo, comisión debidamente autorizada con potestades o limitaciones y cualquier dependencia, persona o usuario de la UNED o autorizado por esta, que tenga acceso o administre información de los diferentes servicios o equipos físicos y virtuales de la plataforma tecnológica administrada por la UIT dentro de la DTIC.

Las responsabilidades pueden ser definidas por perfiles o roles, siendo incluso un ente (persona, comisión, dependencia u otros mencionados anteriormente) el responsable de uno o varios activos y ser parte de diferentes perfiles o roles.

D- Controles

Son las medidas de tipo técnicas, legales, o de normativa interna de la UNED y aplicadas a los diferentes servicios y equipos físicos y virtuales de la plataforma tecnológica administrada por la UIT dentro de la DTIC, cuyo fin es brindar medidas de seguridad informática ante los riesgos que puedan exponerse esos servicios y equipos. Los controles responden a las necesidades propias de la UNED, por lo que son específicos a servicios prioritarios, equipos críticos y funciones propias del negocio.

2-Situación inicial (sustentado en los resultados COBIT® 2019):

A partir del caso de estudio y de los resultados obtenidos mediante la aplicación de COBIT® 2019 en el análisis de la infraestructura tecnológica de virtualización en la UNED, se tiene el punto de partida para la siguiente etapa, que consiste en la definición de los objetivos prioritarios de interés para la seguridad de la información de dicha infraestructura:

Del análisis de resultados, se obtienen los siguientes valores con **importancia alta** y su respectivo propósito definido por COBIT® 2019 para los objetivos de gobierno y gestión:

A- Optimización y gestión del riesgo: “Asegurarse de que el riesgo de negocio relacionado con la I&T no exceda el apetito y tolerancia al riesgo de la empresa, que se identifique y gestione el impacto del riesgo de I&T para el valor de negocio y que se minimicen los posibles fallos de cumplimiento. [28]” y además “Integrar la gestión del riesgo empresarial relacionado con la I&T con la gestión del riesgo empresarial global, y equilibrar los costes y beneficios de la gestión del riesgo empresarial relacionado con las I&T. [28]”

B- Gestión de la seguridad: “Mantener el impacto y la ocurrencia de incidentes de seguridad de la información dentro de los niveles de apetito de riesgo de la empresa. [28]”

C- Gestionar los servicios de seguridad: “Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad de la información. [28]”

D- Gestionar el cumplimiento de los requisitos externos: “Asegurarse de que la empresa cumpla con todos los requisitos externos aplicables. [28]”

Del mismo análisis de resultados, también se extraen como referencia los siguientes valores con **importancia media** y su respectivo propósito definido por COBIT® 2019 para los objetivos de gobierno y gestión:

E- Gestionar las peticiones y los incidentes de servicio: “Lograr una mayor productividad y minimizar las interrupciones mediante la resolución rápida de consultas e incidencias de los usuarios. Evaluar el impacto de los cambios y hacer frente a los incidentes del servicio. Resolver las solicitudes de los usuarios y restaurar el servicio como respuesta ante incidentes. [28]”

F- Gestionar la continuidad: “Adaptarse rápidamente, continuar con las operaciones del negocio y mantener la disponibilidad de los recursos y la información a un nivel aceptable para la empresa en caso de una interrupción significativa (p.ej., amenazas, oportunidades, demandas). [28]”

G- Gestionar los problemas: “Aumentar la disponibilidad, mejorar los niveles de servicio, reducir los costes y atender mejor las necesidades del cliente y lograr su satisfacción mediante una reducción del número de problemas operativos, e identificar las causas raíz como parte de la resolución de problemas. [28]”

H- Gestión de la disponibilidad y capacidad: “Mantener la disponibilidad del servicio, la gestión eficiente de los recursos y la optimización del rendimiento del sistema a través de la predicción de los requisitos futuros de rendimiento y capacidad [28]”

I- Gestionar los controles de procesos de negocio: “Mantener la integridad de la información y la seguridad de los activos de información manejados dentro de los procesos de negocio, dentro de la empresa u operación externalizada. [28]”

3-Situación actual de la seguridad de la información:

En concordancia con las pautas anteriormente descritas, surge la siguiente valoración técnica de la seguridad de la información de la infraestructura tecnológica de virtualización en la UNED:

- La DTIC cuenta con un plan de administración del riesgo, revisado anualmente y alineado a su plan de operaciones anual. Este plan responde a los riesgos que puedan afectar la atención de los requerimientos de mantenimiento y mejora de los sistemas de información, el soporte técnico a los usuarios y la atención de eventos y amenazas de seguridad de informática, así como comprometer el acceso a los servicios y la conectividad de la plataforma tecnológica del centro de datos principal y alterno.
- La DTIC asigna recurso limitado a la atención de la seguridad de la información, específicamente en la Unidad de Seguridad Digital, cuyos esfuerzos incluyen la atención de riesgo ante eventos y amenazas de seguridad, que permitan mantener la continuidad y disponibilidad de los servicios y enfocan parte de sus actividades técnicas en la infraestructura, sistemas de información y protección de la información y privacidad de los usuarios mediante equipos o soluciones de software dedicados a la seguridad. La DTIC no cuenta con un Sistema de Gestión de la Seguridad de la Información (SGSI) claramente definido, que le permita hacer una gestión integral de lo descrito anteriormente.
- La DTIC ha realizado un importante esfuerzo para definir y establecer políticas de seguridad propias de la institución, en cumplimiento de las regulaciones internas y externas, incluyendo el desarrollo de manuales de uso apropiado de equipos de cómputo y acceso a los diferentes servicios mediante roles y privilegios de acceso según el rol y la función. Sin embargo, si bien existe un mapeo general o monitoreo de la seguridad de estos roles, privilegios y servicios, las iniciativas aún requieren de mayor madurez y gestión para lograr un nivel óptimo que le permita prevenir y atender eventos o amenazas hacia sus equipos físicos o virtuales que componen la plataforma tecnológica.

- En cuanto a la importancia del cumplimiento de regulaciones internas y externas, la UNED está bien posicionada y en este aspecto, la DTIC con sus procesos de I&T es parte del éxito alcanzado. Efectivamente el "Índice Institucional de Cumplimiento de Disposiciones y Recomendaciones" (IDR 2019) de la Contraloría General de la República (CGR) coloca en el primer lugar a la Universidad Estatal a Distancia (UNED) en la lista de instituciones públicas de mayor complejidad y con mayor cantidad de disposiciones, que atienden con eficacia, eficiencia y una adecuada gestión las recomendaciones emitidas en los informes de auditoría. [29]" "El IDR es un instrumento que promueve la mejora en la gestión, la rendición de cuentas y la transparencia de la Administración Pública… La UNED obtuvo una nota perfecta de 100. [29]" Lo anterior es una fortaleza de la institución, lo cual se debe aprovechar para realizar mejoras en la seguridad de la información en alineamiento con las regulaciones gubernamentales existentes en la materia, principalmente derivadas de la Contraloría General de la República y del Poder Ejecutivo a través de las iniciativas de Ciberseguridad del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), entre otros.
- La atención de incidentes de servicio en la plataforma tecnológica es gestionada por la UIT dentro de la DTIC. Cuenta con un detalle de incidentes reportados, les da tratamiento oportuno, mantiene un adecuado nivel de comunicación y atención al usuario, establece tiempos de resolución predeterminados y genera reportes detallados de las diferentes situaciones. Lo anterior se puede entender como una fortaleza de la DTIC, si bien existe aún la posibilidad de incorporar mejoras en aspectos de seguridad de la información, a fin de disminuir la posibilidad de ocurrencia de este tipo de eventos.
- Las autoridades de la institución y la DTIC actualmente trabajan en un documento que plantea el manejo integral de la continuidad del negocio, el cual incluye aspectos fundamentales de Análisis de

Impacto al Negocio (BIA), Plan de Continuidad del Negocio (BCP) y Plan para la Recuperación de Desastres (DRP). Este documento se encuentra en una etapa avanzada de elaboración por parte de una comisión institucional que considera el contexto actual de la UNED. Una vez finalizado y aprobado, será una fortaleza para la UNED, pudiendo incluso ser mejorado en aspectos de seguridad de la información a partir de los hallazgos y conclusiones del presente trabajo final de Maestría. Se aclara sin embargo que, debido a su avanzado estado de elaboración, estas mejoras exceden el alcance del presente trabajo.

- La UNED y la DTIC no enfrentan una problemática general en incidentes recurrentes en la operación de la infraestructura tecnológica virtual. En los casos en que esto ha ocurrido, se viene realizando un detalle de la atención de dichos incidentes, pero no estadísticas detalladas o análisis que identifiquen o clasifiquen este tipo de problemas de nivel operativo. Por lo tanto, se considera que ampliar el espectro de la información que se recolecta podría constituir una oportunidad de mejora para fortalecer la seguridad de la información institucional.
- La DTIC realiza anualmente un análisis general de las necesidades tecnológicas para dar sostenibilidad a los servicios en función de su contexto actual. A partir de ello, se presenta como una oportunidad de mejora el uso de un marco de trabajo para la creación de evaluaciones de capacidades actuales de la DTIC y la planificación de las necesidades futuras que permitan garantizar los recursos y la disponibilidad de los servicios de la infraestructura tecnológica.
- La infraestructura tecnológica administrada por la UIT dentro de la DTIC, en su red de telecomunicaciones y centros de datos, alberga la información de los diferentes procesos de la UNED. La protección de la información y la seguridad de los procesos y herramientas tecnológicas es responsabilidad del personal de la UIT, que establece controles que deben ser cumplidos por los colaboradores de la institución y por terceros involucrados. Para

implementar esos controles, no se utilizan estándares ni buenas prácticas internacionalmente reconocidas. Cuando ha sido requerido el acceso a la información por parte de terceros, estos deben cumplir con la normativa interna establecida para ese fin por la UNED y por las normas externas aplicables.

4-Iniciativas específicas propuestas para mejorar el nivel de la seguridad de la información de la infraestructura tecnológica del caso de estudio:

A continuación, se presenta la lista de las iniciativas que se proponen para atender la seguridad de la información de la infraestructura tecnológica del caso de estudio de la UNED, las cuales surgen a raíz del análisis realizado:

Tabla 12: Iniciativas que conforman la propuesta del Plan Director de Seguridad del caso de estudio.

INICIATIVA DE SEGURIDAD	DESCRIPCIÓN	APOYO DOCUMENTAL
1-Desarrollar políticas y/o normativa de seguridad para los diferentes componentes físicos y virtuales de la infraestructura tecnológica y servicios contenidos en esta.	Generar normativa interna que responda a los requerimientos mínimos de seguridad de la información para proteger la infraestructura tecnológica actual, en concordancia con las políticas institucionales existentes, sustentada en la valoración existente de riesgos en I&T y en normas propias de la seguridad de la información, compatibles con la UNED. -Obtener el compromiso de las unidades estratégicas de la DTIC. -Elaborar controles mínimos de seguridad informática acorde a los riesgos identificados. -Mejorar la gestión del inventario de activos de información, incluyendo su actualización periódica y gestión de responsables.	-Sistema Específico de Valoración de Riesgo Institucional (SEVRI) de la UNED. - Ley General de Control Interno N°8292. -ISO/IEC 27005. -CMMI Data Management Maturity Model. -ISF, The Standard of Good Practice for Information Security. -ISO/IEC 27001. -CMMI Cybermaturity Platform. -PMBOK Guide, 6.ª

		edición.
2-Diseño inicial de un SGSI.	Diseñar un Sistema de Gestión de la Seguridad de la Información (SGSI), con alcance integral, a fin de proteger la infraestructura tecnológica virtual y los servicios. -Contemplar las actividades actuales de atención de eventos y amenazas de seguridad informática, continuidad y disponibilidad de los servicios. -Definir el alcance del SGSI, los activos de información que son abarcados y los procesos involucrados, incluyendo sus controles, responsabilidades. -Definir la ruta o pasos a seguir para la implementación y mantenimiento del SGSI diseñado.	- ISO/IEC 20000-1 - ISO/IEC 27001. - ISO/IEC 27002. - ITIL V3. - **COBIT® 2019: APO13-Gestionar la seguridad** -Estrategia Nacional de Ciberseguridad Costa Rica 2017. San José, CR, MICITT, 2017. - ISF, The Standard of Good Practice for Information Security. - CMMI Data Management Maturity Model. - The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1. -CMMI Cybermaturity Platform. - Skills Framework for the Information Age V6. - Institute of Standards and Technology Special Publication 800-53. -HITRUST CSF versión 9
3-Plan de continuidad	Incluir los equipos y servicios de la	-Política de

del negocio	infraestructura tecnológica virtual de la UNED, dentro del alcance del plan de continuidad del negocio. -Atender las interrupciones ocasionadas por eventos no planificados que puedan afectar la infraestructura tecnológica virtual. -Establecer para la UNED los valores aceptables de recuperación de las operaciones, y de disponibilidad de la infraestructura y sus servicios críticos.	continuidad del negocio de la DTIC. (En desarrollo, próximo a implementarse).
4-Optimizar la atención de incidentes recurrentes relacionados a la operación de la infraestructura tecnológica virtual	Documentar los incidentes operativos recurrentes que afecten o puedan afectar la infraestructura tecnológica virtual y los servicios críticos, para realizar un análisis que permita optimizar su resolución y crear oportunidades de prevención y mejora. -Documentar incidentes de manera exhaustiva. -Identificar causas de incidentes relacionadas a la infraestructura tecnológica virtual, y establecer pasos a seguir para corregir o modificar los aspectos disfuncionales, a fin de corregir problemas de disponibilidad del servicio, adquirir equipos más adecuados o utilizar los recursos existentes de manera más efectiva.	- ISO/IEC 20000-1 sección 8.2 Administración de problemas. -CMMI Cybermaturity Platform. - ITIL V3.
5-Gestionar la capacidad de la infraestructura tecnológica virtual	Gestionar la capacidad de la infraestructura tecnológica virtual en función de los requisitos de los servicios soportados en la DTIC y para la UNED, considerando el rendimiento y los valores óptimos de disponibilidad esperada para estos servicios. -Documentar los requerimientos de recursos actuales y a futuro que resulten adecuados para la UNED. -Establecer valores óptimos de nivel de	-Propuesta de Marco de Gobierno y Gestión TI de la UNED (En desarrollo con CONARE). -Documentación interna de la UNED, planificación de capacidad,

	recursos para los requerimientos y brindar seguimiento continuo.	suministro y nivel de servicio. -CMMI Cybermaturity Platform. -ISF, The Standard of Good Practice for Information Security. -ISO/IEC 20000-1. -ITIL V3.
6-Establecer y documentar controles de integridad de la información para la infraestructura tecnológica virtual.	Proponer uso de normativas para la seguridad de la información, específicamente con el fin de atender la integridad de los activos de información de la infraestructura tecnológica virtual. -Extender el uso de estas normativas o buenas prácticas de seguridad a los proveedores que brinden servicios a la infraestructura tecnológica virtual.	-ISO/IEC 27002 sección 7. -National Institute of Standards and Technology Special Publication 800-37. -The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1. -ISF, The Standard of Good Practice for Information Security 2016: BA1.4 Information Validation. -CMMI Cybermaturity Platform: gestion de acceso. -Skills Framework for the Information Age V6, 2015, seguridad y gestión secciones SCTY y SCAD.
7-Otras consideraciones en	Complementar la seguridad de la información de la infraestructura	-ISO/IEC 27001 -Creating a Culture

seguridad de la información.	tecnológica virtual mediante actividades de concientización, ampliando las existentes o generando nuevas y mejorar la comunicación entre las diferentes áreas involucradas, a fin de trabajar la seguridad de la información de la infraestructura tecnológica virtual de una manera integral y transversal a las áreas de la UNED.	of Security, ISACA, 2011

Fuente: Elaboración propia a partir de los resultados de la investigación y aplicación de COBIT® 2019 al caso de estudio en la UNED.

La tabla anterior es la lista de iniciativas claves en seguridad de la información que surgen a partir de la investigación realizada. Estas iniciativas responden a los hallazgos obtenidos al aplicar el marco de trabajo COBIT® 2019 al caso de estudio de la UNED y están alineadas con las prioridades institucionales identificadas en la UNED.

Las iniciativas de la propuesta de Plan Director de Seguridad deben ser ordenadas por prioridad institucional, evaluadas por las autoridades para definir su ruta de ejecución y finalmente aprobadas, quedando a criterio de las autoridades de la UNED y la DTIC realizar una interpretación de las conclusiones y recomendaciones del presente documento.

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES

Con fundamento en el trabajo realizado y en función de los objetivos planteados, se alcanzan las siguientes conclusiones y recomendaciones:

5.1Conclusiones

- No caben dudas respecto a las crecientes necesidades que muestran las organizaciones de distinta naturaleza y tamaño en materia de seguridad de la información. La UNED no escapa de esta realidad. Si bien no es una institución privilegiada en recursos tecnológicos, tampoco se encuentra en una situación totalmente desfavorable. Es indudablemente una organización de grandes dimensiones por su constitución orgánica y de relevancia nacional. Por lo tanto, se transforma en el blanco de incidentes que comprometen la seguridad de la información y enfrenta dificultades para hacerle frente y sobreponerse en tiempo y forma.
- Resulta indiscutible el crecimiento en el uso de infraestructura tecnológica virtual y de los servicios en la nube por parte de las organizaciones modernas, lo cual ocasiona un avance tecnológico que ensancha la brecha en cuanto a preocupaciones vinculadas a la seguridad de la información. En este contexto, la UNED presenta dificultades para el tratamiento de sus equipos críticos, para la identificación de los activos de información, procesos y servicios críticos soportados por los equipos virtuales que administra la DTIC.
- Como cualquier otra organización, la UNED tiene procesos prioritarios que requieren una serie de medidas específicas de protección de la información, incluyendo los aspectos de gestión. En este aspecto, la UNED debe mejorar las cuestiones vinculadas al alineamiento con las necesidades específicas del negocio, buscando un nivel adecuado de seguridad de la información. En caso contrario, se podría estar ensanchando la brecha en seguridad, dejando más expuesta a la institución.
- Actualmente existen normativas técnicas y marcos de trabajo en seguridad de la información con versiones estables y maduras, capaces

de responder a las necesidades de las organizaciones actuales. Esto representa un aliciente para trabajar con tecnologías de información e infraestructura tecnológica virtual de manera apropiada y potenciar las metas del negocio. Para el caso de la UNED, es una oportunidad de mejora que puede proyectarse con alto impacto en la institución con el fin de proteger su plataforma tecnológica y los servicios ofrecidos en esta.

- Llevar a cabo la implementación de normativas y marcos de trabajo en seguridad de la información, si bien requiere de recursos, y fundamentalmente tiempo, no representa un alto costo respecto a los valiosos beneficios que produce, y que pueden ser traducidos fácilmente en valor demostrable para la organización.
- El marco de trabajo COBIT® 2019 es definitivamente un valioso recurso para la atención prioritaria de la seguridad de la información de la organización, más allá de sus múltiples características beneficiosas en tecnologías de la información. Cabe resaltar su reciente actualización que permite ser aplicado de manera flexible en cualquier tamaño de organización, no requiere su implementación total de manera que se puede trabajar por áreas o procesos prioritarios. Para el caso de la seguridad de la información, brinda objetivos específicos de gobierno y gestión que permiten la integración de las normas existentes en la materia, considerando incluso las internas o propias de cada organización.
- Adicionalmente, el uso de un marco de trabajo como COBIT® 2019, que cubre a la organización de extremo a extremo tanto para el gobierno como para la gestión, contribuye a garantizar su permanente actualización y adaptación en el tiempo, permitiendo integrar nuevas tecnologías de manera segura, manteniendo un nivel de protección adecuada de los activos de la organización y considerando actualizaciones en función del avance tecnológico futuro.
- En la presente investigación, se entrega una primera versión del Plan Director de Seguridad para atender las necesidades específicas de la UNED en cuanto a su plataforma virtualizada. Además, este plan considera la necesidad de identificar los servicios críticos soportados por

los equipos virtuales que administra la DTIC y motiva la creación de un sistema de gestión de la seguridad de la información.

5.2 Recomendaciones

- Se sugiere a las autoridades la utilización de COBIT® 2019 como el marco de trabajo reconocido para la gestión de la seguridad de la información de manera sustentable en el tiempo.
- El desarrollo de la investigación permite recomendar el uso de COBIT® para la UNED, así como para cualquier otra organización similar que requiera evaluar la seguridad de la información y potenciar la protección de sus activos de información, generando valor a partir de su utilización.
- Se propone como posible línea de investigación futura la valoración de las características del marco de trabajo COBIT® 2019, haciendo una comparativa con otros marcos de trabajo, metodologías o normas existentes, a fin de evaluar su flexibilidad, compatibilidad y modernidad, entre otros rasgos que permiten atender la seguridad de la información, especialmente al momento de incorporar nuevas tecnologías.
- Finalmente, se insta al lector o personas interesadas en el tema de estudio, valorar la práctica de nuevas investigaciones sobre los aspectos puntuales que ofrece el marco de trabajo COBIT® 2019 en los apartados referidos al gobierno y gestión de la seguridad de la información.

BIBLIOGRAFÍA

[1] R. Hernández Sampieri, C. Fernández y Pilar Baptista, Metodología de la Investigación, Mexico DF: McGraw-Hill, 2006.

[2] UNED, «UNED, institución pionera de la educación a distancia en Costa Rica,» UNED, 17 01 2020. [En línea]. Available: https://www.uned.ac.cr/conociendo-la-uned/historia-y-propuesta. [Último acceso: 17 01 2020].

[3] UNED, «¿Cómo se estudia a distancia y con qué recursos cuento?,» UNED, 17 01 2020. [En línea]. Available: https://principal.uned.ac.cr/ami/adquisiciones/199-conociendo-la-uned/1060-metodologia-y-recursos. [Último acceso: 17 01 2020].

[4] UNED, «INFORME SOBRE EL PROCESO DE CONSULTA MEDIANTE LA IMPLEMENTACIÓN DE MESAS TEMÁTICAS PARA LA CONSTRUCCIÓN DE LOS FUNDAMENTOS PARA EL PLAN DE DESARROLLO ACADÉMICO UNED 2012-2017,» Vicerrectoría Académica UNED, San José, CR, 2013.

[5] P. S. Barrantes, *La Seguridad Informática en infraestructuras tecnológicas virtuales,* Ciudad Autonoma de Buenos Aires, Argentina: FCE-UBA biblioteca digital, 2019.

[6] U. Veracruzana, «Seguridad de la información,» Universidad Veracruzana, 2020. [En línea]. Available: Uv.mx, «Seguridad de la información,» 2019. [En línea]. Available: https://www.uv.mx/celulaode/seguridad-info/tema1.html. [Último acceso: 18 01 2020].

[7] P. A. López, «Seguridad informática,» de *Seguridad informática*, Madrid, Editex, 2010, p. 9.

[8] ISOTools Excellence, «Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad,» ISOTools Excellence, 01 02 2018. [En línea]. Available: https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/. [Último acceso: 09 02 2020].

[9] ISACA, «Resumen Ejecutivo,» de *COBIT 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*, Rolling Meadows, IL 60008 EE.UU., ISACA, 2012, pp. 13, 14.

[10] A. Bernal, A. Oneto, M. Penfold, L. Schneider y J. Wilcox, N° 6. Gobierno Corporativo en América Latina. Importancia para las empresas de propiedad estatal. Serie Políticas Públicas y Transformación Productiva, Caracas: CAF Banco de Desarrollo de América Latina, 2012.

[11] E. d. P. GERENS, «Gestión de riesgos: ¿Qué es? ¿Por qué emplearla? ¿Cómo emplearla?,» GERENS ESCUELA DE POSTGRADO, 18 12 2017. [En línea]. Available: https://gerens.pe/blog/gestion-riesgo-que-por-que-como/. [Último acceso: 21 01 2020].

[12] Deloitte Touche Tohmatsu Limited (DTTL), «Los retos de la función de Compliance,» Deloitte Touche Tohmatsu Limited (DTTL), 2020. [En línea]. Available: https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/retos-de-la-funcion-compliance.html. [Último acceso: 20 01 2020].

[13] Y. R. U. S. Galaz, «GRC como mejor práctica Boletín Gobierno Corporativo | Otoño 2009,» 2009. [En línea]. Available: https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/Gobierno-Corporativo/grc-como-mejor-practica.pdf. [Último acceso: 20 01 2020].

[14] Dirección de Tecnología de Información y Comunicaciones, «Objetivos:Marco Jurídico en Tecnologías de la Información y las Comunicaciones de la UNED,» DTIC, 16 08 2017. [En línea]. Available: https://www.uned.ac.cr/dtic/normas-tecnicas/mj/objetivos. [Último acceso: 20 01 2020].

[15] ISACA, «Gobierno empresarial de la Información y Tecnología,» de *COBIT 2019 Marco de Referencia, Introdución y Metodología*, Schaumburg, IL 60173, USA, ISACA, 2018, p. 11.

[16] ISACA, «Principios de COBIT,» de *COBIT 2019 Marco de Referencia, Introdución y Metodología*, Schaumburg, IL 60173, USA, ISACA, 2018, pp. 11,17,18.

[17] ISACA, «4.2 Objetivos de gobierno y gestión,» de *MARCO DE REFERENCIA COBIT® 2019: INTRODUCCIÓN Y METODOLOGÍA*, Schaumburg, IL 60173, USA, ISACA, 2018, pp. 20,21.

[18] ISACA, «3.4 Mejoras en COBIT® 2019,» de *MARCO DE REFERENCIA COBIT® 2019: INTRODUCCIÓN Y METODOLOGÍA*, Schaumburg, IL 60173, USA, ISACA, 2018, p. 18.

[19] ISACA, «6.4.1 Niveles de capacidad del proceso,» de *MARCO DE REFERENCIA COBIT® 2019: INTRODUCCIÓN Y METODOLOGÍA*, Schaumburg, IL 60173, USA, ISACA, 2018, p. 39.

[20] ISOTools Excellence, «SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información,» ISOTools Excellence, 04 04 2014. [En línea]. Available: https://www.pmg-ssi.com/2014/04/iso-27014-gobernanza-de-seguridad-de-la-informacion/. [Último acceso: 23 01 2020].

[21] A. O. Huerva, «Guía de controles de ciberseguridad para la protección integral de la pyme,» Universitat Oberta de Catalunya, Barcelona, España, 2017.

[22] S. Piecha, «The ISF Standard and Good Practice for I.S. por Sebastian Piecha,» Eleven Paths, 19 05 2016. [En línea]. Available: https://www.elevenpaths.com/es/noticias-y-eventos/elevenpaths-talks/the-isf-standard-and-good-practice-for-i-s/index.html. [Último acceso: 23 01 2020].

[23] ISOTools Excellence, «¿Cómo utilizar la serie SP 800 de la norma ISO 27001?,» ISOTools Excellence, 05 05 2016. [En línea]. Available: https://www.pmg-ssi.com/2016/05/como-utilizar-serie-sp-800-norma-iso-27001/. [Último acceso: 23 01 2020].

[24] NormasISO.com, «ISO 20000 CALIDAD DE LOS SERVICIOS TI,» NormasISO.com, 2020. [En línea]. Available: https://www.normas-iso.com/iso-20000/. [Último acceso: 23 01 2020].

ISACA, «Factores de diseño,» de *COBIT 2019 Marco de* [25] *Referencia, Introdución y Metodología*, Schaumburg, ILLINOIS, USA, ISACA, 2018, p. 23.

I. org, «Capítulo 6. Kit de herramientas de diseño del sistema de [26] gobierno,» de *Diseño de una solución de Gobierno de Información y Tecnología*, Schaumburg, ILLINOIS 60173,, ISACA, 2018, p. 65.

I. N. d. C. -. INCIBE_, «INCIBE_.es,» 14 06 2021. [En línea]. [27] Available: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf.

ISACA, «Objetivos de Gobierno y Gestión de COBIT: Guía [28] detallada,» de *COBIT2019 MArcod e referencia Objetivos de Gobierno y Gestión*, Schaumburg, ILLINOIS, USA, ISACA, 2018, pp. 27-296.

Acontecer Digital, «UNED lidera el ranking de cumplimiento de [29] disposiciones de instituciones públicas en Costa Rica,» Acontecer, 02 11 2019. [En línea]. Available: https://www.uned.ac.cr/acontecer/a-diario/gestion-universitaria/3847-uned-lidera-el-ranking-de-cumplimiento-de-disposiciones-de-instituciones-publicas-en-costa-rica. [Último acceso: 27 09 2021].

ANEXOS

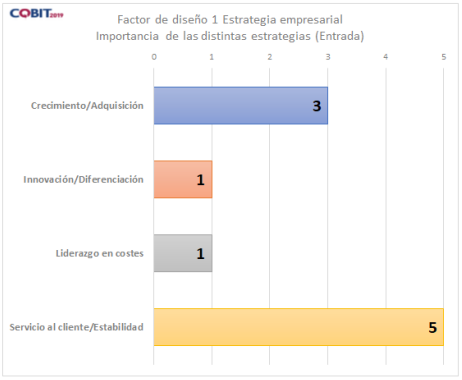
Anexo #1: Resultados de herramienta de diseño COBIT® 2019

	Paso 2: Determinar el alcance inicial del sistema de gobierno				
	Estrategia empresarial	Metas empresariales	Perfil de riesgo	Problemas relacionados con I&T	Alcance inicial: Valoración de los objetivos de gobierno/gestión
Ponderación	1	1	1	1	
EDM01—Asegurar el establecimiento y el mantenimiento del marco de gobierno	5	10	-5	0	10
EDM02—Asegurar la entrega de beneficios	25	-20	20	0	25
EDM03—Asegurar la optimización del riesgo	20	65	20	-5	100
EDM04—Asegurar la optimización de recursos	-25	-20	-5	5	-45
EDM05—Asegurar el compromiso de las partes interesadas	15	-20	-10	-10	-25
APO01—Gestionar el marco de gestión de I&T	0	10	10	-5	15
APO02—Gestionar la estrategia	-15	-20	5	-5	-35
APO03 — Gestionar la arquitectura empresarial	0	-10	30	5	25
APO04—Gestionar la innovación	-25	-25	15	5	-30
APO05—Gestionar el portafolio	-20	-15	-5	-5	-45
APO06—Gestionar el presupuesto y los costes	-25	-35	-5	5	-60
APO07—Gestionar los recursos humanos	5	-25	-5	10	-15
APO08—Gestionar las relaciones	30	-20	45	-5	50
APO09—Gestionar los acuerdos de servicio	35	-5	15	-10	35
APO10—Gestionar los proveedores	-15	-10	0	-5	-30
APO11—Gestionar la calidad	45	-30	35	-10	40
APO12—Gestionar los riesgos	20	65	5	-5	85
APO13—Gestionar la seguridad	25	65	5	-15	80
APO14—Gestionar los datos	0	-5	20	0	15
BAI01—Gestionar los programas	0	-20	30	5	15
BAI02—Gestionar la definición de requisitos	-5	-15	15	5	0
BAI03—Gestionar la identificación y construcción de soluciones	-5	-15	25	0	5
BAI04—Gestionar la disponibilidad y la capacidad	35	5	45	-25	60
BAI05—Gestionar el cambio organizativo	5	-20	40	10	35
BAI06—Gestionar los cambios de TI	0	-10	30	-10	10
BAI07—Gestionar la aceptación y la transición del cambio de TI	0	-10	0	-10	-20
BAI08—Gestionar el conocimiento	-25	-30	15	0	-40
BAI09—Gestionar los activos	0	-45	-40	15	-70
BAI10—Gestionar la configuración	0	10	0	-5	5
BAI11—Gestionar los proyectos	-10	-15	45	15	35
DSS01—Gestionar las operaciones	10	-5	-15	-20	-30
DSS02—Gestionar las peticiones y los incidentes de servicio	45	25	15	-20	65
DSS03—Gestionar los problemas	35	25	10	-15	55
DSS04—Gestionar la continuidad	45	25	5	-15	60
DSS05—Gestionar los servicios de seguridad	25	50	5	-15	65
DSS06—Gestionar los controles de procesos de negocio	10	10	25	-10	35
MEA01—Gestionar la monitorización del rendimiento y la conformidad	0	0	15	-5	10
MEA02—Gestionar el sistema de control interno	0	15	10	-10	15
MEA03—Gestionar el cumplimiento de los requisitos externos	0	65	25	-20	70
MEA04—Gestionar el aseguramiento	0	25	20	-10	35

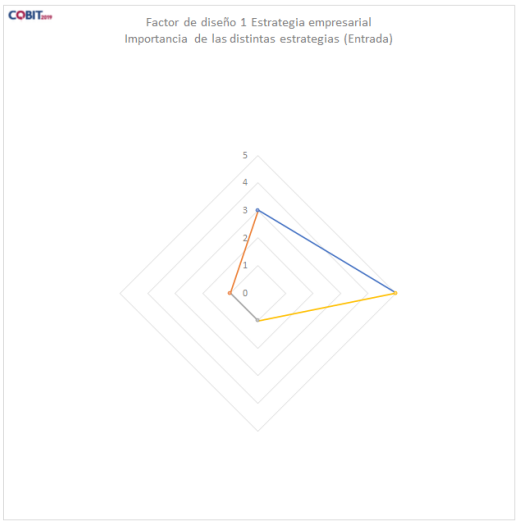
Paso 3: Perfeccionar el alcance del sistema de gobierno						
Escenario de amenazas	Requisitos de cumplimiento	Rol de TI	Modelo de abastecimiento de proveedores para TI	Métodos de implementación de TI	Estrategia de adopción de tecnología	Alcance perfeccionado: Valoración de los objetivos de gobierno/gestión
1	1	1	1	1	1	
-15	0	15	0	0	-5	5
0	0	10	0	0	-5	40
-20	10	0	-15	0	0	100
0	0	15	0	0	0	-40
-10	10	15	0	0	0	-15
-15	0	10	0	0	-5	5
0	0	10	0	0	-5	-40
-15	0	5	0	0	0	20
0	0	10	0	0	-5	-35
0	0	10	0	0	-5	-55
0	0	15	0	0	-5	-65
-10	0	5	0	0	0	-25
0	0	10	0	0	-5	75
-10	0	-5	-25	0	-5	-15
-15	10	-5	-25	0	-5	-95
-10	0	5	0	0	-5	40
-20	10	5	-15	0	-5	80
-20	10	5	0	0	0	100
-15	0	10	0	0	-5	5
0	0	10	0	5	-5	35
0	0	10	0	10	-5	20
0	0	10	0	10	-5	25
-10	0	-5	0	0	-5	55
0	0	15	0	5	-5	65
-15	0	-5	0	10	-5	-5
0	0	5	0	5	-5	-20
0	0	15	0	0	0	-35
0	0	15	0	0	0	-75
-15	0	5	0	0	0	-5
0	0	5	0	5	-5	55
0	0	-5	0	0	0	-45
-15	0	0	0	0	0	65
-10	0	0	0	0	0	60
-20	10	0	0	0	0	65
-15	20	5	0	0	0	100
-15	0	20	0	0	0	55
-15	0	15	-20	0	-5	-20
-10	0	15	0	0	0	25
-15	10	5	0	0	0	95
-15	5	15	0	0	0	55

Sección de entrada—Importancia de cada prototipo de estrategia empresarial

Valor	Importancia (1-5)	Referencia
Crecimiento/Adquisición	3	3
Innovación/Diferenciación	1	3
Liderazgo en costes	1	3
Servicio al cliente/Estabilidad	5	3

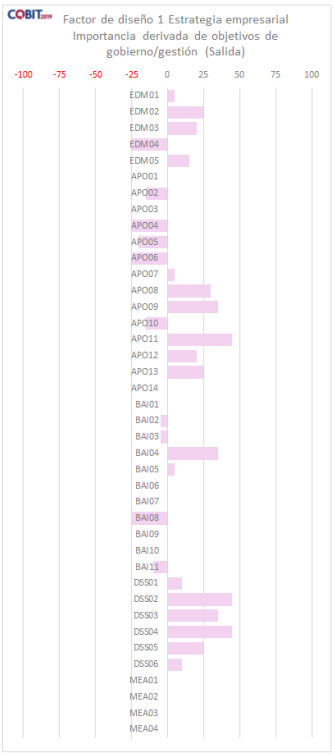


COBIT 2019 Diseño del sistema de gobierno de información y tecnología
Factor de diseño 1 Estrategia empresarial
Sección de entrada—Importancia de cada prototipo de estrategia empresarial

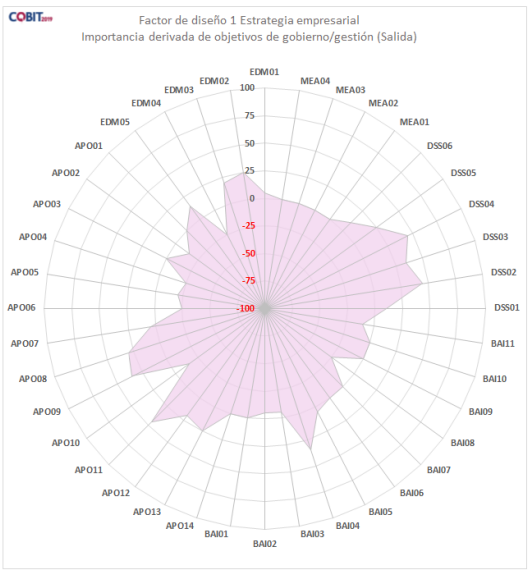


Sección de salida—Importancia relativa derivada de cada objetivo de gobierno/gestión

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	Valoración	Referencia	Importancia relativa
EDM01	13	15	5
EDM02	25	24	25
EDM03	15	15	20
EDM04	14,5	22,5	-25
EDM05	17	18	15
APO01	10	12	0
APO02	20,5	28,5	-15
APO03	20	24	0
APO04	13	21	-25
APO05	22	33	-20
APO06	14,5	22,5	-25
APO07	13	15	5
APO08	23	21	30
APO09	25,5	22,5	35
APO10	15	21	-15
APO11	25	21	45
APO12	18	18	20
APO13	17,5	16,5	25
APO14	10	12	0
BAI01	23	27	0
BAI02	10,5	13,5	-5
BAI03	10,5	13,5	-5
BAI04	20	18	35
BAI05	22,5	25,5	5
BAI06	16,5	19,5	0
BAI07	15	18	0
BAI08	12,5	19,5	-25
BAI09	10	12	0
BAI10	10	12	0
BAI11	20	27	-10
DSS01	12,5	13,5	10
DSS02	25	21	45
DSS03	20	18	35
DSS04	25	21	45
DSS05	17,5	16,5	25
DSS06	12,5	13,5	10
MEA01	10	12	0
MEA02	10	12	0
MEA03	10	12	0
MEA04	10	12	0



Sección de salida—Importancia relativa derivada de cada objetivo de gobierno/gestión



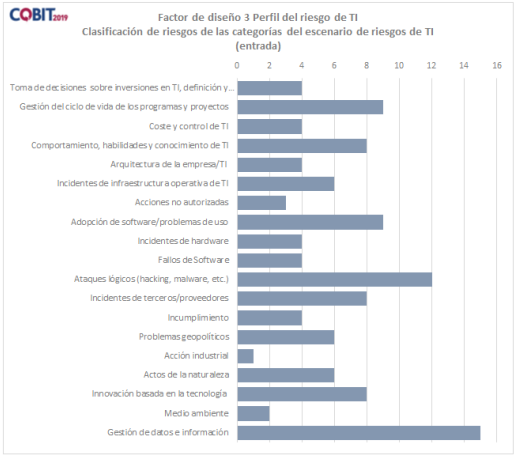
COBIT 2019 Diseño del sistema de gobierno de información y tecnología
Factor de diseño 3 Perfil del riesgo

Sección de entrada—Importancia de cada categoría genérica de riesgo de TI

Sección de entrada—Importancia de cada categoría genérica de riesgo de TI

Categoría del escenario de riesgo	Impacto (1-5)	Probabilidad (1-5)	Clasificación	Referencia
Toma de decisiones sobre inversiones en TI, definición y mantenimiento del portafolio	4	1		9
Gestión del ciclo de vida de los programas y proyectos	3	3		9
Coste y control de TI	4	1		9
Comportamiento, habilidades y conocimiento de TI	4	2		9
Arquitectura de la empresa/TI	4	1		9
Incidentes de infraestructura operativa de TI	3	2		9
Acciones no autorizadas	3	1		9
Adopción de software/problemas de uso	3	3		9
Incidentes de hardware	4	1		9
Fallos de Software	4	1		9
Ataques lógicos (hacking, malware, etc.)	4	3		9
Incidentes de terceros/proveedores	4	2		9
Incumplimiento	4	1		9
Problemas geopolíticos	3	2		9
Acción industrial	1	1		9
Actos de la naturaleza	3	2		9
Innovación basada en la tecnología	4	2		9
Medio ambiente	2	1		9
Gestión de datos e información	5	3		9

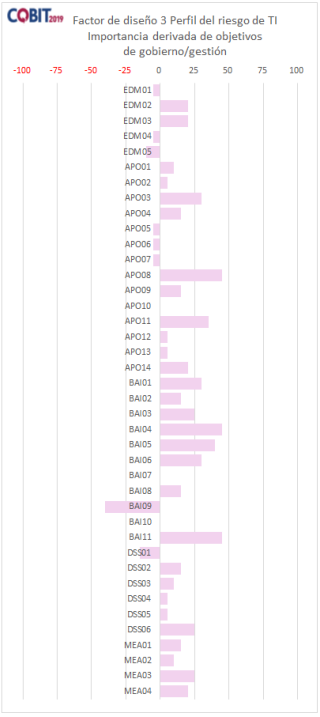
Riesgo muy alto
Riesgo alto
Riesgo normal
Riesgo bajo

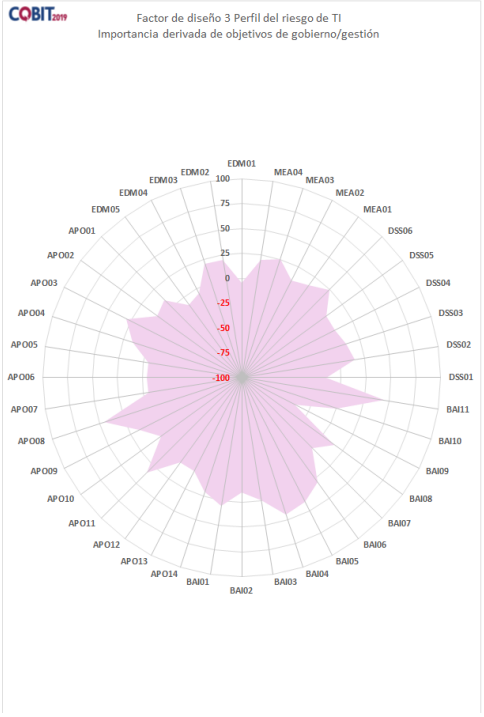


Sección de salida—Importancia relativa derivada de cada objetivo de gobierno/gestión

Sección de salida—Importancia relativa derivada de cada objetivo de gobierno/gestión

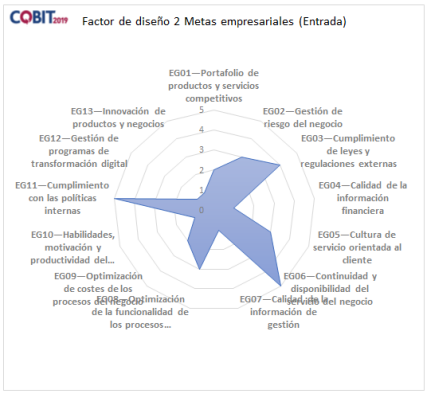
Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	Valoración	Referencia	Importancia relativa
EDM01	122	189	-5
EDM02	113	135	20
EDM03	133	162	20
EDM04	131	198	-5
EDM05	115	189	-10
APO01	246	324	10
APO02	105	144	5
APO03	151	171	30
APO04	36	45	15
APO05	92	144	-5
APO06	99	153	-5
APO07	140	216	-5
APO08	154	153	45
APO09	93	117	15
APO10	150	216	0
APO11	91	99	35
APO12	65	90	5
APO13	72	99	5
APO14	165	198	20
BAI01	71	81	30
BAI02	93	117	15
BAI03	101	117	25
BAI04	9	9	45
BAI05	70	72	40
BAI06	119	135	30
BAI07	79	117	0
BAI08	105	135	15
BAI09	15	36	-40
BAI10	68	99	0
BAI11	36	36	45
DSS01	77	135	-15
DSS02	115	144	15
DSS03	81	108	10
DSS04	152	216	5
DSS05	158	216	5
DSS06	125	144	25
MEA01	170	216	15
MEA02	185	243	10
MEA03	131	153	25
MEA04	181	225	20





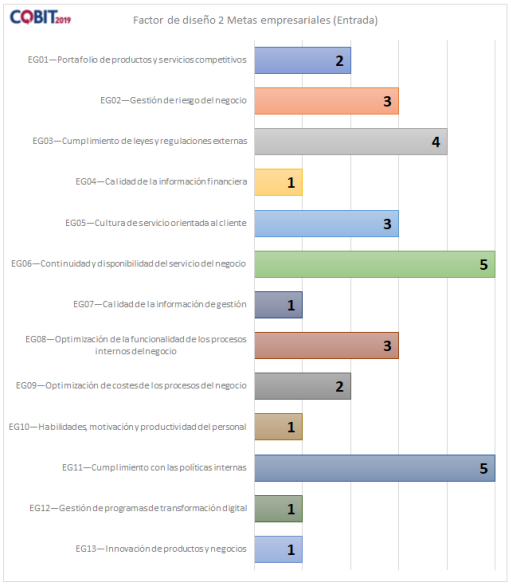
Sección de entrada—Importancia de cada meta empresarial

Valor	Importancia (1-5)	Referencia
EG01—Portafolio de productos y servicios competitivos	2	3
EG02—Gestión de riesgo del negocio	3	3
EG03—Cumplimiento de leyes y regulaciones externas	4	3
EG04—Calidad de la información financiera	1	3
EG05—Cultura de servicio orientada al cliente	3	3
EG06—Continuidad y disponibilidad del servicio del negocio	5	3
EG07—Calidad de la información de gestión	1	3
EG08—Optimización de la funcionalidad de los procesos internos del negocio	3	3
EG09—Optimización de costes de los procesos del negocio	2	3
EG10—Habilidades, motivación y productividad del personal	1	3
EG11—Cumplimiento con las políticas internas	5	3
EG12—Gestión de programas de transformación digital	1	3
EG13—Innovación de productos y negocios	1	3



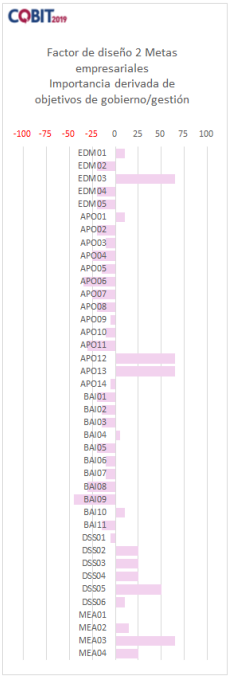
COBIT 2019 Diseño del sistema de gobierno de información y tecnología
Factor de diseño 2 Metas empresariales

Sección de entrada—Importancia de cada meta empresarial

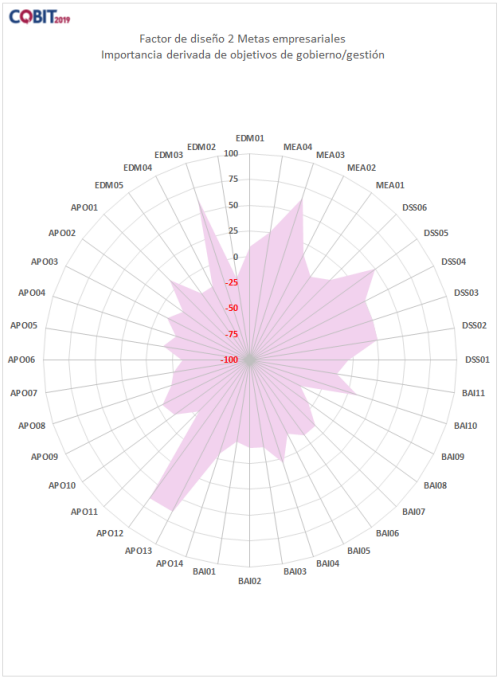


Sección de salida—Importancia relativa derivada de cada objetivo de gobierno/gestión

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	Valoración	Referencia	Importancia relativa
EDM01	89	99	10
EDM02	76	114	-20
EDM03	85	63	65
EDM04	87	129	-20
EDM05	41	63	-20
APO01	160	180	10
APO02	86	132	-20
APO03	99	135	-10
APO04	72	120	-25
APO05	100	141	-15
APO06	64	117	-35
APO07	67	108	-25
APO08	124	189	-20
APO09	49	63	-5
APO10	59	78	-10
APO11	78	132	-30
APO12	48	36	65
APO13	53	39	65
APO14	60	78	-5
BAI01	83	129	-20
BAI02	120	174	-15
BAI03	115	165	-15
BAI04	60	69	5
BAI05	121	183	-20
BAI06	68	90	-10
BAI07	50	69	-10
BAI08	80	135	-30
BAI09	22	51	-45
BAI10	16	18	10
BAI11	94	138	-15
DSS01	49	63	-5
DSS02	56	54	25
DSS03	56	54	25
DSS04	56	54	25
DSS05	101	81	50
DSS06	95	105	10
MEA01	108	135	0
MEA02	127	135	15
MEA03	53	39	65
MEA04	112	111	25



Sección de salida—Importancia relativa derivada de cada objetivo de gobierno/gestión



Sección de entrada—Importancia de cada problema genérico relacionado con I&T

Problemas relacionados con I&T	Importancia (1-3)	Referencia
Frustración entre distintas unidades de TI en toda la organización debido a una percepción de baja contribución al valor del negocio	1	2
Frustración entre distintos departamentos de la empresa (como el cliente de TI) y el departamento de TI debido a iniciativas fracasadas o una percepción de baja contribución al valor del negocio	3	2
Incidentes significativos relacionados con I&T, como pérdida de datos, violaciones de seguridad, fallo del proyecto y errores de la aplicación relacionados con TI	1	2
Problemas de ejecución del servicio por parte de los subcontratistas de TI	2	2
Incumplimiento de los requerimientos regulatorios o contractuales relacionados con TI	2	2
Hallazgos de auditoría regulares u otros informes de evaluación sobre un pobre desempeño de TI o notificación de problemas de calidad y servicio de TI	2	2
Gasto sustancial oculto y fraudulento en I&T, es decir, gasto en TI por departamentos de usuarios fuera del control de los mecanismos de decisión de inversión en IT normales y los presupuestos aprobados	3	2
Duplicaciones o coincidencias entre varias iniciativas u otras formas de recursos malgastados	1	2
Insuficientes recursos de TI, personal con habilidades inadecuadas o personal agotado / insatisfecho	3	2
Cambios o proyectos facilitados por TI que suelen no satisfacer a menudo las necesidades del negocio y que se ejecutan tarde o por encima del presupuesto	1	2
Resistencia de los miembros del consejo de administración, ejecutivos o alta gerencia a involucrarse con las TI o una falta de compromiso empresarial para patrocinar a TI	2	2
Modelo operativo de TI complejo y/o mecanismos de decisión confusos para las decisiones relacionadas con TI	1	2
Excesivamente alto coste de TI	1	2
Implementación obstaculizada o fracasada de nuevas iniciativas o innovaciones causada por la arquitectura y sistemas de TI actuales	3	2
Brecha entre conocimiento tecnológico y empresarial, lo que lleva a que los usuarios del negocio y/o los especialistas en TI hablen un idioma distinto	1	2
Problemas regulares con la calidad de los datos y la integración de datos de distintas fuentes	1	2
Nivel elevado de cómputo para usuarios finales, lo que genera (entre otros problemas) una falta de supervisión y control de calidad de las aplicaciones que se están desarrollando e implementando	2	2
Los departamentos del negocio implementan sus propias soluciones de información con poca o ninguna participación del departamento de TI de la empresa (relacionado con la computación de usuarios finales, que suele surgir de la insatisfacción con las soluciones y servicios de TI)	1	2
Ignorancia sobre y/o incumplimiento de las regulaciones de privacidad	1	2
Incapacidad para explotar nuevas tecnologías o innovar con las TI	1	2

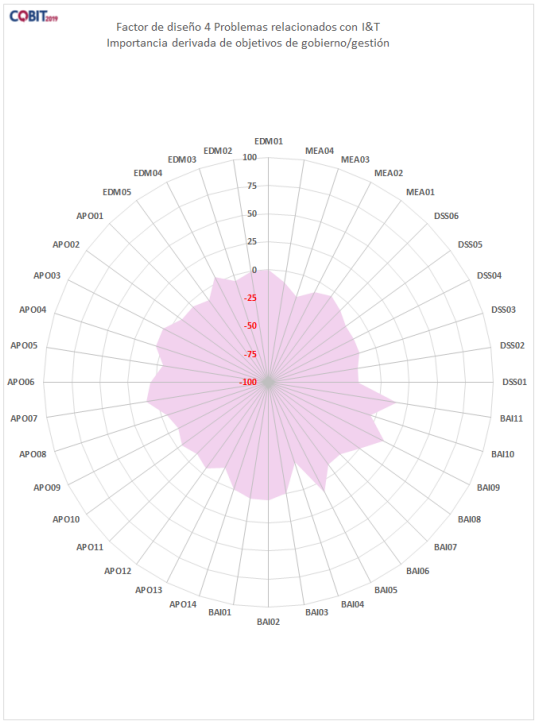
✓	Sin problema
!	Problema
✗	Problema grave

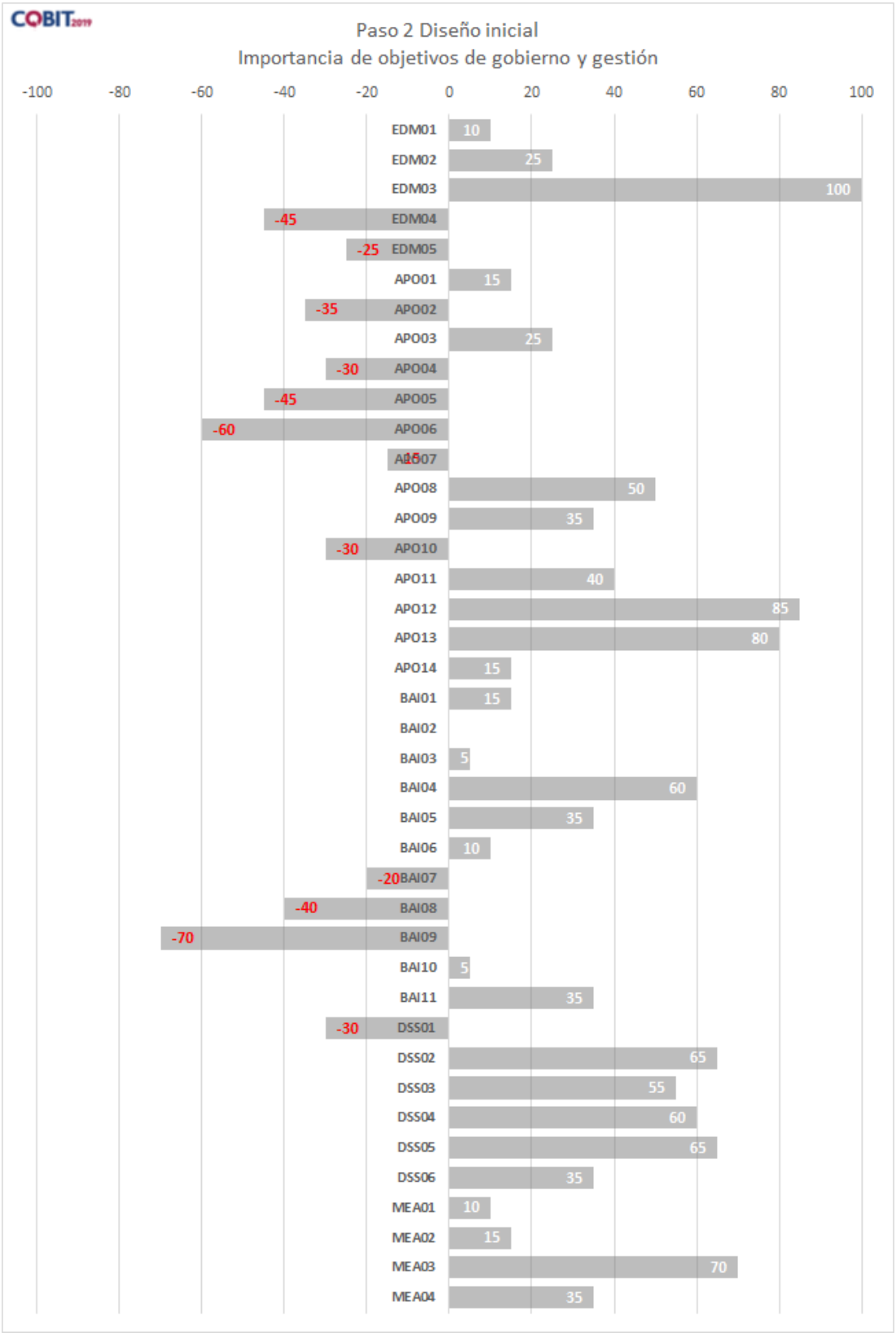
Sección de entrada—Importancia de cada problema genérico relacionado con I&T

Sección de salida—Importancia relativa derivada de cada objetivo de gobierno/gestión

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	Valoración	Referencia	Importancia relativa
EDM01	67	70	0
EDM02	69	70	0
EDM03	43,5	47	-5
EDM04	69	67	5
EDM05	35	41	-10
APO01	52	56	-5
APO02	45,5	50	-5
APO03	68	66	5
APO04	32,5	32	5
APO05	64	68	-5
APO06	62	62	5
APO07	50	47	10
APO08	66	70	-5
APO09	38	43	-10
APO10	35,5	39	-5
APO11	37	43	-10
APO12	47,5	52	-5
APO13	27	33	-15
APO14	57,5	60	0
BAI01	36	35	5
BAI02	51	51	5
BAI03	40	41	0
BAI04	17	23	-25
BAI05	30	28	10
BAI06	36	42	-10
BAI07	34	38	-10
BAI08	30,5	31	0
BAI09	25,5	23	15
BAI10	23	25	-5
BAI11	51	45	15
DSS01	21	27	-20
DSS02	26,5	33	-20
DSS03	27	32	-15
DSS04	17	21	-15
DSS05	24	29	-15
DSS06	25	29	-10
MEA01	56	61	-5
MEA02	43	48	-10
MEA03	22,5	29	-20
MEA04	51,5	58	-10

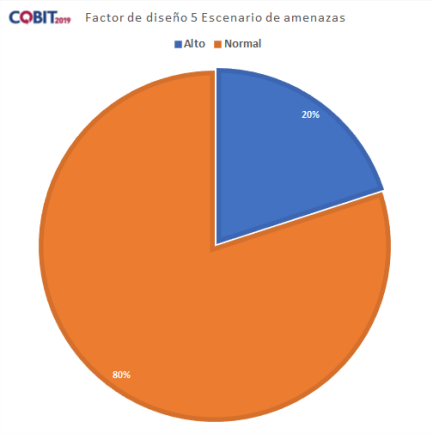
Sección de salida—Importancia relativa derivada de cada objetivo de gobierno/gestión




COBIT 2019
Paso 2 Diseño inicial
Importancia de objetivos de gobierno y gestión
-100
-80
-60
-40
-20
0
20
40
60
80
100
EDM01 10
EDM02 25
EDM03 100
-45 EDM04
-25 EDM05
APO01 15
-35 APO02
APO03 25
-30 APO04
-45 APO05
-60 APO06
APO07
APO08 50
APO09 35
-30 APO10
APO11 40
APO12 85
APO13 80
APO14 15
BAI01 15
BAI02
BAI03 5
BAI04 60
BAI05 35
BAI06 10
-20 BAI07
-40 BAI08
-70 BAI09
BAI10 5
BAI11 35
-30 DSS01
DSS02 65
DSS03 55
DSS04 60
DSS05 65
DSS06 35
MEA01 10
MEA02 15
MEA03 70
MEA04 35

Sección de entrada—Importancia del Escenario de amenazas

Valor	Importancia (100 %)	Referencia
Alto	20%	33%
Normal	80%	67%



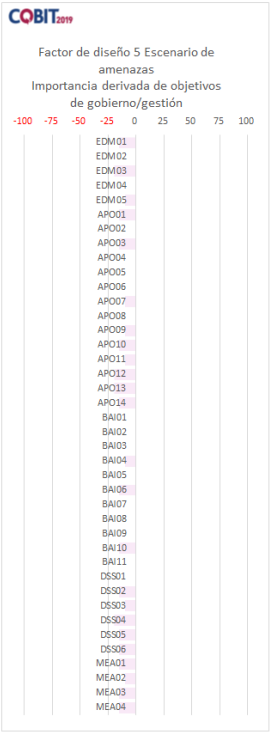
COBIT 2019 Diseño del sistema de gobierno de información y tecnología
Factor de diseño 5 Escenario de amenazas

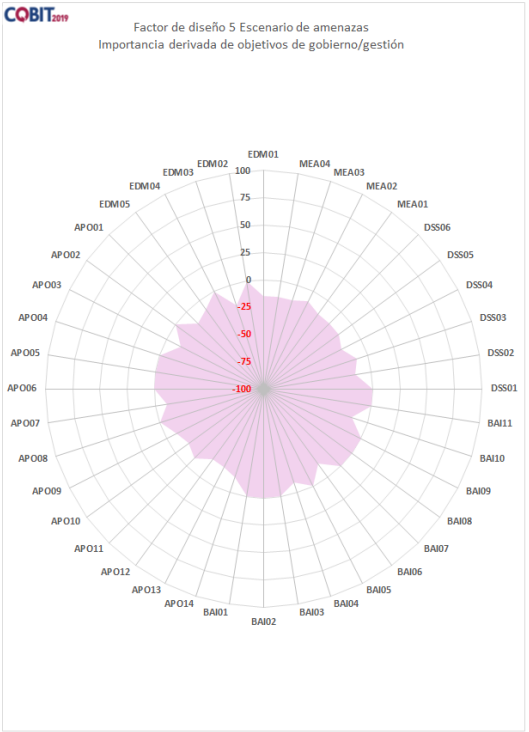
Sección de entrada—Importancia del Escenario de amenazas

Página dejada en blanco intencionadamente

Sección de salida—Importancia relativa derivada de cada objetivo de gobierno/gestión

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	Valoración	Referencia	Importancia relativa
EDM01	1,40	1,66	-15
EDM02	1,00	1,00	0
EDM03	1,60	1,99	-20
EDM04	1,00	1,00	0
EDM05	1,20	1,33	-10
APO01	1,40	1,66	-15
APO02	1,00	1,00	0
APO03	1,40	1,66	-15
APO04	1,00	1,00	0
APO05	1,00	1,00	0
APO06	1,00	1,00	0
APO07	1,20	1,33	-10
APO08	1,00	1,00	0
APO09	1,20	1,33	-10
APO10	1,40	1,66	-15
APO11	1,20	1,33	-10
APO12	1,60	1,99	-20
APO13	1,60	1,99	-20
APO14	1,40	1,66	-15
BAI01	1,00	1,00	0
BAI02	1,00	1,00	0
BAI03	1,00	1,00	0
BAI04	1,20	1,33	-10
BAI05	1,00	1,00	0
BAI06	1,40	1,66	-15
BAI07	1,00	1,00	0
BAI08	1,00	1,00	0
BAI09	1,00	1,00	0
BAI10	1,40	1,66	-15
BAI11	1,00	1,00	0
DSS01	1,00	1,00	0
DSS02	1,40	1,66	-15
DSS03	1,20	1,33	-10
DSS04	1,60	1,99	-20
DSS05	1,40	1,66	-15
DSS06	1,40	1,66	-15
MEA01	1,40	1,66	-15
MEA02	1,20	1,33	-10
MEA03	1,40	1,66	-15
MEA04	1,40	1,66	-15



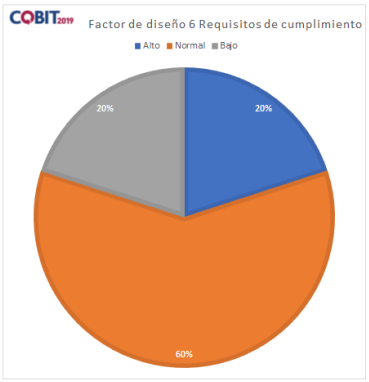


COBIT 2019 Diseño del sistema de gobierno de información y tecnología
Factor de diseño 6 Requisitos de cumplimiento

Sección de entrada—Importancia de los requisitos de cumplimiento

Sección de entrada—Importancia de los requisitos de cumplimiento

Valor	Importancia (100 %)	Referencia
Alto	20%	1
Normal	60%	100%
Bajo	20%	0%

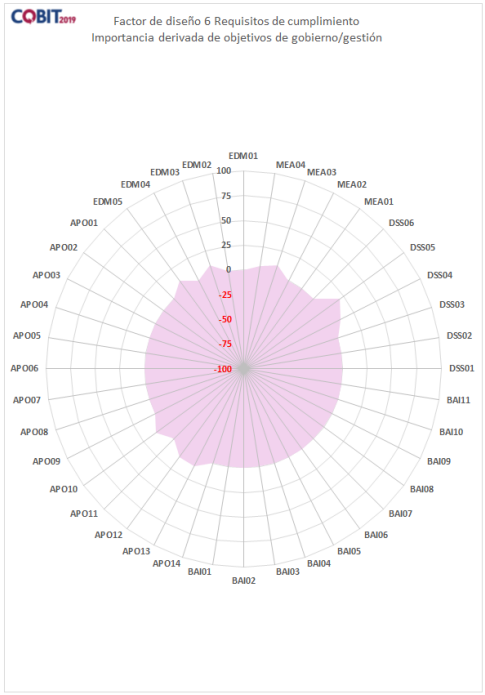


Página dejada en blanco intencionadamente

Sección de salida—Importancia relativa derivada de cada objetivo de gobierno/gestión

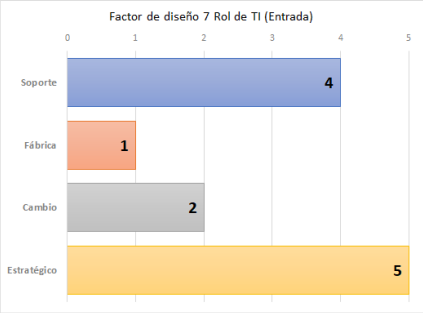
Sección de salida—Importancia relativa derivada de cada objetivo de gobierno/gestión

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	Valoración	Referencia	Importancia relativa
EDM01	2,00	2,00	0
EDM02	1,00	1,00	0
EDM03	2,20	2,00	10
EDM04	1,00	1,00	0
EDM05	1,10	1,00	10
APO01	1,50	1,50	0
APO02	1,00	1,00	0
APO03	1,00	1,00	0
APO04	1,00	1,00	0
APO05	1,00	1,00	0
APO06	1,00	1,00	0
APO07	1,00	1,00	0
APO08	1,00	1,00	0
APO09	1,00	1,00	0
APO10	1,10	1,00	10
APO11	1,00	1,00	0
APO12	2,20	2,00	10
APO13	1,10	1,00	10
APO14	1,50	1,50	0
BAI01	1,00	1,00	0
BAI02	1,00	1,00	0
BAI03	1,00	1,00	0
BAI04	1,00	1,00	0
BAI05	1,00	1,00	0
BAI06	1,00	1,00	0
BAI07	1,00	1,00	0
BAI08	1,00	1,00	0
BAI09	1,00	1,00	0
BAI10	1,00	1,00	0
BAI11	1,00	1,00	0
DSS01	1,00	1,00	0
DSS02	1,00	1,00	0
DSS03	1,00	1,00	0
DSS04	1,10	1,00	10
DSS05	1,20	1,00	20
DSS06	1,00	1,00	0
MEA01	1,00	1,00	0
MEA02	1,00	1,00	0
MEA03	2,20	2,00	10
MEA04	2,10	2,00	5



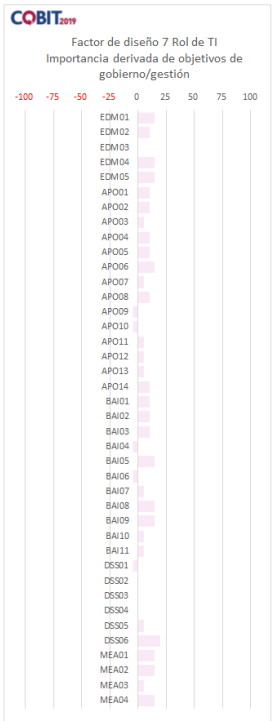
Sección de entrada—Importancia del Rol de TI

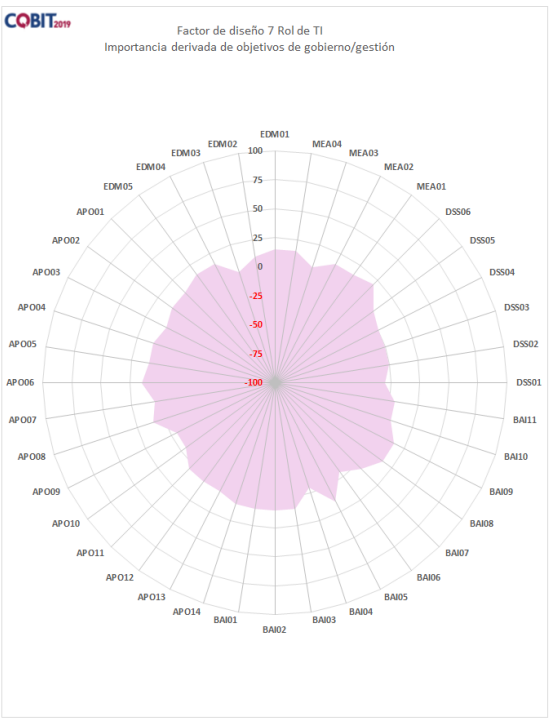
Valor	Importancia (1-5)	Referencia
Soporte	4	3
Fábrica	1	3
Cambio	2	3
Estratégico	5	3



Sección de salida—Importancia relativa derivada de cada objetivo de gobierno/gestión

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	Valoración	Referencia	Importancia relativa
EDM01	29,0	25,5	15
EDM02	25,0	22,5	10
EDM03	24,0	24,0	0
EDM04	17,0	15,0	15
EDM05	17,0	15,0	15
APO01	21,0	19,5	10
APO02	26,0	24,0	10
APO03	19,0	18,0	5
APO04	30,0	27,0	10
APO05	25,0	22,5	10
APO06	17,0	15,0	15
APO07	14,5	13,5	5
APO08	21,5	19,5	10
APO09	19,0	19,5	-5
APO10	19,5	21,0	-5
APO11	18,5	18,0	5
APO12	23,5	22,5	5
APO13	24,0	22,5	5
APO14	21,0	19,5	10
BAI01	21,5	19,5	10
BAI02	26,0	24,0	10
BAI03	26,0	24,0	10
BAI04	19,5	21,0	-5
BAI05	17,0	15,0	15
BAI06	18,5	19,5	-5
BAI07	19,0	18,0	5
BAI08	17,0	15,0	15
BAI09	17,0	15,0	15
BAI10	17,5	16,5	5
BAI11	19,0	18,0	5
DSS01	24,5	25,5	-5
DSS02	25,0	25,5	0
DSS03	27,5	27,0	0
DSS04	27,5	27,0	0
DSS05	29,0	27,0	5
DSS06	19,5	16,5	20
MEA01	17,0	15,0	15
MEA02	17,0	15,0	15
MEA03	14,5	13,5	5
MEA04	17,0	15,0	15





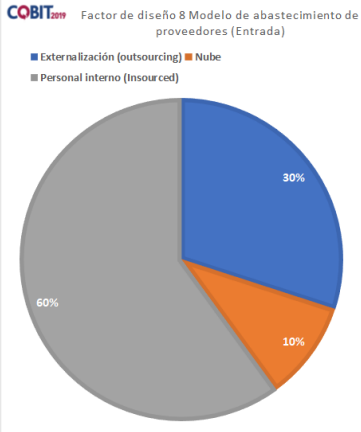
COBIT 2019 Diseño del sistema de gobierno de información y tecnología
Factor de diseño 7 Rol de TI

Sección de entrada—Importancia del Rol de TI

Página dejada en blanco intencionadamente

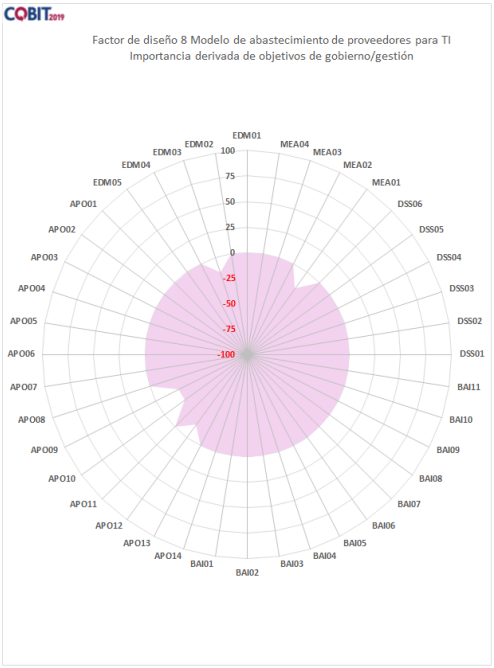
Sección de entrada—Importancia del modelo de abastecimiento de proveedores para TI

Valor	Importancia (100 %)	Referencia
Externalizació	30%	33%
Nube	10%	33%
Personal inter	60%	34%



Sección de salida—Importancia relativa derivada de cada objetivo de gobierno/gestión

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	Valoración	Referencia	Importancia relativa
EDM01	1,00	1,00	0
EDM02	1,00	1,00	0
EDM03	1,10	1,33	-15
EDM04	1,00	1,00	0
EDM05	1,00	1,00	0
APO01	1,00	1,00	0
APO02	1,00	1,00	0
APO03	1,00	1,00	0
APO04	1,00	1,00	0
APO05	1,00	1,00	0
APO06	1,00	1,00	0
APO07	1,00	1,00	0
APO08	1,00	1,00	0
APO09	2,20	2,98	-25
APO10	2,20	2,98	-25
APO11	1,00	1,00	0
APO12	1,40	1,66	-15
APO13	1,00	1,00	0
APO14	1,00	1,00	0
BAI01	1,00	1,00	0
BAI02	1,00	1,00	0
BAI03	1,00	1,00	0
BAI04	1,00	1,00	0
BAI05	1,00	1,00	0
BAI06	1,00	1,00	0
BAI07	1,00	1,00	0
BAI08	1,00	1,00	0
BAI09	1,00	1,00	0
BAI10	1,00	1,00	0
BAI11	1,00	1,00	0
DSS01	1,00	1,00	0
DSS02	1,00	1,00	0
DSS03	1,00	1,00	0
DSS04	1,00	1,00	0
DSS05	1,00	1,00	0
DSS06	1,00	1,00	0
MEA01	1,80	2,32	-20
MEA02	1,00	1,00	0
MEA03	1,00	1,00	0
MEA04	1,00	1,00	0



COBIT 2019 Diseño del sistema de gobierno de información y tecnología
ctor de diseño 8 Modelo de abastecimiento de proveedores para TI

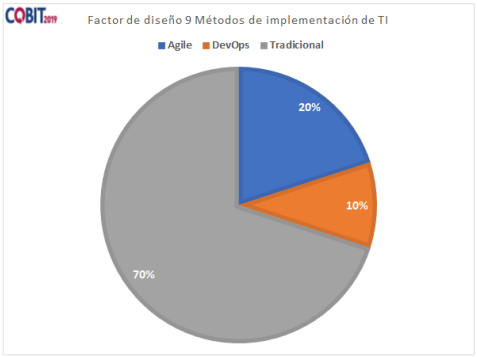
Sección de entrada—Importancia del modelo de abastecimiento de proveedores para TI

Página dejada en blanco intencionadamente

Sección de salida—Importancia relativa derivada de cada objetivo de gobierno/gestión

Sección de entrada—Importancia de los métodos de implementación de TI

Valor	Importancia (100 %)	Referencia
Agile	20%	15%
DevOps	10%	10%
Tradicional	70%	75%

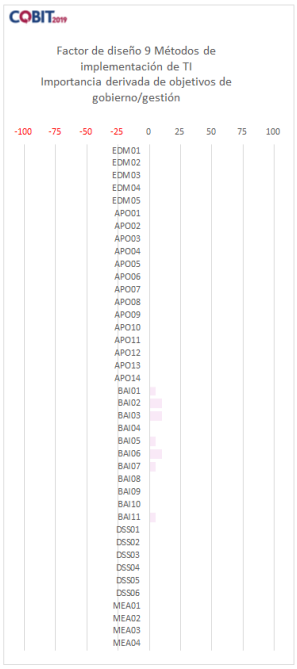


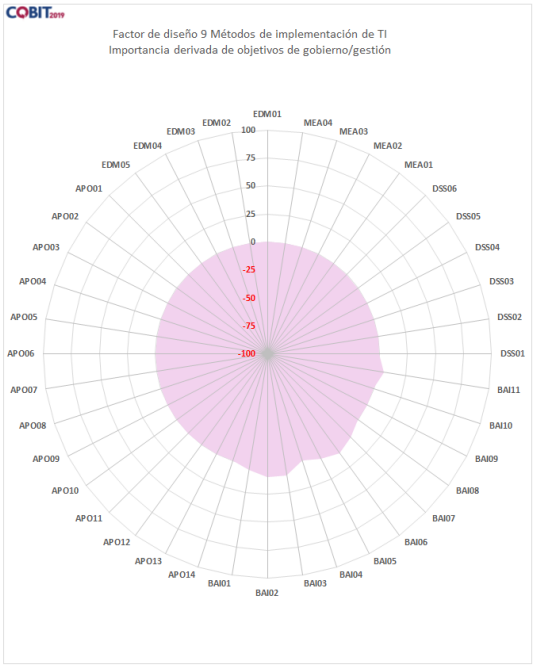
COBIT 2019 Diseño del sistema de gobierno de información y tecnología
Factor de diseño 9 Métodos de implementación de TI
Sección de entrada—Importancia de los métodos de implementación de TI

Página dejada en blanco intencionadamente

Sección de salida—Importancia relativa derivada de cada objetivo de gobierno/gestión

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/gestión	Valoración	Referencia	Importancia relativa
EDM01	1,00	1,00	0
EDM02	1,00	1,00	0
EDM03	1,00	1,00	0
EDM04	1,00	1,00	0
EDM05	1,00	1,00	0
APO01	1,00	1,00	0
APO02	1,00	1,00	0
APO03	1,10	1,10	0
APO04	1,00	1,00	0
APO05	1,00	1,00	0
APO06	1,00	1,00	0
APO07	1,05	1,05	0
APO08	1,00	1,00	0
APO09	1,00	1,00	0
APO10	1,00	1,00	0
APO11	1,00	1,00	0
APO12	1,05	1,05	0
APO13	1,00	1,00	0
APO14	1,00	1,00	0
BAI01	1,25	1,20	5
BAI02	1,60	1,48	10
BAI03	1,80	1,65	10
BAI04	1,00	1,00	0
BAI05	1,35	1,28	5
BAI06	1,60	1,48	10
BAI07	1,45	1,38	5
BAI08	1,00	1,00	0
BAI09	1,00	1,00	0
BAI10	1,20	1,18	0
BAI11	1,30	1,23	5
DSS01	1,15	1,15	0
DSS02	1,05	1,05	0
DSS03	1,05	1,05	0
DSS04	1,00	1,00	0
DSS05	1,00	1,00	0
DSS06	1,00	1,00	0
MEA01	1,15	1,13	0
MEA02	1,00	1,00	0
MEA03	1,00	1,00	0
MEA04	1,00	1,00	0



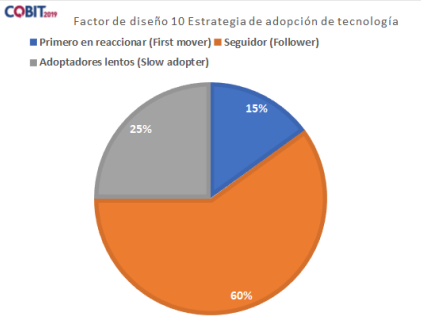


COBIT 2019 Diseño del sistema de gobierno de información y tecnología
Factor de diseño 9 Métodos de implementación de TI
Sección de salida—Importancia relativa derivada de cada objetivo de gobierno/gestión

COBIT 2019 Diseño del sistema de gobierno de información y tecnología
Factor de diseño 10 Estrategia de adopción de tecnología

Sección de entrada—Importancia de la estrategia de adopción de tecnología

Valor	Importancia (100 %)	Referencia
Primero en rea	15%	15%
Seguidor (Follc	60%	70%
Adoptadores le	25%	15%

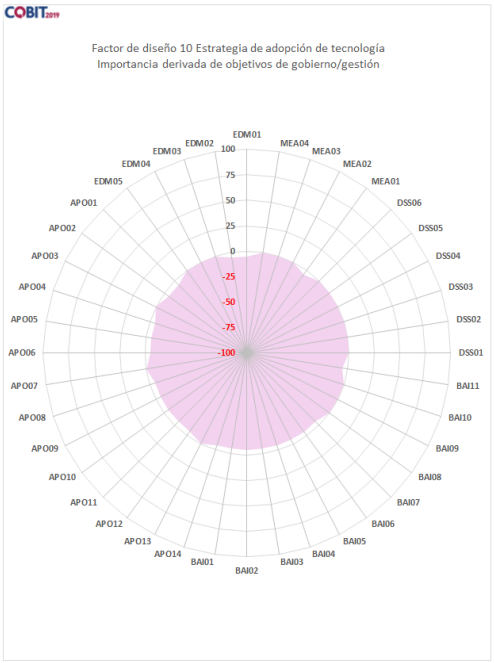


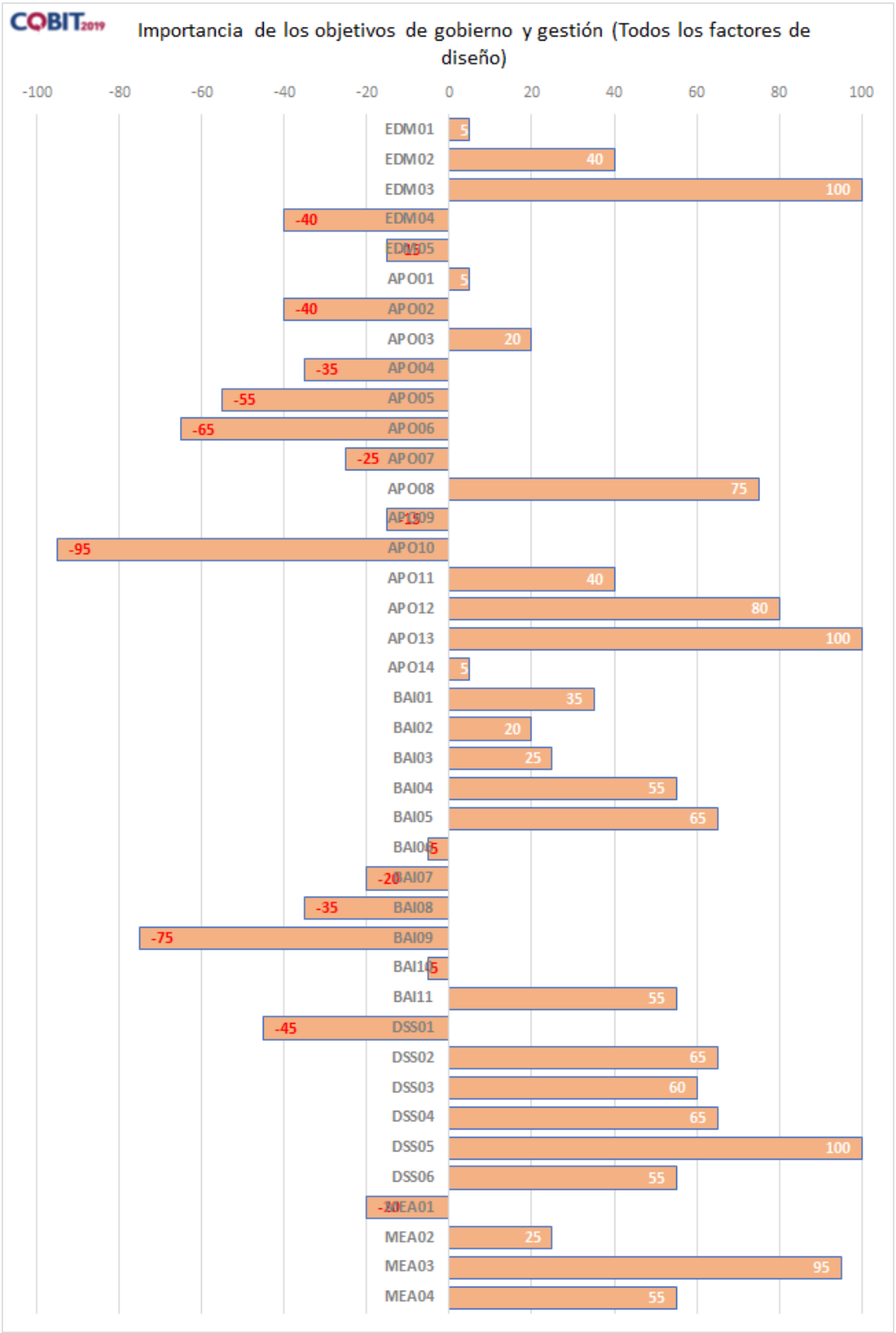
Sección de entrada—Importancia de la estrategia de adopción de tecnología

Página dejada en blanco intencionadamente

Sección de salida—Importancia relativa derivada de cada objetivo de gobierno/gestión

Importancia derivada de objetivos de gobierno/gestión			
Objetivo de gobierno/ gestión	Valoración	Referencia	Importancia relativa
EDM01	2,40	2,50	-5
EDM02	2,48	2,58	-5
EDM03	1,08	1,08	0
EDM04	1,95	2,00	0
EDM05	1,08	1,08	0
APO01	1,53	1,58	-5
APO02	2,78	2,93	-5
APO03	1,15	1,15	0
APO04	2,65	2,85	-5
APO05	2,35	2,50	-5
APO06	1,30	1,35	-5
APO07	1,23	1,23	0
APO08	1,60	1,65	-5
APO09	1,38	1,43	-5
APO10	1,53	1,58	-5
APO11	1,38	1,43	-5
APO12	1,45	1,50	-5
APO13	1,00	1,00	0
APO14	1,83	1,93	-5
BAI01	2,78	2,93	-5
BAI02	2,28	2,43	-5
BAI03	2,35	2,50	-5
BAI04	1,38	1,43	-5
BAI05	1,90	2,00	-5
BAI06	1,83	1,93	-5
BAI07	2,28	2,43	-5
BAI08	1,08	1,08	0
BAI09	1,00	1,00	0
BAI10	1,08	1,08	0
BAI11	2,28	2,43	-5
DSS01	1,00	1,00	0
DSS02	1,00	1,00	0
DSS03	1,08	1,08	0
DSS04	1,08	1,08	0
DSS05	1,08	1,08	0
DSS06	1,00	1,00	0
MEA01	1,90	2,00	-5
MEA02	1,00	1,00	0
MEA03	1,00	1,00	0
MEA04	1,00	1,00	0




COBIT 2019
Importancia de los objetivos de gobierno y gestión (Todos los factores de diseño)
-100
-80
-60
-40
-20
0
20
40
60
80
100
EDM01 5
EDM02 40
EDM03 100
-40 EDM04
EDM05 15
APO01 5
-40 APO02
APO03 20
-35 APO04
-55 APO05
-65 APO06
-25 APO07
APO08 75
APO09 15
-95 APO10
APO11 40
APO12 80
APO13 100
APO14 5
BAI01 35
BAI02 20
BAI03 25
BAI04 55
BAI05 65
BAI06 5
-20 BAI07
-35 BAI08
-75 BAI09
BAI10 5
BAI11 55
-45 DSS01
DSS02 65
DSS03 60
DSS04 65
DSS05 100
DSS06 55
-20 MEA01
MEA02 25
MEA03 95
MEA04 55