

**DESARROLLO DEL MODELO DE INTEGRACIÓN DE LAS NORMAS ISO/IEC
27001:2013, ISO/IEC 27002:2013 Y COBIT V5 FOR INFORMATION SECURITY
PARA LA DEFINICIÓN, DISEÑO Y MODELAMIENTO DE LAS POLÍTICAS DE
SEGURIDAD APLICADO AL DATACENTER DE SONDA COLOMBIA.**

**MARIO ANDRÉS ALBA GARCÍA
JOHN ALEXANDER BELTRÁN BLANCO
MAURICIO ESGUERRA ELIANEGUA**

**UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2014**

**DESARROLLO DEL MODELO DE INTEGRACIÓN DE LAS NORMAS ISO/IEC
27001:2013, ISO/IEC 27002:2013 Y COBIT V5 FOR INFORMATION SECURITY
PARA LA DEFINICIÓN, DISEÑO Y MODELAMIENTO DE LAS POLÍTICAS DE
SEGURIDAD APLICADO AL DATACENTER DE SONDA COLOMBIA.**

**MARIO ANDRÉS ALBA GARCÍA
MAURICIO ESGUERRA ELIANEGUA
JOHN ALEXANDER BELTRÁN BLANCO**

**Trabajo de grado para optar al título de
Especialista en Seguridad Informática**

**Tutor
CARLOS VILLAMIZAR
Ingeniero en Seguridad Informática**

**UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2014**

Nota de Aceptación:

Firma del Director de la Especialización

Firma del Jurado

Firma del Jurado

Bogotá, D.C., Octubre 08 de 2014

CONTENIDO

	pág.
INTRODUCCIÓN	14
1. PROBLEMA	15
1.1 PLANTEAMIENTO DEL PROBLEMA	15
1.1.1 Definición del problema	15
1.1.2 Formulación del problema	15
1.2 JUSTIFICACIÓN	15
1.3 OBJETIVOS	16
1.3.1 Objetivo general	16
1.3.2 Objetivos específicos	17
1.4 ALCANCE	17
2. MARCO TEÓRICO	18
2.1 ANTECEDENTES	18
2.2 TÉRMINOS / CONCEPTOS	18
2.2.1 Normas ISO	18
2.2.1.1 ISO/IEC 27001:2013	18
2.2.1.2 ISO/IEC 27002:2013	26
2.2.2 COBIT	27
2.2.2.1 Definición	27
2.2.2.2 Metodología	27
2.3 HIPÓTESIS	34
3. DISEÑO METODOLÓGICO	35
3.1 TIPO DE INVESTIGACIÓN	35
3.2 UNIVERSO Y MUESTRA	35
3.2.1 Universo	35
3.2.2 Muestra	35

4. VIABILIDAD	36
4.1 RECURSOS	36
4.1.1 Humanos	36
4.1.2 Físicos	36
4.1.3 Técnicos	36
4.2 PRESUPUESTO	37
4.3 CRONOGRAMA	39
5. DISEÑO DEL PROYECTO	41
5.1 PRINCIPIOS DE COBIT 5 PARA SEGURIDAD DE LA INFORMACIÓN	41
5.1.1 Principio 1: Satisfacer las necesidades de las partes interesadas	41
5.1.2. Principio 2: Cubrir la empresa de Extremo a Extremo	42
5.1.3 Principio 3: Aplicar un marco de referencia Único Integrado	42
5.1.4 Principio 4: Hacer posible un Enfoque Holístico	42
5.1.5 Principio 5: Separar el Gobierno de la Gestión.	43
5.2 CATALIZADORES	43
5.2.1 Políticas, principios y marcos de referencia de seguridad de la información	44
5.2.1.1 Principios de la seguridad de la información	45
5.2.1.2 Política general de la seguridad de la información	47
5.2.1.3 Políticas específicas de la seguridad de la información dirigidas por función de la seguridad de la información	47
5.2.1.4 Políticas específicas de la seguridad de la información dirigidas por otras áreas dentro de la empresa	52
5.2.1.5 Ciclo de vida de las Políticas de Seguridad	55
5.2.2 Procesos	55
5.2.2.1 Evaluar, Orientar y Supervisar (EDM)	56
5.2.2.2 Alinear, Planificar y Organizar (APO)	69
5.2.2.3 Construir, Adquirir e Implementar (BAI)	117
5.2.2.4 Entrega, Servicio y Soporte (DSS)	160
5.2.2.5 Supervisar, Evaluar y Valorar (MEA)	187
5.2.3 Estructuras organizativas	200

5.2.3.1 Gerencia de Seguridad de la Información	200
5.2.3.2. Comité de Dirección de Seguridad de la Información	202
5.2.3.3 Comité de Gestión de Riesgo Empresarial	206
6. RESULTADOS	209
7. APORTES	210
8. CONCLUSIONES	211
9. RECOMENDACIONES	212
10. IMPLICACIONES	213
BIBLIOGRAFÍA	214

LISTA DE FIGURAS

	pág.
Figura 1. Principios de COBIT	41
Figura 2. Metas de COBIT	42
Figura 3. Modelo sistemático de Interactuación de Catalizadores COBIT	43
Figura 4. Catalizadores genéricos COBIT 5	45
Figura 5. Principios de COBIT	47
Figura 6. Procesos de COBIT	56

LISTA DE CUADROS

	pág.
Cuadro 1. Comparación de contenidos norma ISO 27001 versiones 2005 y 201	19
Cuadro 2. Documentación requerida para la implementación de la norma ISO 27001:2013.	23
Cuadro 3. Documentación de uso frecuente para la implementación de la norma ISO 27001:2013.	24
Cuadro 4. Nueva estructura y controles de la Norma ISO 27001:2013.	25
Cuadro 5. Comparación de contenido norma ISO 27002 versiones 2005 y 2013	26
Cuadro 6. Procesos o Facilitadores COBIT 5	29
Cuadro 7. Principios de la Seguridad Informática	32
Cuadro 8. Recursos de la Infraestructura tecnológica.	33
Cuadro 9. EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	56
Cuadro 10. EDM02 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad	59
Cuadro 11. EDM03 Asegurar la Optimización del Riesgo	62
Cuadro 12. EDM04 Asegurar la Optimización de Recursos	64
Cuadro 13. EDM05 asegurar la transparencia hacia las partes interesadas	66
Cuadro 14. APO01 Gestionar el Marco de Gestión de TI	69
Cuadro 15. APO02 Gestionar la Estrategia	74
Cuadro 16. APO03 Gestionar la Arquitectura Empresarial	78
Cuadro 17. APO04 Gestionar la Innovación	83
Cuadro 18. APO05 Gestionar el Portafolio	87
Cuadro 19. APO06 Gestionar el Presupuesto y los Costes	91
Cuadro 20. APO07 Gestionar los Recursos Humanos	95
Cuadro 21. APO08 Gestionar las Relaciones	95
Cuadro 22. APO09 Gestionar los Acuerdos de Servicio.	98
Cuadro 23. APO10 Gestionar los Proveedores	101
Cuadro 24. APO11 Gestionar la Calidad	104

Cuadro 25. APO12 Gestionar el Riesgo	109
Cuadro 26. APO13 Gestionar de la Seguridad	113
Cuadro 27. BAI01 Gestionar Programas y Proyectos	117
Cuadro 28. BAI02 Gestionar la Definición de Requisitos	127
Cuadro 29. BAI03 Gestionar la Identificación y Construcción de Soluciones	130
Cuadro 30. BAI04 Gestionar la Disponibilidad y la Capacidad	135
Cuadro 31. BAI05 Gestionar la Introducción del Cambio Organizativo	139
Cuadro 32. BAI06 Gestionar los Cambios	144
Cuadro 33. BAI07 Gestionar la Aceptación del Cambio y la Transición	146
Cuadro 34. BAI08 Gestionar el Conocimiento	152
Cuadro 35. BAI09 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso	155
Cuadro 36. BAI10 Gestionar la Configuración	157
Cuadro 37. DSS01 Gestionar Operaciones	160
Cuadro 38. DSS02 Gestionar Peticiones e Incidentes de Servicio.	164
Cuadro 39. DSS03 Gestionar Problemas	168
Cuadro 40. DSS04 Gestionar la Continuidad	171
Cuadro 41. DSS05 Gestionar Servicios de Seguridad	175
Cuadro 42. DSS06 Gestionar Controles de Proceso de Negocio	182
Cuadro 43. MEA01 Supervisar, evaluar y valorar el rendimiento y la conformidad	187
Cuadro 44. MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno	190
Cuadro 45. MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	197
Cuadro 46. Gerencia de la Seguridad de la Información	200
Cuadro 47. Matriz RACI a Alto Nivel con Prácticas Clave	201
Cuadro 48. Entradas y Salidas COBIT	202
Cuadro 49. Comité de Dirección de Seguridad de la Información	202
Cuadro 50. Mandato, Principios Operativos, Ámbito de Control y Nivel de Autoridad	203
Cuadro 51. ISSC: Matriz RACI a Alto Nivel	205

Cuadro 52. ISSC: Entradas y Salidas	206
Cuadro 53. Comité de Gestión de Riesgo Empresarial (ERM)	207
Cuadro 54. Comité de ERM: Matriz RACI de Alto Nivel	207
Cuadro 55. Custodios de la Información/Propietarios de Negocio: Matriz RACI de Alto Nivel	208

LISTA DE TABLAS

	pág
Tabla 1. Diseño del Proyecto	37
Tabla 2. Desarrollo del Proyecto	37
Tabla 3. Entrega del Proyecto	38
Tabla 4. Administración del Proyecto	38
Tabla 5. Presupuesto Total	38
Tabla 6. Cronograma	39

RESUMEN

El siguiente documento es una presentación del planteamiento para definir un modelo de seguridad óptimo para el Datacenter de Sonda Colombia, el cual integrara las buenas prácticas de gestión de seguridad de la información establecidas en ISO/IEC 27001:2013 y ISO/IEC 27002:2013, y las de gobernabilidad ofrecidas por COBIT 5 FOR INFORMATION SECURITY.

Sonda de Colombia tiene como objetivo ofrecer servicios de TI a varios tipos de clientes, los cuales preocupados por la seguridad de la información consignada en su infraestructura exigen modelos para garantizar la seguridad de esta.

ISO/IEC 27001:2013 y ISO/IEC 27002:2013 regirán los tipos de controles que se deben implementar para garantizar que los riesgos existentes puedan ser manejados, controlados y mitigados apropiadamente.

COBIT 5 FOR INFORMATION SECURITY con su amplia gama de procesos garantizara la gobernabilidad de todos los aspectos del modelo de seguridad

ABSTRACT

The following document presents the approach to define an optimal security model for the datacenter owned by the company Sonda Colombia, which integrates the best practices of management in ISO / IEC 27001:2013 and ISO / IEC 27002:2013, and governance offered by COBIT 5 FOR INFORMATION SECURITY.

This company aims to provide IT services to various types of clients, who are worried about the security of the information in its infrastructure, requiring models to ensure the safety of this.

ISO / IEC 27001:2013 and ISO / IEC 27002:2013 guarantee all types of controls that should be implemented to ensure that the risks could be managed, controlled and mitigated.

COBIT 5 FOR INFORMATION SECURITY with its wide range of governance processes ensure all aspects of the security model, helping to continuously improve them and defining all monitoring protocols.

INTRODUCCIÓN

El presente proyecto constituye una propuesta para trabajo de grado de la Especialización en Seguridad Informática de la universidad Piloto de Colombia. Esta se enmarca en el área de la gestión de seguridad y el riesgo y pretende el desarrollo de un modelo de seguridad que integre las normas ISO/IEC 27001:2013, ISO/IEC 27002:2013 y COBIT V5 FOR INFORMATION SECURITY para el *Datacenter* de servicios de la empresa Sonda Colombia.

La elaboración de modelos de Seguridad que integran varios estándares, se ha convertido en una práctica cada vez más común en las empresas Colombianas. La iniciativa del proyecto surge de la necesidad que tiene Sonda Colombia en ser una compañía competitiva en el mercado y de mejorar su imagen ante sus clientes, así como de generar un modelo de Seguridad que permita obtener los beneficios de incluir tres normas en un mismo modelo de seguridad y brinde un diseño acoplado a las necesidades de la empresa.

La propuesta presenta inicialmente el planteamiento del proyecto, delimitándolo a la presentación final de un Diseño del modelo basado en las necesidades de Sonda, exponiendo las ventajas de aplicar las Normas ISO/IEC 27001:2013, ISO/IEC 27002:2013, así como las diferencias con sus revisiones anteriores y los fundamentos del estándar COBIT 5 FOR INFORMATION SECURITY. Finalmente presenta la viabilidad de ejecutar el proyecto a través de la presentación de un cronograma de actividades, recursos y presupuesto.

1. PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

1.1.1 Definición del problema. Sonda Colombia es una compañía prestadora de servicios de Hosting, Colocation y está lanzando su producto Cloud Computing para diferentes empresas del sector público y privado. Esta tomó la decisión de implementar su propio Datacenter en lugar de contratar este servicio con un tercero.

Actualmente la compañía tiene normas y/o controles que no cumplen en gran medida los requerimientos que garanticen a sus clientes políticas adecuadas para la administración de la información.

Algunos de sus clientes deben presentar informes anuales de cómo administran y controlan sus proveedores de tecnología, encontrando que en su calificación su proveedor Sonda Colombia no cumple con los requerimientos mínimos en seguridad de la información.

Sonda Colombia requiere un modelo de seguridad de la información que permita devolver la confianza a sus clientes principales, así como la formulación de políticas de seguridad que permitan la adecuada administración, prevención y atención de incidentes del Datacenter.

También se pretende tener un modelo único para la organización en su división de servicios que permita abarcar cualquier necesidad crítica de sus clientes en busca de ser integral en cualquier frente de servicio que se pueda presentar.

1.1.2 Formulación del problema. ¿Qué beneficios traería para Sonda Colombia el desarrollo de un modelo de seguridad basado en la integración de las normas ISO/IEC 27001:2013, ISO/IEC 27002:2013 Y de las buenas prácticas ofrecidas por COBIT 5 FOR INFORMATION SECURITY para su Datacenter?

1.2 JUSTIFICACIÓN

La ISO 27001 es un Estándar Internacional de Sistemas de Gestión de Seguridad de la Información que permite a una organización evaluar su riesgo e implementar controles apropiados para preservar la confidencialidad, la integridad y la disponibilidad del valor de la información.

De acuerdo a los lineamientos corporativos con la casa matriz, la norma NTC/ISO 27001 cumple con los objetivos que la organización se ha planteado para prestación de servicios de TI y administración de la información a lo largo de toda

su trayectoria desde 1980.

Con la integración de estos estándares se busca obtener un mayor alcance, haciendo que Sonda sea una compañía competitiva en el mercado y mejorando su imagen ante sus clientes.

La implementación de este modelo, representará para Sonda Colombia:

- Mejora del conocimiento de los sistemas de información, atención a incidentes y los medios de protección.
- Mejora de la disponibilidad de los materiales y datos.
- Protección de la información.
- Diferenciación sobre la competencia y mercado.
- Robustez en la implementación de procesos de seguridad
- Confiabilidad en los clientes con la aplicación de procesos

Igualmente, la implementación de modelos de gestión por procesos como COBIT, permite definir un modelo de gestión de procesos idóneo para el área de TI. Los componentes de este framework ayudan a definir las mejores prácticas para el modelamiento de procesos, planes de auditoría y demás.

Paralelamente, COBIT con su amplio marco de referencia ayudará a:

- Optimizar los servicios, el coste de las TI y de la tecnología.
- Apoyar el cumplimiento de leyes, reglamentos, acuerdos contractuales y políticas de los modelos de seguridad definidos.
- Gestión de nuevas tecnologías de la información de acuerdo a los requisitos de seguridad.
- Unificar el lenguaje corporativo y que se encuentra encaminado en una sola dirección.

1.3 OBJETIVOS

1.3.1 Objetivo general. Desarrollar un modelo de integración de las normas ISO/IEC 27001:2013, ISO/IEC 27002:2013 y COBIT 5 FOR INFORMATION SECURITY para la definición, diseño y modelamiento de las políticas de seguridad aplicadas al Datacenter de Sonda Colombia.

1.3.2 Objetivos específicos

- Identificar los incidentes que han ocurrido en el Datacenter así como el tratamiento que se le ha dado a los mismos.
- Analizar los procesos actuales que se llevan a cabo en la Administración de la información que se maneja en el Datacenter.
- Definir las políticas y métricas del modelo de seguridad para el Datacenter de Sonda Colombia.
- Establecer un modelo y políticas de seguridad que pueda ser aplicable al proceso de certificación ISO/IEC 27001.

1.4 ALCANCE

El proyecto se enmarca en el área de la administración de seguridad y la gestión del riesgo, pretende el desarrollo de un modelo de seguridad que integre las normas ISO/IEC 27001:2013, ISO/IEC 27002:2013 y COBIT 5 FOR INFORMATION SECURITY para el Datacenter de servicios de la empresa Sonda Colombia.

Desde hace más de 37 años Sonda Colombia provee servicios de Data Center a cientos de clientes en Latinoamérica, entre los que destacan empresas mineras, financieras y organizaciones gubernamentales.

Sonda cuenta con más 3.000 m² de salas de equipos, administrando más de 5.000 servidores físicos y más de 500 TB de capacidad de almacenamiento, lo que se suma a las certificaciones de seguridad ISO/IEC 27001, Datacenter certificados Tier III en Santiago (diseño por Uptime Institute) y Sao Paulo (diseño y operación por TÜV Rheinland), SAP Partner Hosting, Cisco Managed Service, entre otras.

Además, Sonda cuenta con un equipo de consultores y profesionales certificados en las principales tecnologías de servidores, almacenamiento, sistemas operativos, bases de datos, monitoreo y seguridad (VMware, Microsoft, SAP, CISCO, HP, IBM, Oracle, Red Hat), que permiten garantizar que la operación de sus centros de datos esté alineada con los niveles de servicios adecuados.

2. MARCO TEÓRICO

2.1 ANTECEDENTES

En el año 1992 se publica un documento llamado “*Code of Practice for Information Security Management*” por el gobierno británico con el objetivo de desarrollar, implementar y medir la efectividad de las prácticas de gestión de la seguridad. En el año 1995 este documento fue publicado por el the British Standards Institute (BSI) como BS7799.

En el año 1996 ISACA lanza la primera versión de Cobit, un grupo de objetivos de control para aplicaciones de negocios.¹

En el año 1999 se publica la primera revisión del código BS7799, incluyendo muchas mejoras. En este mismo año es lanzada la tercera versión de Cobit.

En el año 2000 se república el BS7799 como el estándar ISO ISO/IEC 17799.

En el año 2002 se publica una segunda parte del estándar como BS7799-2, el cual se encuentra alineado con normas como la ISO 9000.²

En el año 2005 se publica una nueva versión de la norma ISO 17799, con dos nuevas secciones y se publica la norma 27001 en reemplazo de la norma BS7799-2.

En el año 2012 se lanza Cobit versión 5.

En el año 2013 se lanza una nueva revisión de la norma ISO 27001, basada en la experiencia obtenida con la implementación de la norma del 2005. De igual forma se lanza una nueva revisión de la norma ISO 27002.

2.2 TÉRMINOS / CONCEPTOS

2.2.1 Normas ISO

2.2.1.1 ISO/IEC 27001:2013. La norma ISO 27001:2005 está basada en un enfoque por procesos y busca brindar un modelo de gestión influenciado por los requerimientos y necesidades de la organización. Para ello utiliza un enfoque basado en procesos que permite la aplicación del modelo PHVA (Planificar, Hacer,

¹ COBIT USER GROUP. Historia del Cobit. [en línea], [consultado el 2 de agosto de 2014]. Disponible en: <http://www.pc-history.org/cob.htm>

² Ibíd.

Verificar, Actuar) para establecer, implementar, operar, seguir, revisar y mejorar el Sistema de gestión de la Seguridad Informática, esta facilita la integración con otros estándares como la ISO 14001:2004.³

La nueva versión de la ISO 27001 está basada en la experiencia obtenida con el uso del estándar ISO 27001:2005, además facilita la integración con otras normas ISO gracias a sus nuevas directivas y se encuentra alineada con la norma ISO 31000 para gestión de riesgos. Por otro lado, se elimina la sección referente al proceso de PHVA y se permite a la organización elegir otro modelo de mejora continua. Dado que la norma está basada en la experiencia obtenida de la norma anterior, es posible mapear el contenido de la norma del 2013 en la norma del 2005.⁴...(Véase Cuadro 1)

Cuadro 1. Comparación de contenidos norma ISO 27001 versiones 2005 y 2013⁵

ISO/IEC 27001:2005	ISO/IEC 27001:2013
0 Introducción	0 Introducción.
1 Alcance.	1 Alcance.
2 Referencias Normativas.	2 Referencias Normativas.
3 Términos y Definiciones.	3 Términos y Definiciones.
4.1 Comprender la organización y su contexto.	8.3 Acción Preventiva.
4.2 Comprender las necesidades y expectativas de las partes interesadas.	5.2.1(c) Identificar y tratar los requerimientos legales y reguladores y las obligaciones de seguridad contractuales.

³ ESTÁNDAR. ISO/IEC. INTERNACIONAL. 17799. Tecnología de información Beta. [en línea], [consultado el 2 de agosto de 2014]. Disponible en: <http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf>

⁴ BSIGROUP. ISO 27001: Código de conducta para los controles de gestión de seguridad de la información. [en línea], [consultado el 2 de agosto de 2014]. Disponible en: <http://www.bsigroup.com/en-GB/iso-27001-information-security/ISOIEC-27001-Revision/>

⁵ Ibíd.

4.3 Determinación del alcance del sistema de gestión de seguridad de la información.	4.2.1 a) Definir el alcance y los límites del SGSI. 4.2.3 f) Realizar una revisión gerencial del SGSI sobre una base regular para asegurar que el alcance permanezca adecuado y se identifiquen las mejoras en el proceso SGSI.
--	--

Cuadro 1. Comparación de contenidos norma ISO 27001 versiones 2005 y 2013. (Continuación)

ISO/IEC 27001:2005	ISO/IEC 27001:2013
4.4. Información del sistema de gestión de seguridad.	4.1 Requerimientos Generales.
5.1 Liderazgo y compromiso.	5.1 Compromiso de la Gerencia.
5.2 Política.	4.2.1 b) Definir una política SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología
5.3 Roles de la organización, responsabilidades y autoridades.	5.1 c) Establecer roles y responsabilidades para la seguridad de información
6.1.1 Acciones para abordar los riesgos y oportunidades.	8.3 Acción preventiva.
6.1.2 Evaluación de riesgos de seguridad de información.	4.2.1 c) Definir el enfoque de valuación del riesgo de la organización. 4.2.1 d) Identificar los riesgos. 4.2.1 e) Analizar y evaluar el riesgo.
6.1.3 Tratamiento de riesgos de seguridad de información.	4.2.1 f) Identificar y evaluar las opciones Para el tratamiento de los riesgos. 4.2.1 g) Seleccionar objetivos de control y controles para el tratamiento de riesgos.
6.1.3 Tratamiento de riesgos de seguridad de información.	4.2.1 j) Preparar un Enunciado de Aplicabilidad. 4.2.2 a) Formular un plan de tratamiento de riesgo.
6.2 Objetivos de seguridad de información y planificación.	5.1 b) Asegurar que se establezcan objetivos y planes SGSI.
7.1 Recursos.	4.2.2 g) Manejar recursos para el SGS. 5.2.1 Provisión de recursos.

7.2 Competencia	5.2.2 Capacitación, conocimiento y capacidad.
7.3 Conciencia.	4.2.2 e) Implementar los programas de capacitación y conocimiento. 5.2.2 Capacitación, conocimiento y capacidad.

Cuadro 1. Comparación de contenidos norma ISO 27001 versiones 2005 y 2013 (Continuación)

ISO/IEC 27001:2005	ISO/IEC 27001:2013
7.4 Comunicación.	4.2.4 c) Comunicar los resultados y acciones a todas las partes interesadas. 5.1 d) Comunicar a la organización la importancia de lograr los objetivos de seguridad de la información y cumplir la política de seguridad de la información.
7.5 Información documentada.	4.3 Requerimientos de documentación.
8.1 Planificación y control operacional.	4.2.2 f) Manejar las operaciones del SGSI.
8.2 Evaluación de riesgos de la seguridad de la información.	4.2.3 d) Revisar las evaluaciones del riesgo a intervalos planeados.
8.3 Tratamiento de riesgos de la seguridad de la información.	4.2.2 b) Implementar el plan de tratamiento de riesgo para poder lograr los objetivos de control identificados 4.2.2 c) Implementar los controles seleccionados en 4.2.1 (g) para satisfacer los objetivos de control.
9.1 Seguimiento, medición, análisis y evaluación.	4.2.2 d) Definir cómo medir la efectividad de los controles o grupos de controles seleccionados. 4.2.3 b) Realizar revisiones regulares de la efectividad del SGSI. 4.2.3 c) Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.
9.2 Auditoría interna	4.2.3 e) Realizar auditorías SGSI internas a intervalos planeados.

9.3 Revisión Gerencial.	4.2.3 f) Realizar una revisión gerencial del SGSI sobre una base regular para asegurar que el alcance permanezca adecuado. 7 Revisión Gerencial del SGSI.
-------------------------	--

Cuadro 1. Comparación de contenidos norma ISO 27001 versiones 2005 y 2013 (Continuación)

ISO/IEC 27001:2005	ISO/IEC 27001:2013
10.1 No conformidad y acciones correctivas.	4.2.4 Mantener y mejorar el SGSI. 8.2 Acción correctiva.
10.2 Mejoramiento continuo	4.2.4 Mantener y mejorar el SGSI. 8.1 Mejoramiento continuo.
Fuente BSI-ISO27001-mapping-guide-UK-EN.Mapping of ISO/IEC 27001:2013 to ISO/IEC 27001:2005.	

El proceso de implementación de la norma está dividido en cuatro etapas que son el Planear, Implementar, Revisar y Mejorar. Dentro de la etapa de planeación se encuentra la definición de la política y objetivos de la empresa, evaluación y tratamiento de riesgos, reporte de la evaluación de riesgos y declaración de aplicabilidad. De igual forma, se debe definir el alcance, los objetivos requeridos para la implementación del estándar, definir los responsables de la seguridad, adicional a ello se debe contar con el compromiso por parte de la alta dirección.

En la etapa de implementación se debe formular el plan para el tratamiento de riesgos, implementar los controles y fomentar los programas de formación y concienciación en seguridad de la información.

En la etapa de revisión se debe realizar el monitoreo y la revisión de los procedimientos, se mide la efectividad de los controles, se realizan las auditorías internas y la aprobación de los riesgos residuales.

En la etapa de mejoramiento se definen las acciones correctivas y preventivas.

Aunque no hay muchos cambios en la norma, se han agregado nuevas definiciones, términos, se han integrado y añadido algunos controles así como la

adición y omisión de algunos documentos requeridos. Para realizar la revisión de la norma ISO 27001:2013 se requiere la elaboración de los siguientes documentos, estos son obligatorios para la implementación de la misma.⁶...(Véase Cuadro 2)

Cuadro 2. Documentación requerida para la implementación de la norma ISO 27001:2013.

Documentos	Capítulo de ISO 27001:2013
Alcance del SGSI	4.3
Políticas y objetivos de seguridad de la información	5.2, 6.2
Metodología de evaluación y tratamiento de riesgos	6.1.2
Declaración de aplicabilidad	6.1.3 d)
Plan de tratamiento del riesgo	6.1.3 e), 6.2
Informe de evaluación de riesgos	8.2
Definición de funciones y responsabilidades de seguridad	A.7.1.2, A.13.2.4
Inventario de activos	A.8.1.1
Uso aceptable de los activos	A.8.1.3
Política de control de acceso	A.9.1.1
Procedimientos operativos para gestión de TI	A.12.1.1
Principios de ingeniería para sistema seguro	A.14.2.5
Política de seguridad para proveedores	A.15.1.1
Procedimiento para gestión de incidentes	A.16.1.5

⁶ STANDARD.COM. Iso 2700. Informe de ISO 27001: Lista de documentación obligatoria requerida por ISO 27001 (Revisión 2013) (PDF). [en línea], [consultado el 2 de agosto de 2014]. Disponible en: http://www.iso27001standard.com/downloads/Checklist_of_Mandatory_Documentation_Required_by_ISO_27001_2013.pdf

Documentos	Capítulo de ISO 27001:2013
Procedimientos de la continuidad del negocio	A.17.1.2
Requisitos legales, normativos y contractuales	A.18.1.1
Fuente Checklist of Mandatory Documentation Required by ISO/IEC 27001 (2013 Revision). Which documents and records are required?	

Adicionalmente, existen documentos de uso frecuente como los mostrados a continuación.

Cuadro 3. Documentación de uso frecuente para la implementación de la norma ISO 27001:2013.

Documentos	Capítulo de ISO 27001:2013
Procedimiento para control de documentos	7.5
Controles para gestión de registros	7.5
Procedimiento para auditoría interna	9.2
Procedimiento para medidas correctivas	10.1
Política Trae tu propio dispositivo (BYOD)	A.6.2.1
Política sobre dispositivos móviles y tele-trabajo	A.6.2.1
Política de clasificación de la información	A.8.2.1, A.8.2.2, A.8.2.3
Política de claves	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
Política de eliminación y destrucción	A.8.3.2, A.11.2.7
Procedimiento para trabajo en áreas seguras	A.11.1.5
Política de pantalla y escritorio limpio	A.11.2.9
Política de gestión de cambio	A.12.1.2, A.14.2.4
Política de creación de copias de seguridad	A.12.3.1
Política de transferencia de la información	A.13.2.1, A.13.2.2, A.13.2.3
Análisis del impacto en el negocio	A.17.1.1

Documentos	Capítulo de ISO 27001:2013
Plan de prueba y verificación	A.17.1.3
Plan de mantenimiento y revisión	A.17.1.3
Estrategia de la continuidad de negocio	A.17.2.1
Fuente: Checklist of Mandatory Documentation Required by ISO/IEC 27001 (2013 Revision). Commonly used non-mandatory documents.	

En cuanto al anexo A, las secciones del anexo se han incrementado a 14 y han sido añadidos 11 nuevos controles...(Véase Cuadro 4)

Cuadro 4. Nueva estructura y controles de la Norma ISO 27001:2013.

Nueva Estructura del Anexo A	Controles añadidos al Anexo A
A5 Políticas de Seguridad. A6 Organización de la Seguridad de la Información. A7 Seguridad de los Recursos Humanos. A8 Gestión de Activos. A9 Control de Acceso. A10 Criptografía. A11 Seguridad Física y del Entorno. A12 Seguridad de las Operaciones. A13 Seguridad de las Comunicaciones. A14 Adquisición, desarrollo y mantenimiento de los sistemas de información. A15 Relaciones con los proveedores A16 Gestión de incidentes de seguridad de información A17 Aspectos de la continuidad del negocio en la Seguridad de la información. A18 Cumplimiento	A.6.1.5 Seguridad de la información en la gestión de proyectos. A.12.6.2 Restricciones en la instalación de software. A.14.2.1 Política de desarrollo seguro. A.14.2.5 Principios de ingeniería de sistemas seguros. A.14.2.6 Entorno de desarrollo seguro. A.14.2.8 Pruebas de seguridad en Sistemas. A.15.1.1 Política de seguridad de la información para las relaciones con proveedores. A.15.1.3 Tecnología de información y comunicación en la cadena de suministro. A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información. A.16.1.5 Respuesta a incidentes de seguridad de la información. A.17.2.1 Disponibilidad de las instalaciones de procesamiento de información.
Fuente: BSI-ISO27001-mapping-guide-UK-EN. Group 2 - Annex A controls.	

2.2.1.2 ISO/IEC 27002:2013. A partir de la publicación de la norma ISO 17799 como ISO 27002 en 2005, este se convierte en un complemento para los controles de la norma ISO 27001 incluidos en el anexo A, esto debido a que brinda mayores posibilidades para la selección de los controles aplicables en las organizaciones. Con la nueva versión del año 2013, se reduce el número total de controles incluidos en la norma pasando de 133 a 114 y se incluye una nueva sección de Criptografía. El cuadro mostrado a continuación muestra la comparación del contenido de las normas.⁷

Cuadro 5. Comparación de contenido norma ISO 27002 versiones 2005 y 201389

ISO/IEC 27002:2005	ISO/IEC 27002:2013
<ul style="list-style-type: none"> - Estructura de la norma - Evaluación y tratamiento del riesgo - Política de seguridad - Aspectos organizacionales de la seguridad de la Organización - Gestión de activos - Seguridad Ligada a los recursos Humanos - Seguridad Física y del entorno - Gestión de las comunicaciones y Operaciones - Control de Acceso - Adquisición, desarrollo y mantenimiento de los sistemas de información - Gestión de Incidentes de la seguridad de la información - Gestión de la continuidad del negocio - Cumplimiento 	<ul style="list-style-type: none"> - Estructura de la norma - Política de seguridad - Evaluación y tratamiento del riesgo - Aspectos organizacionales de la seguridad de la Organización - Seguridad Ligada a los recursos Humanos - Control de Acceso - Criptografía - Seguridad Física y del Entorno - Seguridad en las Operaciones - Seguridad en las Comunicaciones - Adquisición, desarrollo y mantenimiento de los sistemas de información - Relaciones con los proveedores - Gestión de Incidentes de la seguridad de la información - Aspectos de la seguridad de la información en la continuidad del negocio - Cumplimiento
<p>Fuente: ISO/ICE 27002:2013 Information technology — Security techniques — Code of</p>	

⁷ QUICK LINK. ISO 27001: Information technology — Security techniques — Code of practice for information security controls. [en línea], [consultado el 2 de agosto de 2014]. Disponible en: <http://www.iso27001security.com/html/27002.html>

⁸ AENOR. Comprehensive Performance Assessment for local government. [en línea], [consultado el 2 de agosto de 2014]. Disponible en: <http://www.en.aenor.es/aenor/normas/fichanorma.asp?tipo=N&codigo=N0044393&PDF=Si>

⁹ Ibíd.

ISO/IEC 27002:2005	ISO/IEC 27002:2013
practice for information security controls. Contents of ISO/IEC 27002:2013.	

2.2.2 COBIT

2.2.2.1 Definición. COBIT es un “acrónimo para Control Objectives for Information and related Technology (Objetivos de Control para tecnología de la información y relacionada); desarrollada por la Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI).

COBIT es un marco de trabajo aceptado mundialmente para el adecuado control de proyectos de tecnología, los flujos de información y los riesgos que éstas implican. COBIT se utiliza para planear, implementar, controlar y evaluar el gobierno sobre TIC incorporando objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez.

Permite a las empresas aumentar su valor TIC y reducir los riesgos asociados a proyectos tecnológicos. Ello a partir de parámetros generalmente aplicables y aceptados, para mejorar las prácticas de planeación, control y seguridad de las Tecnologías de Información.

COBIT contribuye a reducir las brechas existentes entre los objetivos de negocio, y los beneficios, riesgos, necesidades de control y aspectos técnicos propios de un proyecto TIC; proporcionando un Marco Referencial Lógico para su dirección efectiva.”¹⁰

Los beneficios ofrecidos son:

- Optimizar los servicios y el coste de TI
- Apoyar el cumplimiento de leyes, normas, reglamentos, acuerdos contractuales, entre otros.
- Gestión y gobernabilidad de nuevas tecnologías.
- Reducción de los perfiles de riesgo, promoviendo la correcta administración de la seguridad (COBIT 5).

2.2.2.2 Metodología. COBIT, como marco de referencia de gestión de procesos y más con su versión 5, donde se define un capítulo específico para la gestión del área de seguridad, establece una serie de principios sobre los cuales la organización debe definir, construir, implementar y mantener las políticas de

¹⁰ ITERA IT BUSSINESS PROCESS. ¿Qué es Cobit? [en línea], [consultado el 2 de agosto de 2014]. Disponible en: <http://www.itera.com.mx/ititstitute/maills/chile/cobit.htm>

seguridad.

Los principios, descritos a continuación son los pilares claves de toda la modelación a realizar ya que permiten reducir los perfiles de riesgos a través de una adecuada administración. Estos son:

- **Satisfacer las necesidades de las partes interesadas.** Se debe identificar quienes son los actores interesados en la implementación del modelo. Este es un proceso riguroso; ya que se debe identificar los recursos, áreas, participes, procesos, políticas y demás que serán el objeto de regulación y estandarización, ya que esto permitirá:

- Minimizar el riesgo
- Maximizar los beneficios
- Optimización de recursos
- Entre otros.

Adicionalmente aquí se definirá todo lo correspondiente a evaluar y que se incluirá en los procesos de definición de cronogramas

- **Cubrir la empresa de extremo a extremo:** Seguridad de la información es un concepto que en muchas ocasiones solamente involucra al área de TI de la compañía. Hoy en día, este es un proceso que se debe medir de manera transversal a todas las áreas de la compañía ya que de manera conjunta y como buena práctica, se debe respaldar a todas estas con el fin de garantizar un correcto manejo y procesamiento de la información.

- **La aplicación de un único marco integrado:** La aplicación de las políticas y modelos de seguridad, en muchos casos es una actividad de “apagar incendios”, arreglo lo que falle y queda solucionado, sin tener en cuenta que se pudo afectar y activar alguna otra vulnerabilidad latente en el sistema sin un debido control.

Un marco integrado permitirá controlar de manera conjunta todos los aspectos de flujo de información (almacenamiento, procesamiento, etc.), los procesos de atención de incidentes cuando son requeridos y los procesos de gestión documental.

Normalmente se aplica una matriz de gestión de controles donde se realiza el respectivo cruce del área o áreas de interés y los controles a implementar.

- **Habilitación de un enfoque holístico:** Es importante ver a seguridad de la información como un conjunto integrado de componentes donde todas las áreas interesadas son participes en el proceso de gestionar, garantizar y monitorear. Donde un grupo de personas definidas como los facilitadores se encargaran de ayudar a la organización a integrar las operaciones al modelo de seguridad.

Teniendo en cuenta todos los componentes a involucrar dentro del proceso de gestión de la seguridad:

- Facilitadores
- Directores de área
- Modelo a implementar
- Políticas
- Entre otros.

- **Separación de la gobernabilidad de la gestión:** es indispensable tener en cuenta que:

- **Gobernabilidad:** Asegura las necesidades e intereses de las partes involucradas, con el fin de garantizar el cumplimiento de los objetivos corporativos, apoyando la toma de decisiones, el monitoreo y el cumplimiento.

- **Gestión:** Planes que se construyen, ejecutan y supervisan y que van de acuerdo a los objetivos de la compañía.

Aunque estos conceptos son diferenciados y tienen actividades diferentes, se deben apoyar de manera conjunta.

La definición de un modelo de seguridad implementando COBIT 5 ayuda a satisfacer las múltiples necesidades de la Administración estableciendo un puente entre los riesgos del negocio, los controles necesarios y los aspectos técnicos...(Véase Cuadro 6)

Cuadro 6. Procesos o Facilitadores COBIT 5

Dominio	Proceso
Evaluar, Orientar y Supervisar (Dominio de Gobierno)	EDM01 Asegurar el establecimiento y Mantenimiento del Marco de Gobierno EDM02 Asegurar la entrega de los beneficios EDM03 Asegurar la Optimización del Riesgo EDM04 Asegurar la Optimización de los Recursos EDM05 Asegurar la Transparencia de las Partes Interesadas
Alinear, Planificar y Organizar (Dominio de Administración)	APO01 Gestionar el Marco de Gestión de TI APO02 Gestionar las Estrategias APO03 Gestionar la Arquitectura Empresarial APO04 Gestionar la Innovación APO05 Gestionar Portafolio APO06 Gestionar el Presupuesto y los Costes APO07 Gestionar los Recursos Humanos APO08 Gestionar las Relaciones

Dominio	Proceso
	APO09 Gestionar los Acuerdos de Servicios APO10 Gestionar los Proveedores APO11 Gestionar la Calidad APO12 Gestionar el Riesgo APO13 Gestionar la Seguridad
Construir, Adquirir e Implementar (Dominio de Administración)	BAI01 Gestionar los Programas y Proyectos BAI02 Gestionar la Definición de Requisitos BAI03 Gestionar la Identificación y la Construcción de Soluciones BAI04 Gestionar la Disponibilidad y la Capacidad BAI05 Gestionar la Introducción de Cambios Organizativos BAI06 Gestionar los Cambios BAI07 Gestionar la Aceptación del Cambio y de la Transición BAI08 Gestionar el Conocimiento BAI09 Gestionar los Activos BAI10 Gestionar la Configuración

Cuadro 6. Procesos o Facilitadores COBIT 5 (Continuación)

Dominio	Proceso
Entregar, dar Servicio y Soporte (Dominio de Administración)	DSS01 Gestionar las Operaciones DSS02 Gestionar las Peticiones DSS03 Gestionar los Problemas DSS04 Gestionar la Continuidad DSS05 Gestionar los Servicios de Seguridad DSS06 Gestionar los Controles de los Procesos de Negocio
Supervisar, Evaluar y Valorar (Dominio de Administración)	MEA01 Supervisar, Evaluar y Valorar Rendimiento y Conformidad MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno MEA03 Supervisar, Evaluar y Valorar Conformidad con los Requerimientos Externos
Fuente: Cobit 5 For Information Security	

Además de que provee las buenas prácticas a través de un dominio y un marco de referencia de todos los procesos y presenta las actividades en una estructura manejable y lógica.

De los Procesos o Facilitadores COBIT se debe realizar una clara identificación, ya que por su gran complejidad abarcan bastantes puntos. Para ello se debe realizar el análisis respectivo a cuales van a ser incluidos. La versión de COBIT 5 incluye un numeral y un marco de referencia propicio para la gestión y la gobernabilidad de la seguridad de la información. Así como es un marco de referencia, incluye sus procesos los cuales deben ser incluidos ya que son el eje de integración del marco de referencia de seguridad de la información con los

demás literales del modelo COBIT.

Se debe hacer la aclaración que estos procesos abarcan dos áreas principales que predominan: Gobierno y Gestión, la cual se subdivide en 4 Dominios de Gestión. El Dominio de Gobierno es el encargado de mantener la gobernabilidad del área de TI, mientras que los Dominios de Gestión se encargan de gestionar y controlar toda la parte de TI

Al momento de realizar la evaluación de los procesos COBIT se deben tener en cuenta los principios de la seguridad informática asociándolos con los objetivos, metas planes operativos y demás de la empresa, ya que de esta manera todo el modelo de gestión ira construido de manera transversal a esta...(Véase Cuadro 7)

Cuadro 7. Principios de la Seguridad Informática¹¹

Principio	Definición
Aislamiento	Regular el acceso al sistema
Auditoria	Capacidad de validar cualquier manipulación del sistema y poder determinar quién y cuándo lo realizó.
Autenticidad	Asegurar el origen de la información, preferiblemente validando la identidad del emisor
Confidencialidad	Evitar que las personas no autorizadas no tengan acceso a ninguna parte del sistema
Consistencia	Asegurar que el sistema se comporta de acuerdo a los parámetros establecidos
Disponibilidad	El sistema independiente a un fallo se mantiene funcionando de manera eficiente
Integridad	Asegurar que la información no ha sido manipulada y alterada
Participación universal	Que los usuarios involucrados participen en la correcta gestión de la seguridad
Principio de menor privilegio	Cualquier objeto ¹² involucrado solo debe poseer los accesos requeridos.
Principio del eslabón más débil	El grado de seguridad del sistema está condicionado al grado de seguridad del punto más vulnerable
Punto de control centralizado	Establecer un único punto de control de acceso para cualquier parte del sistema, garantizando que siempre haya que pasar por el aun en caso de un ataque
Seguridad en caso de fallo	En caso de falla del sistema, este deberá quedar en un estado seguro donde no haya pérdida de información.
Simplicidad	Mantener el mayor grado de simplicidad para evitar riesgos ocultos.
Fuente: Cobit 5 For Information Security	

Adicionalmente, validados contra los recursos de TI involucrados en el sistema.

¹¹ FEDERACIÓN DE SERVICIOS A LA CIUDADANÍA. Seguridad informática. ? [en línea], [consultado el 2 de agosto de 2014]. Disponible en: http://www.fsc.ccoo.es/comunes/recursos/99922/doc28596_Seguridad_informatica.pdf

¹² Se define como objeto cualquier usuario, programa, sistema, etc.; que manipulan de alguna manera el sistema.

COBIT define los recursos como:

Cuadro 8. Recursos de la Infraestructura tecnológica.

Aplicaciones	Sistema de aplicación es la suma de todos los procedimientos manuales y automáticos.
Datos	Los elementos de datos son representaciones de la realidad (Personas, cuentas) que pueden ser internos o externos, estructurados y no estructurados, gráficos, sonidos, etc. y que son usados por la empresa en sus operaciones diarias.
Instalaciones	Recursos para alojar las diferentes tecnologías (Físicas y Lógicas).
Personas	Conocimiento, conciencia y productividad del individuo para planear, organizar, adquirir, entregar soportar y monitorear servicios y sistemas.
Tecnología	La tecnología cubre todo lo referente a Hardware, Software, Redes, Sistemas Operativos, Multimedia, etc.
Fuente: Cobit 5 For Information Security	

Selección de los procesos de COBIT relacionados con el diseño del modelo de seguridad

Los recursos de TI necesitan ser administrados por un conjunto de procesos que garanticen su correcta ejecución, con el fin de responder a los objetivos corporativos proporcionando información correcta cuando esta sea precisada.

Se debe dejar claro que los controles ofrecidos por COBIT en cada uno de sus procesos no necesariamente satisfacen todos los requerimientos de información del negocio de igual manera, por ello estos se miden de la siguiente manera:

- **Primario (P):** grado en el que el proceso COBIT impacta directamente el requerimiento de seguridad de la información de interés.
- **Secundario (S):** grado en el que el proceso COBIT impacta indirectamente o en menor medida el requerimiento de seguridad de la información de interés.
- **Blanco (Vacía):** proceso COBIT que podría aplicarse, sin embargo, el requerimiento de seguridad de la información podría ser satisfecho de mejor manera por la aplicación de otro proceso.

2.3 HIPÓTESIS

Hi: Es posible elaborar un modelo de seguridad para el Datacenter de Sonda Colombia que integre las normas ISO/IEC 27001:2013, ISO/IEC 27002:2013y COBIT 5 FOR INFORMATION SECURITY para el Datacenter de servicios de la empresa Sonda Colombia y logre alinearse con los objetivos de la compañía.

Ho: No es posible elaborar un modelo de seguridad para el Datacenter de Sonda Colombia que integre las normas ISO/IEC 27001:2013, ISO/IEC 27002:2013y COBIT 5 FOR INFORMATION SECURITY para el Datacenter de servicios de la empresa Sonda Colombia y se alinee con los objetivos de la compañía.

Ha: Un modelo de seguridad para el Datacenter de Sonda Colombia basado en las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013yCOBIT 5 FOR INFORMATION SECURITY puede ser más apropiado para la compañía.

3. DISEÑO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

La investigación realizada es de tipo no experimental, caracterizada porque no se tiene manipulación directa de variables debido a que el desarrollo del modelo no incluyó pruebas de implementación parcial ó total del modelo.

3.2 UNIVERSO Y MUESTRA

3.2.1 Universo. El universo del presente proyecto se centra en los Datacenter de SONDA, una compañía que cuenta con más 3.000 m² de salas de equipos, administrando más de 5.000 servidores físicos y más de 500 TB de capacidad de almacenamiento, lo que se suma a las certificaciones de seguridad ISO/IEC 27001, Datacenter certificados Tier III en Santiago (diseño por Uptime Institute) y Sao Paulo (diseño y operación por TÜV Rheinland), SAP Partner Hosting, Cisco Managed Service, entre otras.

3.2.2 Muestra. La muestra tomada para el presente proyecto es un nuevo Datacenter de SONDA localizado en la ciudad de Bogotá el cuál será utilizado para la prestación de sus servicios en la nube.

4. VIABILIDAD

4.1 RECURSOS

Para la integración de las normas ISO 27001 y COBIT “ISOBIT”, se requerirá contar con recursos humanos y técnicos que permitan alinear la integración de estos estándares, donde COBIT nos garantizara gobernabilidad e ISO nos permitirá alinear y ajustar controles con la cultura organizacional de SONDA.

Los recursos previstos para la el diseño, planeación y ejecución del proyecto son:

4.1.1 Humanos

- Gerente de proyecto (1): Sera el encargado de planear y garantizar la ejecución del proyecto y cumplimiento del cronograma
- Integrador de estándares ISO y COBIT(2): revisara la integración desde el punto de vista funcional garantizando que la integración permita alinear la cultura organizacional y la misión esencial del servicio de Datacenter identificando la misión crítica real del área, uno de los dos recursos debe conocer a profundidad alguno de los estándares a trabajar
- Auditor de alineamientos de integración (1): Debe ser miembro de la organización para conocer el entorno y funcionamiento de la misma con el fin de garantizar el flujo de trabajo dentro de la integración ISOBIT con los servicios de Datacenter prestados y los procesos ya implementados a nivel administrativo en el área
- Líder de proceso (1): Líder del proceso de seguridad en la compañía u área que permita justificar la alineación de controles y estándares.
- Auditor de controles (2): Este auditor del control debe ser ajeno a la implementación a los procesos y al área ya que el control y la descripción del control debe ser entendible para su correcta aplicación

4.1.2 Físicos

- Equipos de cómputo: Equipos donde se puedan elaborar los documentos y llevar a cabo el diseño y definir actividades

4.1.3 Técnicos. Se deben definir qué tipo de insumos técnicos se van a necesitar para el desarrollo de la metodología, en este caso sería necesario contar con las normas ISO27001 y COBIT

4.2 PRESUPUESTO

Tabla 1. Diseño del Proyecto

TAREAS DEL PROYECTO	HORAS MANO OBRA	COSTO MANO OBRA (COP)	TOTAL POR TAREA
Desarrollar especificaciones funcionales	26	\$520.000,00	\$520.000,00
Desarrollar arquitectura de integración ISO/COBIT	48	\$960.000,00	\$960.000,00
Desarrollar especificaciones de integración preliminar	36	\$720.000,00	\$720.000,00
Desarrollar especificaciones de la integración detallada	24	\$480.000,00	\$480.000,00
Desarrollar plan de prueba de alineación a la organización	24	\$480.000,00	\$480.000,00
Subtotal	158	\$3.160.000,00	\$3.160.000,00
Fuente: autores			

Tabla 2. Desarrollo del Proyecto

Desarrollar Modelo de Seguridad basado en normas ISO y COBIT	24	\$480.000,00	\$480.000,00
Obtener información de procesos activos no documentados en la compañía	48	\$960.000,00	\$960.000,00
Alinear y crear procesos de control basados en ISO alineados a COBIT	48	\$960.000,00	\$960.000,00
Desarrollar Procesos alineados a la organización	18	\$360.000,00	\$360.000,00
Realizar prueba de control de procesos	36	\$720.000,00	\$720.000,00
Subtotal	174	\$3.480.000,00	\$3.480.000,00
Fuente: autores			

Tabla 3. Entrega del Proyecto

Modelado de controles base	16	\$320.000,00	\$320.016,00
Mapa de modelamiento dirigido a líderes de procesos	16	\$320.000,00	\$320.016,00
Realizar prueba de aceptación del modelo	10	\$200.000,00	\$200.010,00
Realizar auditoría de procesos base para el modelo	24	\$480.000,00	\$480.024,00
Proporcionar guía de control del modelo	10	\$200.000,00	\$200.010,00
Documentar y entregar controles modelados	36	\$720.000,00	\$720.036,00
Subtotal	112	2.240.000,00	2.240.112,00
Fuente: autores			

Tabla 4. Administración del Proyecto

Reuniones/informes de progreso con líder de proceso compañía	34	\$680.000,00	\$680.034,00
Reuniones/informes de estado con grupo de trabajo	20	\$400.000,00	\$400.020,00
Revisión conforme a actualizaciones de estándares ISO y COBIT	10	\$200.000,00	\$200.010,00
Validar compatibilidad de normas con otros procesos o áreas de la compañía	15	\$300.000,00	\$300.015,00
Administración de tiempo global	6	\$120.000,00	\$120.006,00
Control de calidad	6	\$120.000,00	\$120.006,00
Administración global del proyecto	12	\$240.000,00	\$240.012,00
Subtotal	103	\$2.060.000,00	\$2.060.103,00
Fuente: autores			

Tabla 5. Presupuesto Total

Total		547	10.940.000,00	10.940.215,00
--------------	--	------------	----------------------	----------------------

4.3 CRONOGRAMA

Tabla 6. Cronograma

NOMBRE DE TAREA	NOMBRE DE SUBTAREA	DURACIÓN	COMIENZO	FIN
Diseño del proyecto		10 días	Vie 06/06/14	Lun 15/06/14
	Desarrollar especificaciones funcionales	2 días	Vie 06/06/14	Sab 07/06/14
	Desarrollar arquitectura de integración ISO/COBIT	3 días	Dom 08/06/14	Mar 10/06/14
	Desarrollar especificaciones de integración preliminar	4 días	Mie 11/06/14	Sab 14/06/14
	Desarrollar especificaciones de la integración detallada	1 día	Dom 15/06/14	Dom 15/06/14
Desarrollar plan de prueba de alineación a la organización		2 días	Lun 16/06/14	Mar 17/06/14
	Identificar política de seguridad si no existe construirla	1 día	Lun 16/06/14	Lun 16/06/14
	alinear política a la misión y visión de la compañía	1 día	Mar 17/06/14	Mar 17/06/14
Desarrollo del Proyecto		32 días	Mie 18/06/14	Sab 19/07/14
	Desarrollar modelo de gobernabilidad ISO - COBIT	20 días	Mie 18/06/14	Lun 07/07/14
	Obtener información de procesos activos no documentados en la compañía	3 días	Mar 08/07/14	Jue 10/07/14
	Alinear y crear procesos de control basados en ISO alineados a COBIT	3 días	Vie 11/07/14	Dom 13/07/14

Tabla 6. Cronograma (Continuación)

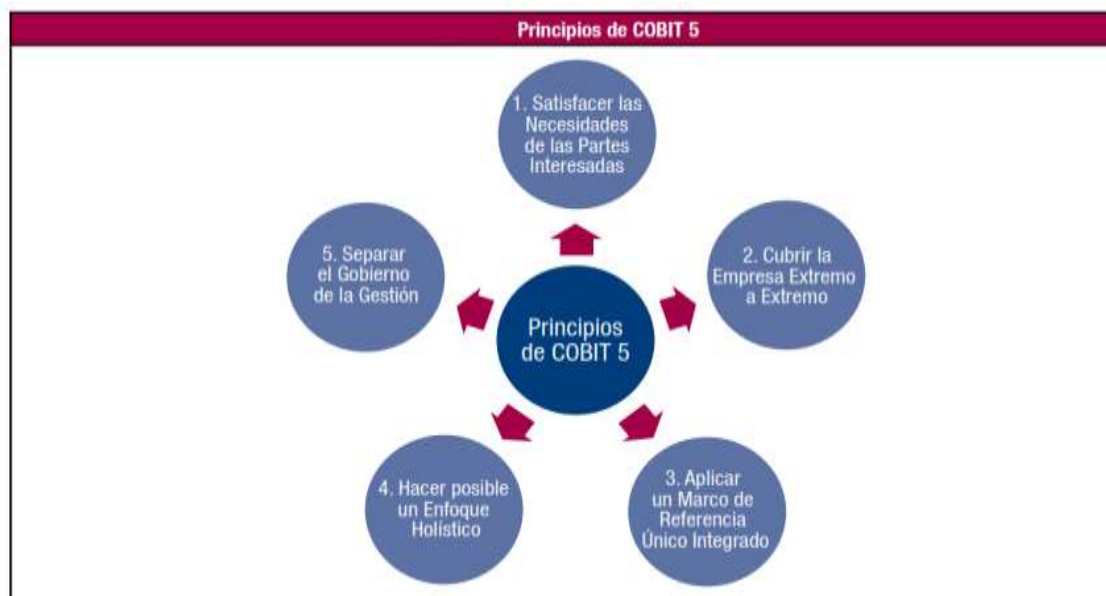
NOMBRE DE TAREA	NOMBRE DE SUBTAREA	DURACIÓN	COMIENZO	FIN
Desarrollo del Proyecto	Desarrollar Procesos alineados a la organización	2 días	Lun 14/07/14	Mar 15/07/14
	Realizar prueba de control de procesos para el modelamiento	4 días	Mie 16/07/14	Sab 19/07/14
ENTREGA DEL PROYECTO		15 días	Dom 20/07/14	Dom 03/08/14
	modelamiento de controles base	2 días	Dom 20/07/14	Lun 21/07/14
	Documento del modelo orientado a líderes de procesos	2 días	Mar 22/07/14	Mie 23/07/14
	Realizar auditoria de procesos base del modelo	3 días	Jue 24/07/14	Sab 26/07/14
	Proporcionar guía de control en el modelamiento	2 días	Dom 27/07/14	Lun 28/07/14
	Documentar y entregar modelamiento de controles	6 días	Mar 29/07/14	Dom 03/08/14
	Fuente: autores			

5. DISEÑO DEL PROYECTO

COBIT 5 For Information Security es un framework para gestión de la seguridad de la información. SONDA como empresa proveedora de servicios de TI, pretende a mediano plazo la expansión de los servicios prestados a sus actuales y futuros clientes con el montaje de un datacenter que ofrezca servicios cloud. Adicionalmente pretende garantizar la seguridad de la información que será consignada en dichos servicios; en contraste, la empresa debe estar en capacidad de responder de manera correcta ante cualquier requerimiento de seguridad.

Para ello COBIT plantea 5 principios fundamentales:

Figura 1. Principios de COBIT



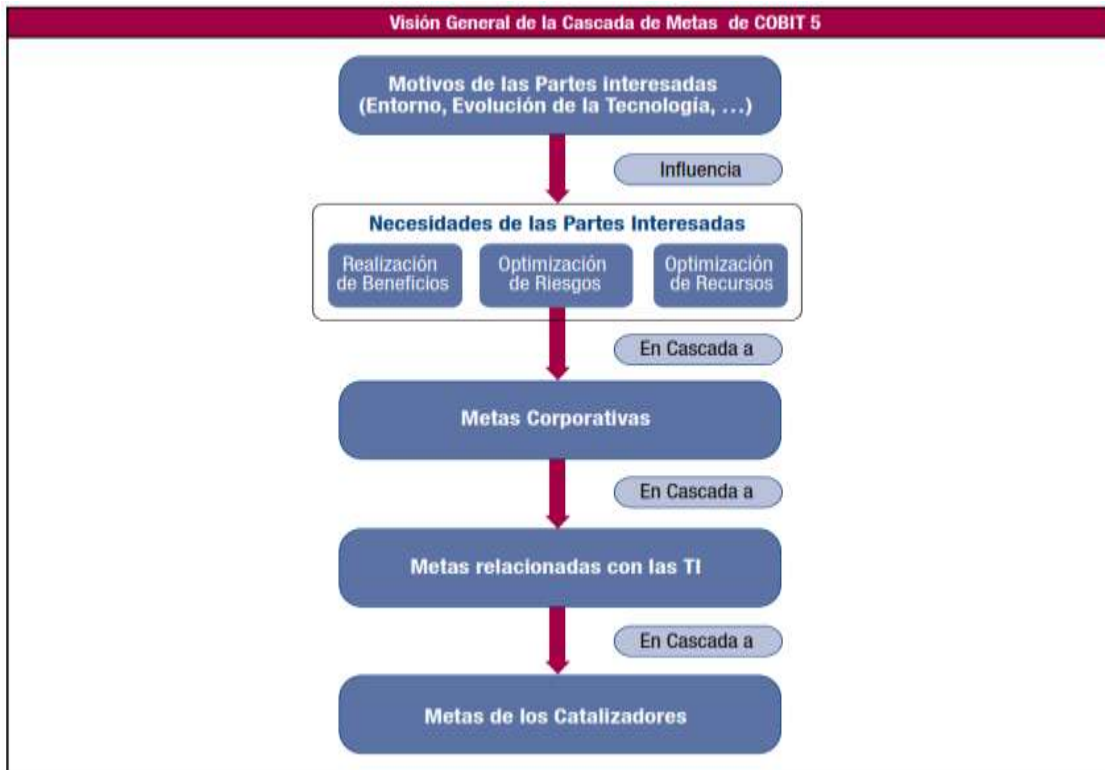
Fuente: Cobit 5 for Information security

5.1 PRINCIPIOS DE COBIT 5 PARA SEGURIDAD DE LA INFORMACIÓN

5.1.1 Principio 1: Satisfacer las necesidades de las partes interesadas. Toda empresa tiene como función importante generar un valor agregado a sus clientes y demás relacionados, igualmente se debe tener presente que cada uno tiene objetivos y metas completamente diferentes, pero que de una u otra forma deben coexistir para generar un equilibrio y para ello es importante poder garantizar la correcta sinergia entre todas las partes, validar que los intereses de cada parte están influenciados por diferentes motivos (donde estas convergen de metas corporativas a más específicas como las operativas) y principalmente que la seguridad de la información es una necesidad importante y fundamental ya que es el motor de cualquier proceso.

Para ello es importante tener en cuenta el siguiente diagrama de cascada de metas:

Figura 2. Metas de COBIT



Fuente: Cobit 5 for Information security

5.1.2. Principio 2: Cubrir la empresa de Extremo a Extremo. Se debe tener en cuenta todas las perspectivas corporativas, ya que de manera más integra se llega al enfoque esperado sin descuidar aspectos que pueden llegar a ser relevantes. COBIT permite el apoyo de áreas que específicamente no dependan de TI pero que dan soporte a TI.

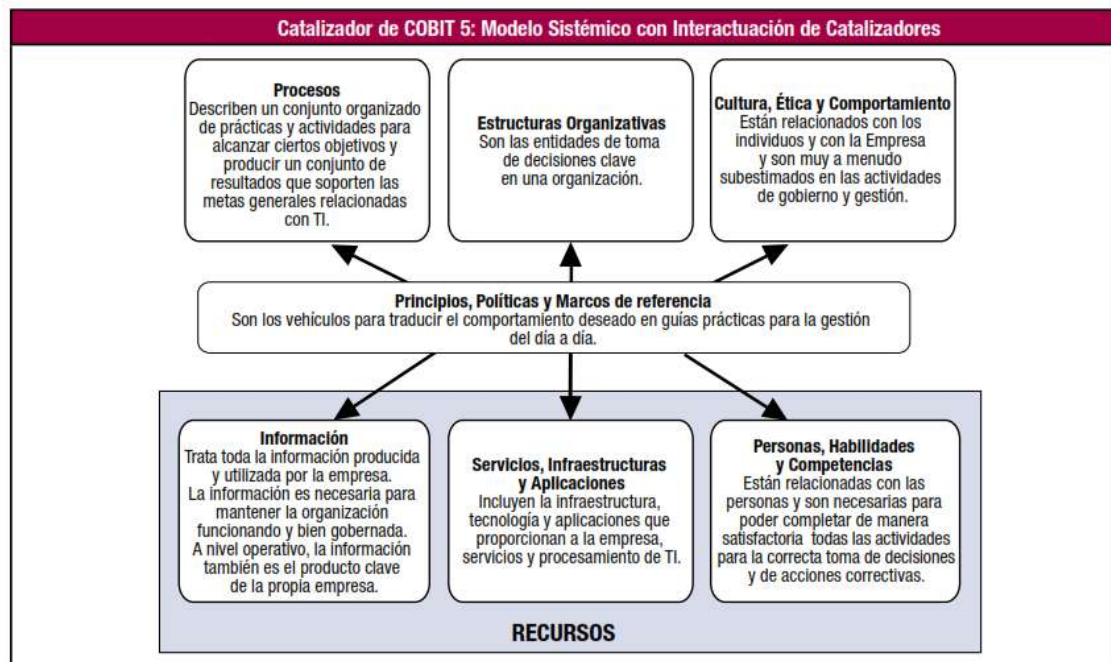
5.1.3 Principio 3: Aplicar un marco de referencia Único Integrado. Existen muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades relacionadas con las TI. COBIT 5 For Information Security es un marco más completo en cuanto a la cobertura de la general que presta a la empresa, y proporciona una base unificada de conceptos que son utilizados para integrar de manera efectiva otros marcos de referencia, estándares y prácticas que se utilicen.

5.1.4 Principio 4: Hacer posible un Enfoque Holístico. Un marco efectivo de

Gobernabilidad debe permitir una evolución iterativa e interactiva, debe estar en capacidad de responder a las diferentes necesidades del negocio cuando estas sean requeridas, para ello el marco holístico de COBIT 5 y sus catalizadores permiten esta interacción entre cada una de las partes asumiendo así el poder gestionar y controlar el cambio.

Estos catalizadores son:

Figura 3. *Modelo sistemático de Interactuación de Catalizadores COBIT*



Fuente: Cobit 5 for Information security

5.1.5 Principio 5: Separar el Gobierno de la Gestión. COBIT 5 hace una clara distinción entre Gobierno y Gestión. El Gobierno hace referencia a la evaluación de las necesidades, condiciones y opciones de todas las partes involucradas para poder alcanzar las metas corporativas de una manera equilibrada y acordadas para la correcta toma de decisiones; mientras que la Gestión, se encarga de planificar, construir, ejecutar y controlar todas las actividades que se encargan de cumplir con dichas metas.

5.2 CATALIZADORES

Los catalizadores son factores que, individual y colectivamente, influyen sobre si algo funcionará – en este caso, el gobierno y la gestión de la empresa TI. Los catalizadores son guiados por los objetivos de alto nivel relacionados con TI.

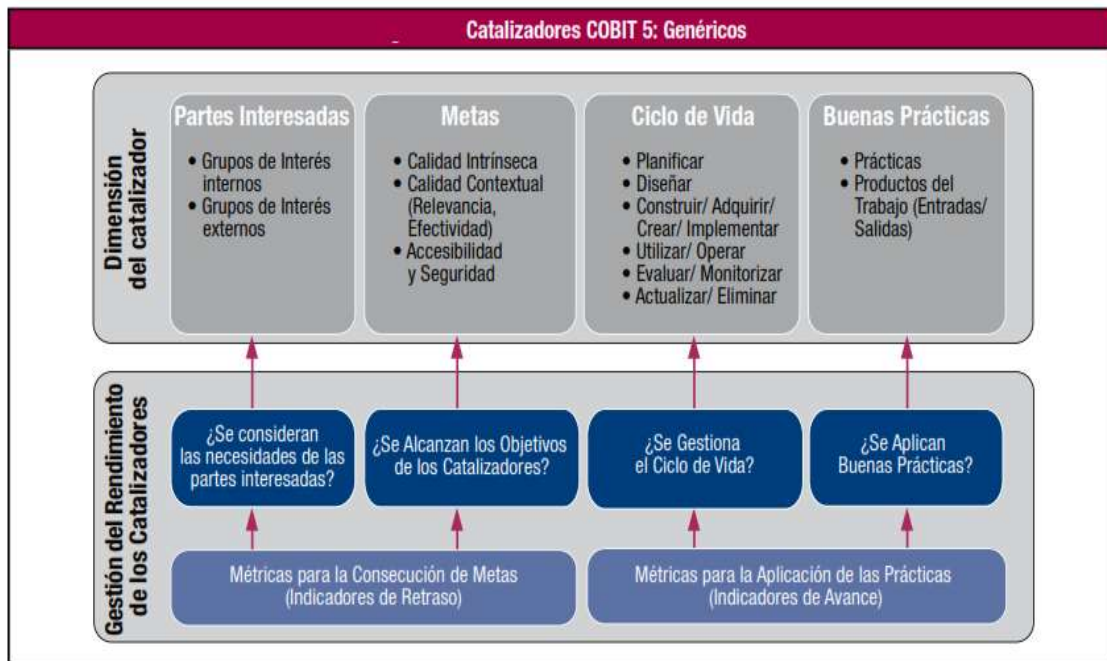
Teniendo en cuenta estos 5 principios ofrecidos por COBIT, se tiene presente la siguiente orientación para la administración de la presentación de los correspondientes catalizadores:

- Las políticas, principios y marcos de referencia de seguridad de la información.
- Los procesos, incluyendo detalles y actividades específicos de seguridad de la información.
- Las estructuras organizativas específicas de seguridad de la información.
- En términos de cultura, ética y comportamiento, los factores determinantes para el éxito del gobierno y la gestión de la seguridad de la información.
- Los tipos de información específicos de la seguridad de la información para permitir el gobierno y la gestión de la seguridad de la información en la empresa.
- Las capacidades de servicio necesarias para proporcionar seguridad de la información y las funciones relacionadas con la empresa.
- Las personas, habilidades y competencias específicas para seguridad de la información.

Dada la estructura organizacional de SONDA, donde ya existen perfiles encargados de la administración, gestión, documentación y seguimiento de las diferentes partes de los servicios ofrecidos a sus clientes, los catalizadores de Cultura, ética y comportamiento, los tipos de información específicos, Capacidades del servicio y Personas, habilidades y competencias no serán tenidos en cuenta ya que existen procesos para la definición de los mismos, los cuales ya se encuentran evaluados por los procesos de recursos humanos y las necesidades del negocio.

5.2.1 Políticas, principios y marcos de referencia de seguridad de la información

Figura 4. Catalizadores genéricos COBIT 5



Fuente: Cobit 5 for Information security

Las políticas, los principios y los marcos de referencia son los medios que usará SONDA para definir el camino a seguir, el comportamiento deseado de cada una de las partes involucradas y que traducidos en guías formales, serán los mecanismos para llegar a establecer los comportamientos deseados.

5.2.1.1 Principios de la seguridad de la información. Dado que los principios de seguridad de la información de COBIT 5 para Seguridad de la Información, se aplican a cualquier modelo de negocio, estos serán tomados por SONDA como base para su operación.

Dar soporte al negocio:

- Centrarse en el negocio para asegurar que la seguridad de la información está integrada en las actividades de negocio esenciales.
- Dar calidad y valor a las partes interesadas para asegurar que la seguridad de la información aporta valor y cumple con los requisitos de negocio.
- Cumplir con los requisitos legales y regulatorios relevantes para asegurar que se cumplen las obligaciones estatutarias, se gestionan las expectativas de las partes interesadas y se evitan las penalizaciones.

- Proporcionar información oportuna y exacta sobre el desempeño de la seguridad de la información para dar soporte a los requisitos del negocio y gestionar el riesgo de la información.
- Evaluar las amenazas actuales y futuras para analizar y evaluar las amenazas de seguridad emergentes de manera que se puedan tomar acciones oportunas e informadas para mitigar el riesgo.
- Promover la mejora continua en la seguridad de la información para reducir costes, mejorar la eficiencia y eficacia y promover una cultura de mejora continua de la seguridad de la información.

Defender el negocio:

- Adoptar una estrategia basada en el riesgo para asegurar que el riesgo se trata de forma consistente y efectiva.
- Proteger la información clasificada para prevenir su revelación a personas no autorizadas.
- Concentrarse en las aplicaciones críticas para el negocio para priorizar los escasos recursos de seguridad de la información mediante la protección de las aplicaciones de negocio en las que un incidente de seguridad tendría un mayor impacto en el negocio.
- Desarrollar los sistemas de forma segura para construir sistemas de calidad y rentables en los que las personas del negocio puedan confiar.

Promover un comportamiento responsable en seguridad de la información:

- Actuar de manera profesional y ética para asegurar que las actividades relacionadas con la seguridad de la información se desarrollan de manera fiable, responsable y efectiva.
- Fomentar una cultura positiva de seguridad de la información para proporcionar una influencia de seguridad positiva en el comportamiento de los usuarios finales, reducir la probabilidad de que ocurran incidentes de seguridad y limitar su impacto potencial en el negocio.

Figura 5. Principios de COBIT



Fuente: Cobit 5 for Information security

5.2.1.2 Política general de la seguridad de la información. La alta dirección de SONDA, teniendo en cuenta que la información es un factor de alta importancia y criticidad en el desarrollo de los negocios actuales y un activo fundamental para el normal desarrollo de las actividades comerciales y operativas de la compañía, establece políticas, normas, planes de mejoramiento continuo y actividades de capacitación y sensibilización como parte integral de la gobernabilidad corporativa, ofreciendo a los usuarios, clientes, proveedores y demás entidades y personas relacionadas con la empresa niveles apropiados de integridad, disponibilidad y confidencialidad de la información de propiedad y/o administrada por SONDA, dando cumplimiento a los requisitos legales.

Basados en que SONDA ya ha implementado la norma ISO20000 y que algunos de sus procesos son compatibles con ISO27001, las siguientes políticas ya están siendo aplicadas:

- Gestión de incidentes de seguridad
- Recursos humanos
- Gestión de activos
- Relación con los proveedores
- Continuidad del negocio

5.2.1.3 Políticas específicas de la seguridad de la información dirigidas por función de la seguridad de la información

- Políticas de seguridad de la información

Descripción. SONDA debe asegurar la documentación de las políticas de seguridad de la información, incluyendo la definición de responsabilidades generales y específicas para la gestión de la seguridad de la información. Estas deben ser actualizadas constantemente asegurando que las revisiones de las mismas queden registradas junto con un control de todos los cambios relevantes realizados.

Objetivo. Administrar y mantener la seguridad de la información en SONDA de acuerdo con los requerimientos del negocio, leyes y regulaciones.

Alcance. Las disposiciones contenidas en la presente política, son de aplicación obligatoria para todas las áreas y personal de SONDA. Tanto los usuarios de SONDA como los de las empresas contratistas y terceros, deberán cumplir estrictamente lo establecido en la presente Política.

- Control de acceso

Descripción. Se deben implementar medidas de seguridad que permitan establecer permisos de acceso a los recursos de información de SONDA, en base a su cargo, responsabilidades, relaciones con terceros y el nivel de información al que tendrán acceso. Para ello se deben establecer procedimientos para registro y eliminación de usuarios, sensibilizar al personal acerca de las responsabilidades que adquieren respecto al uso de contraseñas y uso adecuado de equipos y establecer derechos de acceso basados en niveles y privilegios de información.

Objetivo

- Proporcionar seguridad razonable con respecto a la integridad y seguridad de los sistemas y recursos de información de SONDA, a través de un adecuado manejo y mantenimiento de las cuentas del usuario y los derechos y privilegios asociados con ellas, para acceder a los servidores, aplicaciones, bases de datos y datos.

- Implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información. Dichos procedimientos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Alcance. Esta política aplica a todos los sistemas de SONDA, incluyendo sin limitar a las aplicaciones comerciales, bases de datos, aplicaciones desarrolladas internamente, equipos, instalaciones, sistemas, y redes que la organización posea

en la actualidad o en el futuro, de manera que la no inclusión explícita en el presente documento, no constituye argumento para no proteger los activos de información que se encuentren en otras formas.

- Seguridad física y ambiental

Descripción. Se debe tener control de acceso a la información y a aquellos activos que la procesan, a través del establecimiento y clasificación de áreas, clasificación de los activos por nivel de sensibilidad, protección del cableado de energía y telecomunicaciones, realización de mantenimientos preventivos, restricciones para ingreso y retiro de equipos e ingreso a áreas protegidas, identificación de los empleados e implementación de medidas de seguridad para control y limitación de acceso a información clasificada.

Objetivo

- Impedir el acceso no autorizado, daños o interferencias a los activos de información dentro de la organización.
- Prevenir pérdidas, daños o compromiso de los bienes e interrupción de las actividades de SONDA.
- Evitar el robo y/o hurto de activos de información y de los equipos que la procesan.
- Implementar medidas para proteger la información manejada por el personal en el marco de sus labores habituales.

Alcance. Esta política debe ser cumplida por todo el personal de SONDA y los terceros autorizados para acceder a los activos y a las instalaciones de la organización.

- Mantenimiento, desarrollo y adquisición de sistemas informáticos

Descripción. Asegurar un nivel de protección adecuado al desarrollar, adquirir o realizar mantenimientos de sistemas informáticos a través del establecimiento de requisitos mínimos de seguridad necesarios para nuevos desarrollos, control de cambios, prevención de pérdida de integridad de la información, incorporación de controles criptográficos en desarrollos relacionados con información sensible, supervisión y monitoreo a terceros, control de acceso a archivos y códigos fuente de programas y establecer procedimientos adecuados para desarrollo y pruebas de software que no afecten la integridad de los programas en producción y que aseguren un nivel de seguridad adecuado durante todas las etapas del ciclo de desarrollo.

Objetivo

- Asegurar una adecuada protección para el desarrollo, mantención y adquisición de los programas de aplicación de SONDA que se utilizan para apoyar las funciones críticas del negocio.
- Identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación de los Sistemas Informáticos, diseñando controles de validación de datos de entrada, procesamiento interno y salida de datos.

Alcance. Esta política se aplica a todos los desarrollos, mantención y adquisición de aplicaciones, sistemas de información y equipos de comunicación de SONDA.

- Gestión de incidentes de seguridad

Descripción. Se deben establecer mecanismos que permitan a empleados, terceros y contratistas reportar incidentes de seguridad de la información teniendo en cuenta medidas de preservación de evidencia, uso de mesas de ayuda y definición de responsables del escalamiento, resolución y reporte de casos

Objetivo

- Establecer procedimientos operativos para gestionar apropiadamente las debilidades y eventos de seguridad.
- Asegurar que se toman acciones para prevenir los eventos de seguridad.
- Reducir los daños ocasionados por los incidentes de seguridad.

Alcance. Esta política debe ser cumplida por todo el personal de SONDA y los terceros autorizados para acceder a los activos y a las instalaciones de la organización.

- Control de criptografía

Descripción. Los empleados de Sonda deberán asegurar la confidencialidad de la información de acuerdo a los niveles de información establecidos, a través del cifrado de información denominada como sensible, el uso de firmas digitales al realizar intercambio de información a través de canales de comunicaciones, asegurar el uso de llaves criptográficas complejas y el intercambio de las mismas a través de un medio seguro.

Objetivo

- Asegurar el uso efectivo de la criptografía en las comunicaciones que involucren el intercambio de información sensible para SONDA.
- Asegurar la integridad, confidencialidad y autenticidad de la información almacenada o transmitida por SONDA.

Alcance. Esta política debe ser cumplida por todo el personal de SONDA y los terceros con los cuales se requiera el intercambio de información sensible.

- Seguridad en las operaciones

Descripción. Se debe asegurar que todos los procedimientos relacionados con la operación del Datacenter de Sonda sean controlados a través de medidas de seguridad que incluyan la documentación y notificación de decisiones relacionadas con la operación del mismo, la optimización de los recursos del Datacenter, la disponibilidad de puntos de restauración de los sistemas de información y el almacenamiento y revisión de logs generados por equipos de misión crítica de SONDA.

Objetivo

- Establecer procedimientos operativos para la administración de sistemas informáticos que aseguren la calidad de los procesos que se implementan en el ámbito operativo, a fin de minimizar los riesgos de pérdida de confidencialidad, integridad y disponibilidad de la información.
- Definir los requisitos de planeamiento de sistemas y procesos de aceptación del usuario para proteger los activos de información dentro de SONDA.
- Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información y comunicaciones, estableciendo responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y segregación de funciones.

Alcance. Esta política se aplica a todos los equipos, redes, aplicaciones y bases de datos que procesan información de SONDA o de aquellos clientes en los que SONDA cumpla el rol de Custodio de la Información.

5.2.1.4 Políticas específicas de la seguridad de la información dirigidas por otras áreas dentro de la empresa

- Organización de la seguridad de la información

Descripción. Sonda debe asegurar la creación de un “Comité de Seguridad de la Información” el cual tendrá la responsabilidad de llevar a cabo la gestión, evaluación, solución de materias relacionadas con la seguridad del Datacenter, la aprobación y revisión de proyectos de seguridad, modificación y aceptación de nuevas políticas de seguridad y la asignación de propietarios de información y responsables de la misma.

Objetivo. Establecer un modelo de seguridad para controlar la operación e implementación de seguridad de la información en SONDA.

Alcance. Las disposiciones contenidas en la presente política, son de aplicación obligatoria para todas las áreas y personal de SONDA. Tanto los usuarios de SONDA como los de las empresas contratistas y terceros, deberán cumplir estrictamente lo establecido en la presente Política.

- Recursos humanos

Descripción. SONDA debe velar por la seguridad de sus activos de información asociados a los recursos humanos a través de la verificación de antecedentes a los candidatos, verificación del Curriculum Vitae de los candidatos, sensibilización de los empleados con las políticas de seguridad de SONDA, acuerdos de confidencialidad y no divulgación de información y el entrenamiento a los empleados ante el correcto uso de sistemas de información.

Objetivo

- Establecer mecanismos específicos para realizar un proceso de selección que asegure el control adecuado de potenciales empleados de SONDA y de Este modo reducir el riesgo de errores humanos por falta de competencias, el mal uso de equipamiento de la compañía, robo y fraude.

- Reducir los daños ocasionados por incidentes de seguridad y mal funcionamiento de las medidas de control asociadas a la contratación, desempeño y desvinculación del personal.

- Asegurar que los empleados, contratistas y terceros estén conscientes de las amenazas de la seguridad de la información y que se comprometan al cumplimiento de política de seguridad de la información en la organización, durante el desempeño de sus labores.

Alcance. Esta política debe ser cumplida por todo el personal de SONDA y los terceros autorizados para acceder a los activos y a las instalaciones de la organización.

- Gestión de activos

Descripción. Sonda debe realizar una Clasificación de información adecuada que permita conocer a los responsables, custodios y propietarios de la misma, su importancia y su importancia, teniendo en cuenta criterios basados en los perjuicios que podría causar la divulgación de la misma. Así mismo se debe establecer una clasificación de activos de información según su tipo, confidencialidad, nivel de acceso y tipo de información que contiene, con el fin de facilitar el control del uso de activos por los empleados y proveedores que tengan relación con SONDA.

Objetivos

- Establecer los mecanismos para asegurar la protección de los activos de información en todas sus formas y medios, a través de un proceso de clasificación conforme a su sensibilidad e importancia.
- Mantener un adecuado nivel de protección de los activos de información mediante la asignación de Propietarios de la Información a todos los activos de información críticos.
- Definir pautas generales para asegurar una adecuada clasificación y control de la información.

Alcance. Las disposiciones contenidas en la presente política, son de aplicación obligatoria para todas las áreas y personal de SONDA. Tanto los usuarios de SONDA como los de las empresas contratistas y terceros, deberán cumplir estrictamente lo establecido en la presente política.

- Seguridad de las comunicaciones

Descripción. Se deben establecer responsabilidades y procedimientos formales para la gestión y operación de todo el equipamiento computacional y sistemas de información. Esto a través de proyecciones de capacidad de carga de los sistemas actuales, el reporte de casos que hayan comprometido la seguridad de la información, el control de los servicios administrados por terceros, la prevención y detección de software malicioso, la prevención de robo de activos de información, el intercambio seguro de información y la protección de medios que contengan información sensible.

Objetivo

- Consolidar la seguridad de la información dentro de QUINTEC a través de una administración apropiada por parte de las Gerencias, Áreas, grupos e individuos asignados a cada función.
- Definir en forma clara las responsabilidades de cada funcionario en el contexto de la seguridad de la información.
- Mantener la seguridad de las instalaciones donde se procesa información de la organización y de los activos accedidos por terceras partes.

Alcance. Esta política debe ser cumplida por todo el personal de SONDA y los terceros autorizados para acceder a los activos y a las instalaciones de la organización.

- Relación con los proveedores

Descripción. SONDA debe asegurar que todo proveedor vele por la integridad, confidencialidad y disponibilidad de los activos de Sonda y la información contenida en ellos en el momento de la prestación de sus servicios, así como el control de los cambios que realice sobre los mismos y el establecimiento de controles que permita evaluar su desempeño.

Objetivo

- Asegurar los activos de la compañía que son accedidos por terceros.
- Asegurar el uso adecuado de información suministrada a terceros a través de acuerdos con los proveedores.

Alcance. Las disposiciones contenidas en la presente política, son de aplicación obligatoria para todos los proveedores relacionados con SONDA como los de las empresas contratistas y terceros.

- Continuidad del negocio

Descripción. Sonda debe establecer procedimientos que permitan mantener la operación del Datacenter en caso de que se produzca una interrupción de las actividades regulares a través de pruebas periódicas de los planes de contingencia definidos, revisión de resultados, planes de mejora, identificación de procesos y recursos críticos y la asignación de responsabilidades a los empleados involucrados con los planes de contingencia.

Objetivo. Establecer medidas que mitiguen las interrupciones de las actividades calificadas como sensibles o críticas de SONDA debido a los efectos de fallas o desastres y asegurar su restauración oportuna.

Alcance. Esta política se aplica a los procesos de negocios calificados como críticos de SONDA.

- **Cumplimiento**

Descripción. SONDA debe asegurar el cumplimiento de sus políticas y procedimientos de seguridad a través de la identificación de estatutos, regulaciones y requerimientos contractuales que la afectan, la verificación de legitimidad y confiabilidad de los proveedores, el resguardo de los sistemas durante el transcurso de auditorías, control de destrucción de registros de información, control de información de terceros y la sensibilización y control del cumplimiento de dichas políticas por parte del personal de SONDA.

Objetivo

- Asegurar que todas las áreas y dependencias, dentro de la organización estén cumpliendo las políticas y procedimientos de seguridad. Además, esta política apunta a asegurar que los controles estén operando para proteger apropiadamente los activos de información.

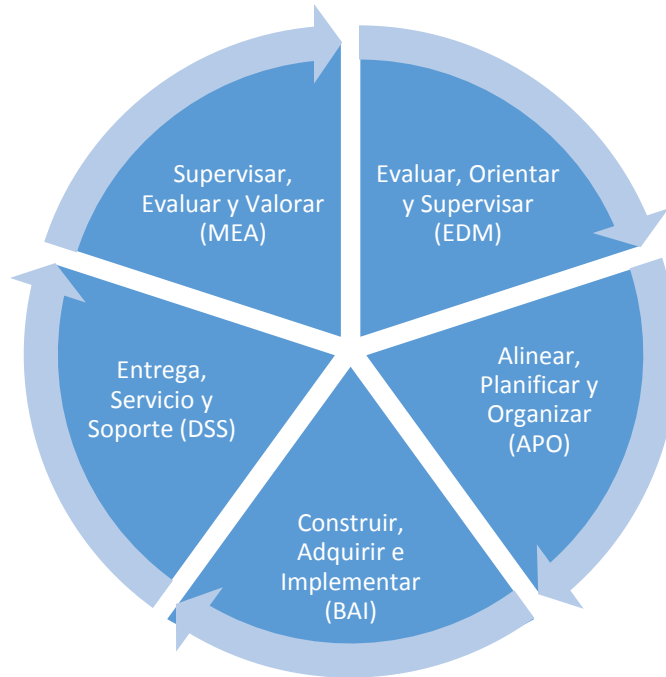
- Asegurar que se cumplan los requisitos legales, las obligaciones contractuales, regulatorias y derechos de propiedad intelectual por parte de SONDA.

Alcance. Esta política se aplica a todas las áreas y dependencias de SONDA, las cuales están sujetas a revisiones y auditorías regulares para asegurar el cumplimiento de las políticas y las normativas legales. Para esto, el Comité de Seguridad de la Información designará un responsable para el monitoreo, mejora continua, retroalimentación y cumplimiento de las políticas establecidas.

5.2.1.5 Ciclo de vida de las Políticas de Seguridad. Dado que estas políticas están alineadas a los objetivos corporativos se debe tener en cuenta que están susceptibles al cambio a medida que pasa el tiempo. Es conveniente validar las regulaciones que puedan llegar a existir así como de la evolución continua del negocio.

5.2.2 Procesos. En este numeral se definen los procesos COBIT 5 For Information Security aplicados al modelo de negocio SONDA, en donde representan tanto las necesidades del mismo como los objetivos y las métricas de medición de estos... (Véase Cuadros 9 al 55).

Figura 6. Procesos de COBIT



Fuente: Cobit 5 For Information Security

5.2.2.1 Evaluar, Orientar y Supervisar (EDM)

Cuadro 9. EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno

<p>Descripción del Proceso Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.</p>	
<p>Declaración del Propósito del Proceso: Proporcionar un enfoque consistente, integrado y alineado con el enfoque del gobierno de la empresa. Para garantizar que las decisiones relativas a TI se han adoptado en línea con las estrategias y objetivos de la empresa, garantizando la supervisión de los procesos de manera efectiva y clara, el cumplimiento con los requerimientos regulatorios y legales y que se han alcanzado los requerimientos de gobierno de los miembros del Consejo de Administración.</p>	
<p>EDM01 Metas y métricas del proceso específicas de seguridad</p>	
<p>Metas del proceso específicas de seguridad</p>	<p>Métricas relacionadas</p>

Cuadro 9. EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno. Continuación				
El sistema de gobierno de seguridad de la información está integrado en la empresa.	<p>Número de procesos de negocio y de TI en los que la seguridad de la información está integrada.</p> <p>Porcentaje de procesos y prácticas con clara trazabilidad a los principios de seguridad.</p> <p>Número de brechas de seguridad de la información relativas a no conformidades con las directrices de comportamiento ético y profesional</p>			
Se obtiene garantía sobre el sistema de gobierno de la seguridad de la información.	<p>Frecuencia de revisiones independientes del gobierno de la seguridad de la información</p> <p>Frecuencia de los informes sobre el gobierno de la seguridad de la información al comité ejecutivo y al consejo de administración</p> <p>Cumplimiento con el programa y revisiones internas y/o externas</p> <p>Número de no-conformidades</p>			
EDM01 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad				
Práctica de Gobierno	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
EDM01.01 Evaluar el sistema de gobierno. Identificar y comprometerse continuamente con las partes interesadas de la empresa, documentar la comprensión de los requerimientos y realizar una estimación del actual y futuro diseño del gobierno de TI de la empresa.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Factores internos y externos del entorno (obligaciones legales, regulatorias y contractuales) y tendencias	Principios que rigen la seguridad de la información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Analizar e identificar los factores del entorno internos y externos (obligaciones legales, regulatorias y contractuales) y las tendencias en el entorno del negocio que pueden influir en el diseño del gobierno de la seguridad de la información.				
Evaluar el grado en el que la seguridad de la información cumple con las necesidades de negocio y da cumplimiento con las obligaciones legales y regulatorias				
Articular los principios que guiarán el diseño de los catalizadores de la seguridad de la información y promoverán un entorno positivo de seguridad.				

Cuadro 9. EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno. Continuación

Comprender la cultura empresarial de la toma de decisiones y determinar el modelo óptimo de toma de decisiones para seguridad de la información.				
Práctica de Gobierno	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
EDM01.02 Orientar el sistema de gobierno. Informar a los líderes y obtener su apoyo, su aceptación y su compromiso. Guiar las estructuras, procesos y prácticas para el gobierno de TI en línea con los principios, modelos para la toma de decisiones y niveles de autoridad diseñados para el gobierno. Clasificar la información necesaria para una toma de decisiones informadas.	EDM01.01	Principios que rigen la de la información seguridad	Cultura y entorno positivo de seguridad de la información	Interno
	APO02.05	Estrategia de seguridad de la información		
Actividades específicas de seguridad (Adicionales a las Actividades de COBIT 5)				
Obtener el compromiso de la alta dirección con la seguridad de la información y la gestión de riesgos de la información.				
Asignar una función de seguridad de la información de alcance global dentro de la				
Asignar un comité de dirección de seguridad de la información (ISSC).				
Disponer procedimientos jerárquicos de notificación y de escalado de decisiones.				
Alinear la estrategia de seguridad de la información con la estrategia del negocio.				
Fomentar un entorno y cultura positivos de seguridad de la información.				

Cuadro 9. EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno. Continuación

Práctica de Gobierno	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
EDM01.03 Supervisar el sistema de gobierno. Supervisar la ejecución y la efectividad del gobierno de TI de la empresa. Analizar si el sistema de gobierno y los mecanismos implementados (incluyendo estructuras, principios y procesos) están operando de forma efectiva y proporcionan una supervisión apropiada de TI.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Legislación y regulación relacionada con la seguridad de la información	Evaluación de cumplimiento del sistema de gobierno	Interno
Actividades específicas de seguridad (Adicionales a las Actividades de COBIT 5)				
Supervisar los mecanismos ordinarios y rutinarios para garantizar que el uso de los sistemas de medida de la seguridad de la información cumplen con la legislación y regulación relacionada con la seguridad de la información. Analizar la totalidad de las implicaciones del cambiante contexto de las amenazas.				
Fuente: Cobit 5 For Information Security				

Cuadro 10. EDM02 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad

EDM02 Asegurar la Entrega de Beneficios
<p>Descripción del Proceso</p> <p>Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costes aceptables</p>

Cuadro 10. EDM02 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad. Continuación				
Declaración del Propósito del Proceso Asegurar un valor óptimo de las iniciativas de TI, servicios y activos disponibles; una entrega coste eficiente de los servicios y soluciones y una visión confiable y precisa de los costes y de los beneficios probables de manera que las necesidades del negocio sean soportadas efectiva y eficientemente.				
EDM02 Metas y Métricas del Proceso específicas de Seguridad				
Metas del Proceso específicas de		Métricas Relacionadas		
Los beneficios, costes y riesgos de las inversiones en seguridad de la información son equilibradas y gestionadas y contribuyen en su valor óptimo.		Porcentaje de reducción del riesgo frente a desviación del presupuesto (presupuestado frente a proyección)		
		Cantidad de nuevos clientes en el semestre vs cantidad de clientes en el semestre anterior.		
EDM02 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de				
Práctica de Gobierno	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
EDM02.01 Evaluar la optimización de valor. Evaluar continuamente las inversiones, servicios y activos del portafolio de TI para determinar la probabilidad de alcanzar los objetivos de la empresa y aportar valor a un coste razonable. Identificar y juzgar cualquier cambio de directrices que necesite ser comunicado a la dirección ejecutiva para optimizar la creación de valor.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Evaluación del alineamiento estratégico	Portafolio y catálogo de servicios actualizado	Interno
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
Identificar y registrar los requisitos de las partes interesadas (tales como accionistas, reguladores, auditores y clientes) para proteger sus intereses y aportar valor a través de la actividad de seguridad de la información. Establecer directrices en consonancia con lo anterior.				

Cuadro 10. EDM02 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad. Continuación

Práctica de Gobierno	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
EDM02.02 Orientar la optimización del valor. Orientar los principios y las prácticas de gestión de valor para posibilitar la materialización del valor óptimo de las inversiones habilitadas por TI a lo largo de todo su ciclo de vida económico.	Fuera del ámbito de COBIT 5 para Seguridad	Tipos y criterios de inversión	Tipos y criterios de inversión actualizados	Interno
	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Tipos y criterios de inversión	Tipos y criterios de inversión actualizados	Interno
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
Establecer un método para demostrar el valor de la seguridad de la información (incluyendo la definición y recolección de datos relevantes) para asegurar el uso eficiente de los activos existentes relacionados con la seguridad de la información.				
Asegurar el uso de medidas financieras y no financieras para describir el valor aportado por las iniciativas de seguridad de la información.				
Usar métodos enfocados al negocio para la comunicación del valor aportado por las iniciativas de seguridad de la información.				
Práctica de Gobierno	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
EDM02.03 Supervisar la optimización de valor. Supervisar los indicadores clave y sus métricas para determinar el grado en que el negocio está obteniendo el valor y los beneficios esperados de los servicios e inversiones habilitadas por TI.			Retroalimentación sobre el valor aportado por las iniciativas de seguridad de la información	Interno

Cuadro 10. EDM02 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad. Continuación				
Identificar los problemas significativos y considerar las acciones correctivas. Los beneficios esperados de los servicios e inversiones habilitadas por TI. Identificar los problemas significativos y considerar las acciones correctivas.			Retroalimentación sobre el valor aportado por las iniciativas de seguridad de la información	Interno
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
Seguir los resultados de las iniciativas de seguridad de la información y compararlos con las expectativas para asegurar la entrega de valor frente a los objetivos del negocio.				
Fuente: Cobit 5 For Information Security				

Cuadro 11. EDM03 Asegurar la Optimización del Riesgo

EDM03 Asegurar la Optimización del Riesgo	
<p>Descripción del Proceso Asegurar que la probabilidad de ocurrencia e impacto al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado, analizado y tratado.</p>	
<p>Declaración del Propósito del Proceso Asegurar que los riesgos relacionados con TI de la empresa sean gestionados garantizando un nivel apropiado de aceptación del riesgo. en el valor de la empresa se identifica y se gestiona y que el potencial fallo en el cumplimiento se reduce al mínimo</p>	
EDM03 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	Métricas Relacionadas
1. La gestión del riesgo asociado a la información forma parte de la gestión general de los riesgos corporativos (ERM).	Nivel de Riesgo de seguridad de la información relacionada con el nivel de riesgo del negocio. Nivel de Riesgo de negocio eficazmente mitigado con controles de seguridad de la información
EDM03 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad	

Cuadro 11. EDM03 Asegurar la Optimización del Riesgo. Continuación				
Práctica de Gobierno	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
EDM03.01 Evaluar la gestión de riesgos. Examinar y evaluar	Fuera del ámbito de COBIT 5	Indicadores clave del riesgo de la	Alineamiento de los KRIs de la empresa	EDM03.02
Cuadro 11. EDM03 Asegurar la Optimización del Riesgo. Continuación				
continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el nivel de riesgo de la empresa es apropiado y si el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado.	para Seguridad de la información	(KRIs) Orientación sobre nivel de riesgo de la empresa	con los KRIs de seguridad de la información	
			Nivel aceptable del riesgo de seguridad de la información	EDM03.02 EDM03.03
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
Determinar el nivel de riesgo corporativo al nivel del consejo de administración.				
Medir el nivel de integración de la gestión del riesgo de la información con el modelo general de ERM.				
Práctica de Gobierno	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
EDM03.02 Orientar la gestión de riesgos. Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que el riesgo TI actual no excede el nivel de riesgo del consejo de administración	EDM03.01	lineamiento de los KRIs de la empresa con los KRIs de seguridad de la información Nivel aceptable del riesgo de seguridad de la información	Políticas de gestión del riesgo actualizadas	Interno
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
Integrar la gestión del riesgo de la información con el modelo general de ERM.				

Cuadro 11. EDM03 Asegurar la Optimización del Riesgo. Continuación				
Práctica de Gobierno	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
EDM03.03 Supervisar la gestión de riesgos. Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su solución.	EDM03.01	Nivel aceptable del riesgo de seguridad de	Acciones correctivas para solventar las desviaciones en la gestión del riesgo	Interno
	APO01.03	Políticas de Seguridad de la información		
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
Supervisar el perfil del riesgo de la información de la compañía, para conseguir un equilibrio óptimo entre riesgos y oportunidades de negocio.				
Incluir los resultados de los procesos de gestión del riesgo de la información como entradas para el cuadro de mando de riesgos general de negocio.				
Fuente: Cobit 5 For Information Security				

Cuadro 12. EDM04 Asegurar la Optimización de Recursos

EDM04 Asegurar la Optimización de Recursos	
<p>Descripción del Proceso</p> <p>Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste adecuado.</p>	
<p>Declaración del Propósito del Proceso</p> <p>Asegurar que las necesidades de recursos de la empresa son cubiertas de un modo óptimo, que el coste TI es optimizado y que con ello se incrementa la probabilidad de la obtención de beneficios y la preparación para cambios futuros.</p>	
EDM04 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de	Métricas Relacionadas
Los recursos de seguridad de la información son optimizados.	Estudio comparativo del gasto en seguridad de la información en relación a años anteriores y/u organizaciones similares o buenas prácticas del sector. Costes de controles implementados en el año vs el año anterior

Cuadro 12. EDM04 Asegurar la Optimización de Recursos. Continuación				
Los recursos de la seguridad de la información están alineados con los requisitos del negocio.		Cuantía de la desviación respecto al presupuesto para seguridad de la información Porcentaje de reutilización de soluciones de seguridad de la información		
EDM04 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad				
Práctica de Gobierno	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
EDM04.01 Evaluar la gestión de recursos. Examinar y evaluar continuamente la necesidad actual y futura de los recursos relacionados con TI, las opciones para la asignación de recursos (incluyendo estrategias de aprovisionamiento) y los principios de asignación y gestión para cumplir de manera con las necesidades de la empresa.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Plan de recursos aprobado	Recursos de seguridad de la información actualizados	Interno
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
Evaluar la eficacia de los recursos de seguridad de la información en términos de suministro, formación, concienciación y competencias de los recursos necesarios en comparación con las necesidades del negocio.				
Práctica de Gobierno	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
EDM04.02 Orientar la gestión de recursos. Asegurar la adopción de principios de gestión de recursos	Fuera del ámbito de COBIT 5 para Seguridad	Asignación de responsabilidades para la gestión de recursos	Recursos de seguridad de la información actualizados	Interno

Cuadro 12. EDM04 Asegurar la Optimización de Recursos. Continuación				
para permitir un uso óptimo de los recursos de TI a lo largo de su completo ciclo de vida.	de la Información			
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
Asegurar que la gestión de los recursos de seguridad de la información está alineada con las necesidades del negocio.				
Práctica de Gobierno	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
EDM04.03 Supervisar la gestión de recursos. Supervisar los objetivos y métricas clave de los procesos de gestión de recursos y establecer cómo serán identificados, seguidos e informados para su resolución las desviaciones o los problemas.			Acciones correctivas para solventar las desviaciones en la gestión de los recursos	Interno
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
Medir la eficacia, eficiencia y capacidad de los recursos de seguridad de la información respecto a las necesidades del negocio.				
Fuente: Cobit 5 For Information Security				

Cuadro 13. EDM05 asegurar la transparencia hacia las partes interesadas

EDM05 Asegurar la Transparencia hacia las Partes Interesadas
<p>Descripción del Proceso Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de TI de la empresa son transparentes, con aprobación por parte de las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.</p>
<p>Declaración del Propósito del Proceso Asegurar que la comunicación con las partes interesadas sea efectiva y oportuna y que se ha establecido una base para la elaboración de informes con el fin de aumentar el desempeño, identificar áreas susceptibles de mejora y confirmar que las estrategias y los objetivos relacionados con TI concuerdan con la estrategia corporativa.</p>

Cuadro 13. EDM05 asegurar la transparencia hacia las partes interesadas. Continuación				
EDM05 Metas y Métricas del Proceso específicas de Seguridad				
Metas del Proceso específicas de Seguridad		Métricas Relacionadas		
Se ha establecido un protocolo informativo completo, oportuno y preciso sobre la seguridad de la información.		Cantidad de informes entregados dentro del plazo previsto. Porcentaje de informes con datos validados.		
Las partes interesadas se encuentran informadas de la situación actual de la seguridad y de los riesgos de la información de toda la organización.		Grado de satisfacción de las partes interesadas con el protocolo informativo sobre la seguridad de la información (oportuno, completo, relevante, fiable, preciso, etc.) y su frecuencia, basado en encuestas.		
EDM05 Prácticas, Entradas /Salidas y Actividades del Proceso específicas de				
Práctica de Gobierno	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas. Examinar y juzgar continuamente los requisitos actuales y futuros de comunicación con las partes interesadas y de la elaboración de informes, incluyendo tanto los requisitos obligatorios (p.ej. de regulación)de elaboración de informes, como la comunicación a otros interesados. Establecer los principios de la comunicación.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Evaluación de los requisitos corporativos de elaboración de informes	Requisitos de elaboración de informes y canales de comunicación de Seguridad de la Información	Interno
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
Determinar la audiencia, incluyendo individuos y grupos internos o externos, para la				
Identificar los requisitos para la elaboración de informes de seguridad de la información a las partes interesadas (p.ej., qué información es requerida, cuándo es requerida y cómo es presentada).				
Estableceros medios y canales adecuados con las personas interesadas y responsables de la seguridad de la información.				

Cuadro 13. EDM05 asegurar la transparencia hacia las partes interesadas. Continuación

Práctica de Gobierno	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes. Garantizar el establecimiento de una comunicación y una elaboración de informes eficaces, incluyendo mecanismos para asegurar la calidad y la completitud de la información, vigilar la elaboración de informes y crear una estrategia de comunicación con las partes interesadas.			Informes de estado de la Seguridad de la Información	Interno
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
Priorizar la notificación de problemas de seguridad de la información a las partes interesadas.				
Realizar auditorías internas y externas para evaluar la eficacia del programa de gobierno de la seguridad de la información.				
Elaborar informes de estado de la seguridad de la información de forma regular para las partes interesadas que incluyan información de las actividades de seguridad, desempeño, logros, perfiles de riesgo, beneficios de negocio, temas 'calientes' (p.ej. computación en la nube, productos de consumo) riesgos destacados (incluyendo cumplimiento y auditoría) e insuficiencias de capacidad.				
Práctica de Gobierno	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
EDM05.03 Supervisar la comunicación con las partes interesadas. Supervisar la eficacia de la comunicación con las partes interesadas. Evaluar los mecanismos para asegurarla precisión, la fiabilidad y la eficacia y determinar si se están cumpliendo los requisitos de los diferentes interesados			Supervisión y elaboración de informes de Seguridad de la Información	Interno

Cuadro 13. EDM05 asegurar la transparencia hacia las partes interesadas. Continuación
1. Definir la supervisión y elaboración de informes de seguridad de la información (p.ej., utilizando indicadores clave de desempeño [KPIs] para la seguridad de la información y la gestión de riesgos de la información que estén basados en métricas y medidas del dominio MEA)
Fuente: Cobit 5 For Information Security

5.2.2.2 Alinear, Planificar y Organizar (APO)

Cuadro 14. APO01 Gestionar el Marco de Gestión de TI

APO01 Gestionar el Marco de Gestión de TI				
Descripción del Proceso de COBIT 5 Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.				
Declaración del Propósito del Proceso de COBIT 5 Proporcionar un enfoque de gestión consistente que permita cumplir los requisitos de gobierno corporativo e incluya procesos de gestión, estructuras, roles y responsabilidades organizativos, actividades fiables y reproducibles y habilidades y competencias.				
APO01 Metas y Métricas del Proceso específicas de Seguridad				
Metas del Proceso específicas de Seguridad		Métricas Relacionadas		
1. Se ha establecido y comunicado eficazmente la integración de la seguridad de la información con los marcos de TI y de negocio que operan en la empresa.		- Porcentaje de actividades de apoyo al alineamiento dentro del portafolio de la estrategia de seguridad de la información que resultan alineadas con la estrategia de negocio.		
APO01 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO01.01 Definir la estructura organizativa. Establecer una estructura interna y extensa que refleje las necesidades del negocio y las prioridades de TI	EDM01.01	Principios que rigen la seguridad de la información	Estructura y mandato del ISSC	Interna

Cuadro 14. APO01 Gestionar el Marco de Gestión de TI. Continuación				
Implementar las estructuras de dirección requeridas (p. ej., comités) para permitir que la toma de decisiones de gestión se lleve a cabo de la forma más eficaz y eficiente posible.				
	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Estrategia de TI Normas y directrices de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Alinear la organización relativa a la seguridad de la información con los modelos				
Establecer un ISSC (o equivalente).				
Definir la función de seguridad de la información, incluyendo roles internos y externos, capacidades y derechos de decisión requeridos.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO01.03 Mantener los catalizadores del sistema de gestión. Mantener los catalizadores del sistema de gestión y del entorno de control para las TI de la empresa y garantizar que están integrados y alineados con la filosofía y el estilo operativo de gobierno y de gestión de la empresa. Dichos catalizadores incluyen una comunicación clara de expectativas/requisitos. El sistema de gestión debería fomentar la cooperación interdepartamental y el trabajo en equipo, promover el cumplimiento y la mejora continua y tratar las desviaciones en el proceso (incluidos los fallos).	EDM01.01	Principios que rigen la seguridad de la información	Políticas de seguridad de la información y afines	EDM03.03 APO07.01 APO07.06 APO12.01 BAI01.01 BAI01.11 BAI02.01 BAI03.08 BAI05.01 BAI06.01 DSS01.02 DSS02.01 MEA01.01 MEA02.01
	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Reglas y regulaciones relativas a la seguridad de la información Normas y directrices de seguridad de la información		

Cuadro 14. APO01 Gestionar el Marco de Gestión de TI. Continuación				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Considerar el entorno interno de la empresa, incluyendo la cultura y la filosofía de la gestión, la tolerancia al riesgo, los valores éticos, el código de conducta, la rendición de cuentas y los requisitos de seguridad de la información.				
Alinearse con las normas y códigos de buenas prácticas de seguridad de la información aplicable, nacional e internacional, y evaluar las buenas prácticas disponibles de seguridad de la información.				
Desarrollar políticas de seguridad de la información y afines, teniendo en cuenta los requisitos de negocio, y el cumplimiento a las obligaciones legales, regulatorios y contractuales de seguridad, las políticas organizativas de alto nivel y el entorno interno de la empresa.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO01.04 Comunicar los objetivos y la dirección de gestión. Comunicar la sensibilización y la comprensión de los objetivos y la dirección de TI a las partes interesadas y usuarios pertinentes a lo largo de toda la empresa.	EDM01.0 1	Principios que rigen la seguridad de la información	Programa de formación y concienciación en seguridad de la información	APO02.0 6 BAI08.01
	APO02.0 6	Comunicación de los objetivos de la seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Definir las expectativas en relación a la seguridad de la información, incluyendo la ética y la cultura específica de la organización.				
Desarrollar un programa de concienciación en seguridad de la información.				
Establecer métricas para medir los comportamientos en relación a la seguridad de la información.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO01.06 Definir la propiedad de la información (datos) y de los sistemas. Definir y mantener las responsabilidades sobre la propiedad				

Cuadro 14. APO01 Gestionar el Marco de Gestión de TI. Continuación				
dad de los activos de información y los sistemas de información. Asegurar que los propietarios toman decisiones sobre la clasificación de la información y los sistemas y sobre su protección de acuerdo con esta clasificación.	Interno	Definición de la función de seguridad de la información y su ubicación en la empresa	Roles y responsabilidades de seguridad de la información	APO11.0 1
			Directrices de clasificación de información	DSS05.0 2
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir la propiedad de sistemas y datos al nivel de la empresa dentro de los procesos de gestión de seguridad de la información.				
2. Asignar custodios de seguridad de la información en los procesos de gestión de seguridad de la información.				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO01.07 Gestionar la mejora continua de los procesos. Evaluar, planificar y ejecutar la mejora continua de los procesos y su madurez para asegurar que son capaces de entregarse conforme a los objetivos de la empresa, de gobierno, de gestión y de control.	MEA01.04	Planes de acciones correctivas y preventivas actualizados, cumplimiento de los objetivos de seguridad y revisión por la dirección de las políticas, controles técnicos, administrativos de seguridad de la información	Documentación sobre procesos, tecnología y aplicaciones y normalización Formación del equipo de seguridad de la información	Interna
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Considerar formas de mejorar la eficiencia y la eficacia de la función de seguridad de la información, p.ej., mediante la formación del equipo de seguridad de la información; la documentación de procesos, tecnología y aplicaciones; y la normalización y la automatización del proceso.				

Cuadro 14. APO01 Gestionar el Marco de Gestión de TI. Continuación				
Revisar los informes (tales como los informes de auditoría y las evaluaciones de riesgo) que detallan las debilidades en los controles y procesos de seguridad de la información.				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO01.08 Mantener el cumplimiento con las políticas y procedimientos. Poner en marcha procedimientos para mantener el cumplimiento y la medición del funcionamiento de las políticas y otros catalizadores del marco de referencia; hacer cumplir las consecuencias del no cumplimiento o del desempeño inadecuado. Hacer un seguimiento de las tendencias y del rendimiento y considerarlos en el diseño futuro y la mejora del marco de control.	APO02.06 Fuera del ámbito de COBIT 5 para Seguridad de la Información	Plan de seguridad de la información Objetivos de la Organización Reglas y regulaciones relativas a la seguridad de la información Normas y directrices de seguridad de la información	Evaluación del cumplimiento de seguridad de la información	APO02.02 APO12.01
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Planificar y realizar evaluaciones periódicas para determinar el cumplimiento de las políticas y procedimientos de seguridad de la información.				
<p>Objetivos de la organización</p> <p>Reglas y regulaciones relativas a la seguridad de la información</p> <p>Normas y directrices de seguridad de la información</p>				
Fuente: Cobit 5 For Information Security				

Cuadro 15. APO02 Gestionar la Estrategia

APO02 Gestionar la Estrategia	
<p>Descripción del Proceso de COBIT 5 Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos.</p>	
<p>Declaración del Propósito del Proceso de COBIT 5 Alinear los planes estratégicos de TI con los objetivos del negocio. Comunicar claramente los objetivos y las cuentas asociadas para que sean comprendidos por todos, con la identificación de las opciones estratégicas de TI, estructurados e integrados con los planes de negocio.</p>	
<p>APO02 Metas y Métricas del Proceso específicas de Seguridad</p>	
Metas del Proceso específicas de	Métricas Relacionadas
<p>1. Se define y mantiene un marco de política de seguridad de la información.</p>	<p>Número de actualizaciones de la política de seguridad de la información Aprobación de la política de seguridad de la información por la Dirección</p>
<p>2. Existe una estrategia integral de seguridad de la información y está alineada con la estrategia general de la empresa y de TI.</p>	<p>Porcentaje de iniciativas de seguridad de la información completadas frente a las planeadas</p>
<p>3. La estrategia de seguridad de la información es rentable, apropiada, realista, factible, orientada a la empresa y equilibrada.</p>	<p>Porcentaje y número de iniciativas para las que se ha calculado una métrica de valor (p.ej., el retorno de la inversión [ROI]) Datos de las encuestas de satisfacción de los grupos de interés de la empresa sobre la eficacia de la estrategia de seguridad de la información</p>
<p>4. La estrategia de seguridad de la información está alineada con las metas y objetivos estratégicos de la empresa a largo plazo</p>	<p>Porcentaje de proyectos en los portafolios de proyectos de la empresa y de TI que incluyen seguridad de la información Porcentaje de iniciativas/proyectos de TI en que los requisitos de seguridad de la información están promovidos por los propietarios de negocio</p>
<p>APO02 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad</p>	

Cuadro 15. APO02 Gestionar la Estrategia. Continuación.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO02.01 Comprender la dirección de la empresa. Considerar el entorno actual y los procesos de negocio de la empresa, así como	EDM01.01	Principios que rigen la seguridad de la información	Fuentes de alto nivel y prioridades para los cambios	APO02.02
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Comprender cómo la seguridad de la información debería apoyar los objetivos generales de la empresa y proteger los intereses de las partes implicadas teniendo en cuenta la necesidad de gestionar el riesgo de la información, al tiempo que se cumplen los requisitos de conformidad legal y regulatoria y se aporta valor a la empresa.				
2. Comprender la vigente arquitectura de empresa e identificar las deficiencias potenciales de seguridad de la información.				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO02.02 Evaluar el entorno, capacidades y rendimiento actuales. Evaluar el rendimiento de las actuales capacidades internas de negocio y de TI, así como el de los servicios externos de TI; y desarrollar una perspectiva de la arquitectura empresarial en relación a TI. Identificar los problemas que se están experimentando y generar recomendaciones en las áreas que pueden beneficiarse de estas mejoras. Considerar los aspectos diferenciadores y las opciones de los proveedores de servi -	APO01.08	Evaluación de cumplimiento de la seguridad de la información	Capacidades de seguridad de la información	APO02.03 APO04.04 APO08.05 APO09.05 APO11.01 BAI01.01 BAI02.01 BAI04.01

Cuadro 15. APO02 Gestionar la Estrategia. Continuación.				
cios, y el impacto financiero, los costes y beneficios potenciales de utilizar servicios externos.	APO02.01	Fuentes de alto nivel y prioridades para los cambios		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir unas capacidades básicas de seguridad de la información.				
2. Crear criterios de seguridad de la información pertinentes y claros para identificar el riesgo y priorizar las deficiencias a tratar.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO02.03 Definir las capacidades objetivo para TI. Definir las capacidades objetivo para el negocio y para TI y los servicios de TI necesarios. Esto debería estar basado en el entendimiento del entorno empresarial y sus necesidades.	APO02.02	Capacidades de seguridad de la información	Necesidades de seguridad de la información en las capacidades objetivo para TI	APO02.04
	BAI02.01	Necesidades de seguridad de la información		
	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Normas y regulaciones de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Garantizar que los requisitos de seguridad de la información se incluyen en la definición de las capacidades objetivo para TI.				
2. Definir el estado objetivo para la seguridad de la información.				
3. Definir y consensuar el impacto de los requisitos de seguridad de la información en la arquitectura de la empresa, considerando a las partes interesadas pertinentes.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO02.05 Definir el plan estratégico y la hoja de ruta. Crear un plan estratégico que defina, en cooperación con las partes interesadas relevantes, como los	EDM01.01	Principios que rigen la seguridad de la información	Estrategia de seguridad de la información	EDM01.02 APO01.08 APO03.01

Cuadro 15. APO02 Gestionar la Estrategia. Continuación.				
<p>los objetivos estratégicos de la empresa. Incluyendo cómo TI apoyará el programa aprobado de inversiones, los procesos de negocio, los servicios y los activos de TI. Orientar las tecnologías para definir las iniciativas que se requieren para cubrir las diferencias, la estrategia de abas tecimiento y las medidas que se utilizarán para supervisar el logro de los objetivos, para dar prioridad a las iniciativas y combinarlas en una hoja de ruta a alto nivel.</p>	EDM01.01	Principios que rigen la seguridad de la información	Estrategia de seguridad de la información	EDM01.02 APO01.08 APO03.01
	APO13.02	Casos de negocio de seguridad de la información	Hoja de ruta estratégica de seguridad de la información	BAI05.04
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir la estrategia de seguridad de la información y alinearla con las estrategias de TI y de negocio y con los objetivos globales corporativos.				
2. Garantizar que la estrategia y la hoja de ruta actuales de TI tienen en consideración los requisitos de seguridad de la información.				
3. Crear un plan de acción que incluya una planificación tentativa, interdependencias entre las iniciativas y métricas (el qué) y objetivos (el cuánto) que puedan relacionarse con los beneficios corporativos.				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO02.06 Comunicar la estrategia y la dirección de TI. Crear conciencia y comprensión	APO01.04	Programa de formación y concienciación en seguridad de la información	Comunicación de los objetivos de seguridad de la información	APO01.04 APO01.08 APO04.04 APO04.05 APO07.01

del negocio y de los objetivos y dirección de TI, como se encuentra reflejada en la estrategia de TI, a través de comunicaciones a las partes interesadas actuales y a los usuarios de toda la empresa.	APO01.04	Programa de formación y concienciación en seguridad de la información	Comunicación de los objetivos de seguridad de la información	APO07.05 APO07.06 APO09.05 APO11.01
			Plan de seguridad de la información	BAI01.01 BAI01.04 BAI01.08 BAI01.11 BAI02.01 BAI05.03 BAI05.04
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir el plan de seguridad de la información, identificando las consecuencias prácticas para la empresa de la seguridad de la información.				
2. Comunicar la estrategia de seguridad de la información y el plan de seguridad de la información a la empresa y a todas las partes interesadas pertinentes.				
3. Dar a conocer la función de seguridad de la información dentro de la empresa, y fuera de ella si es pertinente.				
Fuente: Cobit 5 For Information Security				

Cuadro 16. APO03 Gestionar la Arquitectura Empresarial

APO03 Gestionar la Arquitectura Empresarial
<p>Descripción del Proceso de COBIT 5 Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Definir los requisitos para la taxonomía, las normas, las directrices, los procedimientos, las plantillas y las herramientas y proporcionar un vínculo para estos componentes. Mejorar la adecuación, aumentar la agilidad, mejorar la calidad de la información y generar ahorros de costes potenciales mediante iniciativas tales como la reutilización de bloques de componentes para los procesos de construcción.</p>
<p>Declaración del Propósito del Proceso de COBIT 5 Representar a los diferentes módulos que componen la empresa y sus interrelaciones, así como los principios rectores de su diseño y evolución en el tiempo, permitiendo una entrega estándar, sensible y eficiente de los objetivos operativos y estratégicos.</p>
<p>APO03 Metas y Métricas del Proceso específicas de Seguridad</p>

Cuadro 16. APO03 Gestionar la Arquitectura Empresarial. Continuación.				
Metas del Proceso específicas de Seguridad		Métricas Relacionadas		
1. Los requisitos de seguridad de la información se han incorporado a la arquitectura de la empresa y se han traducido en una arquitectura de seguridad formalizada.		Número de excepciones a los estándares de arquitectura de seguridad de la información		
2. La arquitectura de seguridad de la información se entiende como parte de la arquitectura general de la empresa.		Número de desviaciones entre la arquitectura de seguridad de la información y la arquitectura de la empresa		
3. La arquitectura de seguridad de la información está alineada con la arquitectura de la empresa y evoluciona según cambia ésta.		Fecha de la última revisión y/o actualización de los controles de seguridad de la información aplicados a la arquitectura de la empresa		
4. Se utilizan un marco y una metodología de arquitectura de seguridad de la información para permitir la reutilización de componentes de seguridad de la información entre distintas partes de la empresa.		Porcentaje de proyectos que utilizan el marco y la metodología de arquitectura de seguridad de la información Número de personas formadas en el marco y la metodología de seguridad de la información.		
APO03 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO03.01 Desarrollar la visión de la arquitectura de empresa. La visión de la arquitectura proporciona una primera descripción de alto nivel de las arquitecturas de partida y objetivo, cubriendo los dominios de negocio, información, datos, aplicaciones y tecnología. La visión de la arquitectura proporciona al promotor la herramienta clave para vender los beneficios de la capacidad propuesta a las partes interesadas de la empresa	APO02.04	Análisis comparativo de la capacidad de seguridad de la información	Visión de arquitectura de seguridad de la información Propuesta de valor, metas y métricas de seguridad de la información	Interno
	APO02.05	Estrategia de seguridad de la información		

Cuadro 16. APO03 Gestionar la Arquitectura Empresarial. Continuación.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir los objetivos y requisitos de seguridad de la información para la arquitectura de empresa.				
2. Definir la propuesta de valor de la seguridad de la información así como las metas y métricas afines.				
3. Tener en cuenta las buenas prácticas del sector al construir la visión de la arquitectura de seguridad de la información.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO03.02 Definir la arquitectura de referencia. La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Arquitectura de empresa	Definición de la arquitectura deseada de la seguridad de la información	APO03.03
			Descripciones de partida de los dominios y definición de la arquitectura	APO13.02
			Modelo de la arquitectura de la información	DSS05.04 DSS05.06
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar la inclusión de elementos, políticas y normas de seguridad de la información en el repositorio de arquitectura.				
2. Asegurar que la seguridad de la información se encuentra integrada a lo largo de todos los dominios de la arquitectura (p. ej., negocio, información, datos, aplicaciones, tecnología).				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO03.03 Seleccionar las oportunidades y las soluciones. Racionalizar las desviaciones entre las arquitecturas de referencia y objetivo, considerando tanto la perspectiva técnica				

Cuadro 16. APO03 Gestionar la Arquitectura Empresarial. Continuación.				
como la del negocio y agrupándolas en paquetes de trabajo de proyecto. Integrar el proyecto con todos los programas de inversiones relacionados con TI para asegurar que las iniciativas relacionadas con la arquitectura estén alineadas y que, estas iniciativas, sean parte del cambio general en la empresa. Hacer de ello un esfuerzo en colaboración con las partes interesadas clave de la empresa y en TI para evaluar el grado de preparación de la empresa para su transformación e identificar oportunidades.	APO03.02	Definición de la arquitectura deseada de seguridad de la información	Estrategia de migración y puesta en marcha de la arquitectura de seguridad de la información	APO03.04
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar la inclusión de los requisitos de seguridad de la información cuando se analicen carencias y cuando se seleccionen soluciones para la empresa.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO03.04 Definir la implementación de la arquitectura. Crear un plan de implementación y de migración viable, acorde con la cartera de proyectos y programas.	APO03.03	Estrategia de implementación y migración de la arquitectura de seguridad de la información	Arquitectura de seguridad de la información y plan de implementación del servicio detallados	Interno

Cuadro 16. APO03 Gestionar la Arquitectura Empresarial. Continuación.				
Asegurar que el plan está estrechamente coordinado para asegurar que se aporta valor y se disponen de los recursos necesarios para finalizar los trabajos.	APO03.03	Estrategia de implementación y migración de la arquitectura de seguridad de la información	Arquitectura de seguridad de la información y plan de implementación del servicio detallados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Alinear la seguridad de la información con la arquitectura de TI.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO03.05 Proveer los servicios de arquitectura empresarial. La provisión de los servicios de arquitectura de empresa incluye la guía y supervisión de los proyectos a implementar, la formalización de las maneras de trabajar mediante los contratos de arquitectura, la medición y comunicación del valor añadido por la arquitectura y la supervisión del cumplimiento.			Guía para la puesta en marcha de servicios de arquitectura de seguridad de la información	DSS01.01
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir normas de seguridad de la información y diseñar patrones en apoyo a la arquitectura empresarial.				
2. Asegurar que cualquier adquisición tecnológica o actividad de cambio en el negocio incluye revisiones de seguridad de la información para confirmar que se cumplen los requisitos de seguridad de la información.				
Fuente: Cobit 5 For Information Security				

Cuadro 17. APO04 Gestionar la Innovación

APO04 Gestionar la Innovación				
<p>Descripción del Proceso de COBIT 5 Mantener un conocimiento de la tecnología de la información y las tendencias relacionadas con el servicio, identificar las oportunidades de innovación y planificar la manera de beneficiarse de la innovación en relación con las necesidades del negocio. Analizar cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI, así como a través de las tecnologías ya existentes y por la innovación en procesos empresariales y de TI. Influir en la planificación estratégica y en las decisiones de la arquitectura de empresa.</p>				
<p>Declaración del Propósito del Proceso de COBIT 5 Lograr ventaja competitiva, innovación empresarial y eficacia y eficiencia operativa mejorada mediante la explotación de los desarrollos tecnológicos para la explotación de la información.</p>				
APO04 Metas y Métricas del Proceso específicas de Seguridad				
Metas del Proceso específicas		Métricas Relacionadas		
1. Se promueve la innovación dentro del programa de seguridad de la información.		Porcentaje del presupuesto asignado a investigación y desarrollo en seguridad de la información		
2. Se tienen en cuenta los requisitos de seguridad de la información cuando se habilita la innovación.		Número de puestos que incluyen aspectos de innovación		
APO04 Security-specific Process Practices, Inputs/Outputs and Activities				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO04.01 Crear un entorno favorable para la innovación. Crear un entorno que sea propicio para la innovación, considerando la cultura, la gratificación, la colaboración, los foros tecnológicos y los mecanismos para promover y captar ideas de los empleados.			Plan de innovación en seguridad de la información	APO04.06

Cuadro 17. APO04 Gestionar la Innovación. Continuación				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Mantener políticas y principios de seguridad de la información que respalden la innovación, al tiempo que se gestiona el riesgo de la información.				
2. Establecer enlaces con la investigación y otros servicios de asesoramiento en seguridad.				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO04.02 Mantener un entendimiento del entorno de la empresa. Trabajar junto a las partes interesadas relevantes para entender sus retos. Mantener un entendimiento adecuado de la estrategia corporativa y del entorno competitivo, así como de otras restricciones de modo que las oportunidades habilitadas por las nuevas tecnologías puedan ser identificadas.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Investigación externa	Evaluaciones de impacto de nuevas iniciativas en la seguridad de la información	Interna
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Comprender, en todo momento, los catalizadores de la seguridad de la información para identificar oportunidades y limitaciones de la innovación tecnológica.				
2. Determinar los efectos e impacto de las innovaciones en la tecnología, el entorno y la seguridad de la información.				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO04.03 Supervisar y explorar el entorno tecnológico. Realizar una supervisión sistemática				

Cuadro 17. APO04 Gestionar la Innovación. Continuación				
<p>y una exploración del entorno externo a la empresa para identificar tecnologías emergentes que tengan el potencial de crear valor (por ejemplo, materializando la estrategia corporativa, optimizando costos, evitando la obsolescencia y habilitando de una mejor manera los procesos corporativos y de TI). Supervisar el mercado, la competencia, sectores industriales y tendencias legales y regulatorias para poder analizar tecnologías emergentes o ideas innovadoras en el contexto empresarial.</p>	<p>Fuera del ámbito de COBIT 5 para Seguridad de la Información</p>	<p>Investigación externa</p>	<p>Tendencias emergentes identificadas en seguridad de la información</p>	<p>APO08.02</p>
<p>Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)</p>				
<p>1. Llevar a cabo investigación y una exploración del entorno externo para identificar tendencias emergentes en seguridad de la información.</p>				
<p>2. Fomentar la realimentación de las partes interesadas sobre la innovación en seguridad de la información.</p>				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
<p>APO04.04 Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras. Analizar las tecnologías emergentes identificadas y/o otras sugerencias de innovación TI. Trabajar con las</p>	APO02.02	Capacidades de	<p>Evaluación del cumplimiento de los requisitos de seguridad de la información</p>	<p>APO04.05</p>
	APO02.06	Plan de seguridad de la información		

Cuadro 17. APO04 Gestionar la Innovación. Continuación				
partes interesadas para validar los supuestos sobre el potencial de las nuevas tecnologías y la innovación.	BAI02.01	Requisitos de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Evaluar las innovaciones identificadas en base a los catalizadores de seguridad de la información.				
2. Apoyar las actividades de prueba de concepto para iniciativas de innovación, con el objetivo de asegurar la cobertura de los requisitos de seguridad de la información. Evaluar el cumplimiento de estos requisitos.				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO04.05 Recomendar iniciativas apropiadas adicionales. Evaluar y supervisar los resultados de las pruebas de concepto y, si son favorables, generar recomendaciones para más iniciativas y obtener el soporte de las partes interesadas.	APO02.06 APO04.04	Plan de seguridad de la información Evaluación del cumplimiento de los requisitos de seguridad de la información	Recomendaciones en seguridad de la información a partir de los resultados de la prueba de concepto	Interna
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Proporcionar asesoramiento en seguridad de la información a partir de los resultados de las pruebas de concepto de iniciativas de innovación de TI.				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO04.06 Supervisar la im-	APO04.01			

Cuadro 17. APO04 Gestionar la Innovación. Continuación				
plementación y el uso de la innovación. Supervisar la implementación y el uso de las tecnologías emergentes durante la integración, adopción y durante todo el ciclo de vida económico para garantizar que se producen los beneficios prometidos y para identificar las lecciones aprendidas	APO04.01	Plan de innovación en seguridad de la información	Planes de innovación ajustados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Medir los beneficios y riesgos para la seguridad durante la prueba de concepto y otras actividades de innovación.				
Fuente: Cobit 5 For Information Security				

Cuadro 18. APO05 Gestionar el Portafolio

APO05 Gestionar el Portafolio
<p>Descripción del Proceso de COBIT 5 Ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación. Evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos así como en su valor y riesgo corporativo. Mover los programas seleccionados al portafolio de servicios activos listos para ser ejecutados. Supervisar el rendimiento global del portafolio de servicios y programas proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas.</p>
<p>Declaración del Propósito del Proceso de COBIT 5 Optimizar el rendimiento del portafolio global de programas en respuesta al rendimiento de programas y servicios y a las cambiantes prioridades y demandas corporativas.</p>
APO05 Metas y Métricas del Proceso específicas de Seguridad

Cuadro 18. APO05 Gestionar el Portafolio. Continuación				
Metas del Proceso específicas de Seguridad		Métricas Relacionadas		
1. Las inversiones en seguridad de la información están asignadas según la tolerancia al riesgo.		Número de casos de negocio de inversión en seguridad de la información que no realizan evaluaciones de riesgo		
2. Los cambios en el programa de seguridad de la información se reflejan en los portafolios relevantes de servicios, activos y recursos de TI.		Porcentaje de cambios del programa de seguridad de la información reflejado en los portafolios relevantes		
APO05 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO05.01 Establecer la combinación deseada de inversiones. Revisar y garantizar la claridad de las estrategias y servicios actuales corporativos y de TI. Definir una adecuada combinación de inversiones, basada en los costes, la alineación con la estrategia y medidas financieras, tales como coste y retorno esperado de la inversión a lo largo de todo el ciclo de vida económico, grado de riesgo y tipo de beneficio para los programas del portafolio.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Evaluación del riesgo	Combinación deseada de inversiones en seguridad de la información	APO05.02
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir la combinación deseada de inversiones en seguridad de la información, teniendo en cuenta el riesgo para la empresa, los beneficios financieros y no financieros y el potencial retorno de las iniciativas.				

Cuadro 18. APO05 Gestionar el Portafolio. Continuación				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO05.02 Determinar la disponibilidad y las fuentes de fondos. Determinar las fuentes potenciales de fondos, las diferentes opciones de financiación y las implicaciones de las fuentes de financiación sobre las expectativas de retorno de la inversión.	APO05.01	Combinación deseada de inversiones en seguridad de la información	Opciones de financiación	APO05.03
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Revisar las posibilidades internas y externas para cubrir los recursos necesarios de seguridad de la información.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO05.03 Evaluar y seleccionar los programas a financiar. A partir de los requisitos de la combinación de inversiones del portafolio general, evaluar y priorizar casos de negocio de programas y decidir sobre las propuestas de inversión. Asignar fondos e iniciar los programas.	APO05.02	Opciones de financiación	Programa de seguridad de la información	Interna
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar la existencia de un programa de seguridad de la información.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO05.04 Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversión	Interno			Interno

Cuadro 18. APO05 Gestionar el Portafolio. Continuación				
Periódicamente, supervisar y optimizar, el rendimiento del portafolio de inversiones y de los programas individuales, a lo largo de todo el ciclo de vida de dichas inversiones.	Interno			Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No son necesarias guías específicas sobre seguridad de la información para esta práctica. Las actividades genéricas de COBIT 5 pueden ser utilizadas como guía adicional.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO05.05 Mantener los portafolios. Mantener los portafolios de programas y proyectos de inversión, servicios de TI y activos de TI.	Interno			Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No son necesarias guías específicas sobre seguridad de la información para esta práctica. Las actividades genéricas de COBIT 5 pueden ser utilizadas como guía adicional.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO05.06 Gestionar la consecución de beneficios. Supervisar los beneficios de proporcionar y mantener servicios y capacidades TI apropiadas sobre la				
Cuadro 18. APO05 Gestionar el Portafolio. Continuación				
base del caso de negocio acordado en vigor.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Presupuesto del programa	Perfil actualizado del riesgo de seguridad de la información	Interna

Cuadro 18. APO05 Gestionar el Portafolio. Continuación
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)
1. Proporcionar información sobre el logro de la confidencialidad, la integridad y la disponibilidad de la información, como entrada a la gestión de la consecución de beneficios.
2. Evaluar los cambios en el perfil de riesgo de seguridad de la información, para ilustrar la consecución de beneficios.
Fuente: Cobit 5 For Information Security

Cuadro 19. APO06 Gestionar el Presupuesto y los Costes

APO06 Gestionar el Presupuesto y los Costes	
<p>Descripción del Proceso de COBIT 5 Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuesto, coste y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costes a la empresa. Consultar a las partes interesadas para identificar y controlar los costes totales y los beneficios en el contexto de los planes estratégicos y tácticos de TI, e iniciar acciones correctivas cuando sea necesario.</p>	
<p>Declaración del Propósito del Proceso de COBIT 5 Fomentar la colaboración entre TI y las partes interesadas de la empresa para catalizar el uso eficaz y eficiente de los recursos relacionados con las TI y brindar transparencia y responsabilidad sobre el coste y valor de negocio de soluciones y servicios. Permitir a la empresa tomar decisiones informadas con respecto a la utilización de soluciones y servicios de TI.</p>	
APO06 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	Métricas Relacionadas
1. La asignación de presupuestos y costes a seguridad de la información se prioriza de forma eficaz.	Porcentaje de alineamiento entre los recursos de TI y las iniciativas importantes de control y seguridad de la información Resultado de la cantidad de problemas generados en la asignación de recursos debidos a incidentes en seguridad de la información
APO06 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad.	

Cuadro 19. APO06 Gestionar el Presupuesto y los Costes. Continuación.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO06.01 Gestionar las finanzas y la contabilidad. Establecer y mantener un método de contabilización para todos los costes, inversiones y depreciaciones relacionadas con las TI, como parte integral de los sistemas financieros empresariales y un plan de cuentas para administrar las inversiones y los costes de TI. Capturar y asignar los costes reales, analizar las desviaciones entre las previsiones y los costes reales, e informar usando los sistemas empresariales de medición financiera.	Interno			Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No son necesarias guías específicas sobre seguridad de la información para esta práctica. Las actividades genéricas de COBIT 5 pueden ser utilizadas como guía adicional.				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO06.02 Priorizar la asignación de recursos. Implementar un proceso de toma de decisiones para priorizar la asignación de recursos y definir las reglas para las inversiones discrecionales realizadas, a título individual, por las unidades de negocio. Incluir el uso potencial de proveedores de servicios			Priorización de las iniciativas.	APO06.03

Cuadro 19. APO06 Gestionar el Presupuesto y los Costes. Continuación.				
externos y considerar las opciones de compra, desarrollo y alquiler			Priorización de las iniciativas.	APO06.03
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que cuando se prioriza la asignación de recursos, se tienen en consideración criterios para la priorización acordes a los perfiles de riesgo de la				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO06.03 Crear y mantener presupuestos. Preparar un presupuesto que refleje las prioridades de inversión que apoyen los objetivos estratégicos, tomando como base la cartera de programas habilitados por TI y de servicios de TI.	APO06.02	Priorización de las iniciativas	Presupuesto para la seguridad de la información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir un presupuesto para la seguridad de la información.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO06.04 Modelar y asignar costes. Establecer y utilizar un modelo de costes de TI basado en la definición del servicio, asegurando que la asignación de costes de los servicios es identificable, medible y predecible, para fomentar el uso responsable de los recursos, incluidos aquellos proporcionados por proveedores de servicio. Revisar y comparar periódicamente la idoneidad del modelo de costes/prorrateo, para mantener su pertinencia y				

Cuadro 19. APO06 Gestionar el Presupuesto y los Costes. Continuación.				
adecuación a las cambiantes actividades del negocio y de TI.	Interno			Interno
APO07 Gestionar los Recursos Humanos				
<p>Descripción del Proceso de COBIT 5 Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.</p>				
<p>Declaración del Propósito del Proceso de COBIT 5 Optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa.</p>				
<p>0. No son necesarias guías específicas sobre seguridad de la información para esta práctica. Las actividades genéricas de COBIT 5 pueden ser utilizadas como guía adicional.</p>				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO06.05 Gestionar costes. Poner en marcha un proceso de gestión de costes que compare los costes reales con los presupuestos. Los costes deben ser supervisados y comunicados y, en caso de desviaciones, identificados oportunamente, así como evaluado su impacto en los procesos y servicios empresariales.	Interno			Interno
<p>Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)</p>				
<p>0. No son necesarias guías específicas sobre seguridad de la información para esta práctica. Las actividades genéricas de COBIT 5 pueden ser utilizadas como guía adicional.</p>				
<p>Fuente: Cobit 5 For Information Security</p>				

Cuadro 20. APO07 Gestionar los Recursos Humanos

APO08 Gestionar las Relaciones	
<p>Descripción del Proceso Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándolas hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usando términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves.</p>	
<p>Tabla 26. APO07 Gestionar los Recursos Humanos</p>	
<p>Declaración del Propósito del Proceso Crear mejores resultados, mayor confianza en la tecnología y conseguir un uso efectivo de los recursos.</p>	
<p>APO08 Metas y Métricas del Proceso específicas de Seguridad:</p>	
Metas del Proceso específicas de Seguridad	Métricas Relacionadas
<p>1. Se ha establecido una estructura de coordinación, comunicación y enlace entre la función de seguridad de la información y varios grupos de interés</p>	<p>Porcentaje de representación de la seguridad de la información en los comités de negocio</p>
<p>2. Los grupos de interés reconocen la seguridad de la información como un catalizador del negocio</p>	<p>Tasa de inclusión de las iniciativas de seguridad de la información en las propuestas de inversión</p>
<p>Fuente: Cobit 5 For Information Security</p>	

Cuadro 21. APO08 Gestionar las Relaciones

APO08 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
<p>APO08.01 Entender las expectativas del negocio. Entender los problemas y objetivos actuales del negocio y sus expectativas para TI</p>	<p>Fuera del ámbito de COBIT 5 para Seguridad de la Información</p>	<p>Metas y objetivos del negocio</p>	<p>Comprensión de los procesos de negocio de la empresa</p>	<p>APO08.02 APO08.03</p>

Cuadro 21. APO08 Gestionar las Relaciones. Continuación				
Asegurar que los requisitos son entendidos, gestionados y comunicados y su estado acordado y aprobado				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Entender el negocio y cómo la seguridad de la información lo habilita/afecta.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO08.02 Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio. Identificar oportunidades potenciales para que TI sea catalizadora de un mejor rendimiento empresarial.	APO04.03	Tendencias emergentes en seguridad de la información identificadas	Innovaciones en Seguridad de la Información	APO08.03
	APO08.01	Comprensión de los procesos de negocio de la empresa		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Entender las tendencias y las nuevas tecnologías en seguridad de la información y cómo pueden ser aplicadas, de modo innovador, para mejorar el rendimiento de los procesos de negocio.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO08.03 Gestionar las relaciones con el negocio. Gestionar la relación con los clientes (representantes del negocio). Asegurar que los roles y responsabilidades de la relación están definidos, asignados y que se facilita la comunicación.	APO08.01	Comprensión de los procesos de	Estrategia para lograr el compromiso de las partes interesadas	Interna
	APO08.02	Innovaciones en seguridad		
	DSS02.02	Incidentes y peticiones de servicio de seguridad de la información.		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				

Cuadro 21. APO08 Gestionar las Relaciones. Continuación				
1. Establecer un método para influir en los contactos clave en relación con seguridad de la información.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO08.04 Coordinar y comunicar. Trabajar con las partes interesadas y coordinar, de extremo a extremo, la entrega de los servicios de TI y las soluciones proporcionadas al negocio.	Fuera del ámbito de COBIT 5 para Seguridad de la información	Plan de comunicación	Estrategia de comunicación de la seguridad de la información	Interna
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Establecer los canales de comunicación adecuados entre la función de seguridad de la información y el negocio.				
2. Establecer la presentación de informes y métricas sobre seguridad de la información de forma adecuada.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO08.05 Proveer datos de entrada para la mejora continua de los servicios. Mejorar y evolucionar continuamente los servicios basados en TI y la entrega del servicio a la empresa, para alinearlos con unos cambiantes requisitos de empresa y tecnológicos.	APO02.02	Capacidades de seguridad	Integración de la seguridad de la información en el proceso de mejora continua	Interna
	BAI02.01	Requisitos de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Incorporar los requisitos de seguridad de la información al proceso de mejora				

Cuadro 22. APO09 Gestionar los Acuerdos de Servicio.

APO09 Gestionar los Acuerdos de Servicio				
<p>Descripción del Proceso Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la empresa, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento.</p>				
<p>Tabla 28. APO09 Gestionar los Acuerdos de Servicio</p>				
<p>Declaración del Propósito del Proceso Asegurar que los servicios TI y los niveles de servicio cubren las necesidades presentes y futuras de la empresa.</p>				
<p>APO09 Metas y Métricas del Proceso específicas de Seguridad</p>				
Metas del Proceso específicas de			Métricas Relacionadas	
<p>1. Los acuerdos de nivel de servicio (ANS) tienen en cuenta los requisitos de seguridad de la información</p>			<p>Porcentaje de acuerdos de servicio que incluyen metas de seguridad de la información.</p>	
<p>APO09 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad</p>				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
<p>APO09.01 Identificar servicios TI. Analizar los requisitos del negocio y el modo en que los servicios de TI y los niveles de servicio soportan los procesos de negocio. Discutir y acordar servicios potenciales y niveles de servicio con el negocio, y compararlos con el vigente portafolio de servicios para identificar servicios nuevos o modificados, u opciones de nivel de servicio.</p>			<p>Requisitos de seguridad de la información en los servicios de TI identificados</p>	<p>APO09.02</p>
<p>Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)</p>				
<p>Identificar los requisitos de seguridad de información de los servicios de TI identificados.</p>				

Cuadro 22. APO09 Gestionar los Acuerdos de Servicio. Continuación				
Definir y verificar el portafolio de servicios de seguridad de la información.				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO09.02 Catalogar servicios basados en TI. Definir y mantener uno o más catálogos de servicios para grupos destinatarios relevantes. Publicar y mantener los servicios TI activos en los catálogos.	APO09.01	Requisitos de seguridad de la información en los servicios de TI identificados.	Catálogo de servicios de seguridad de la información	Interna
Cuadro 22. APO09 Gestionar los Acuerdos de Servicio				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Publicar un catálogo de servicios de seguridad de la información.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO09.03 Definir y preparar acuerdos de servicio. Definir y preparar los acuerdos de servicio basándose en las opciones de los catálogos de servicio. Incluir acuerdos internos de nivel de operaciones.	BAI03.11	Servicios de seguridad de la Información.	Acuerdos de nivel de servicio (ANSs)	APO09.04 DSS05.02
			Acuerdos de nivel de operaciones (OLAs)	
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Incluir requisitos de seguridad de la información en todos los ANSs.				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO09.04 Supervisar e informar de los niveles de servicio. Supervisar los niveles de	APO09.03			APO09.05

servicio, informar de las mejoras e identificar tendencias. Proporcionar información de gestión adecuada para ayudar a la gestión del rendimiento.	APO09.03	Acuerdos de nivel de servicio (ANSs)	Informes de rendimiento de nivel de servicio de seguridad de la información	APO09.05
	BAI03.11	Servicios de seguridad de la Información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Vigilar la eficacia de la seguridad de la información dentro de la supervisión del nivel de servicio				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO09.05 Revisar acuerdos de servicio y contratos. Llevar a cabo revisiones periódicas de los acuerdos de servicio y revisarlos cuando sea necesario.	APO02.02	Capacidades de seguridad de la información.	Acuerdos de nivel de servicios (ANSs) actualizados	Interna
	APO02.06	Plan de seguridad de la información.		
	APO09.04	Informes de rendimiento de nivel de		
	BAI02.01	Requisitos de seguridad de la información.		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Revisar periódicamente los requisitos de seguridad de la información en función de la actualización de las necesidades de negocio.				
Fuente: Cobit 5 For Information Security				

Cuadro 23. APO10 Gestionar los Proveedores

APO10 Gestionar los Proveedores				
<p>Descripción del Proceso Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.</p>				
<p>Declaración del Propósito del Proceso Minimizar el riesgo de proveedores que no rindan y asegurar precios competitivos.</p>				
<p>APO10 Metas y Métricas del Proceso específicas de Seguridad</p>				
Metas del Proceso específicas de Seguridad		Métricas Relacionadas		
<p>Se evalúa periódicamente a los proveedores y los contratos; y se disponen planes adecuados de mitigación del riesgo.</p>		<p>Porcentaje de proveedores que cumplen los requisitos acordados N° de brechas de seguridad de los sistemas de información causados por proveedores N° de eventos de seguridad de la información que llevan a incidentes Frecuencia de incidentes de seguridad de la información con proveedores N° de revisiones independientes de seguridad de la información de los proveedores</p> <ul style="list-style-type: none"> ● Cantidad de auditorías realizadas a terceros. 		
<p>Los proveedores reconocen la seguridad de la información como un importante catalizador de negocio.</p>		<p>Porcentaje de contratos con proveedores que incluyen requisitos de seguridad de la información N° de incidentes de seguridad de la información relacionados con proveedores</p>		
<p>APO10 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad</p>				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
<p>APO10.01 Identificar y evaluar las relaciones y contratos con proveedores.</p>				

Cuadro 23. APO10 Gestionar los Proveedores. Continuación.				
Identificar proveedores y contratos asociados y categorizarlos por tipo, relevancia y criticidad. Establecer un criterio de evaluación de contratos y proveedores y evaluar la cartera general de proveedores y contratos actuales y alternativos.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Análisis de riesgos de proveedores	Catálogo de proveedores	APO10.04 APO10.05 BAI03.04
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Llevar a cabo las evaluaciones de riesgos de la información y definir el perfil de riesgo de la misma.				
Definir la relación y requisitos de los proveedores basándose en el perfil de riesgo de la información.				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO10.02 Seleccionar proveedores. Seleccionar proveedores de acuerdo a prácticas justas y formales que aseguren la selección del que mejor se adapte a los requisitos. Los requisitos deberían estar optimizados con las aportaciones de nuevos proveedores potenciales.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
No son necesarias guías específicas sobre seguridad de la información para esta práctica. Las actividades genéricas de COBIT 5 pueden ser utilizadas como guía adicional.				

Cuadro 23. APO10 Gestionar los Proveedores. Continuación				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
<p>APO10.03 Gestionar contratos y relaciones con proveedores. Formalizar y gestionar las relaciones con cada proveedor. Gestionar, mantener y supervisar los contratos y la entrega de servicios. Asegurar que los nuevos contratos o los cambios son conformes a las normas de la empresa, a las leyes y a las regulaciones. Gestionar los conflictos contractuales.</p>				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
No son necesarias guías específicas sobre seguridad de la información para esta práctica. Las actividades genéricas de COBIT 5 pueden ser utilizadas como guía adicional.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
<p>APO10.04 Gestionar el riesgo en el suministro. Identificar y gestionar los riesgos relacionados con la capacidad de los proveedores de proporcionar de manera continua una entrega del servicio segura, eficaz y eficiente</p>	APO10.01	Catálogo de proveedores	Valoración del riesgo del proveedor, actualizada	APO10.05

Cuadro 23. APO10 Gestionar los Proveedores. Continuación.
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)
Reevaluar, periódicamente, los perfiles de seguridad de los proveedores, a partir de los requisitos de seguridad de la información y de otros tipos.
Fuente: Cobit 5 For Information Security

Cuadro 24. APO11 Gestionar la Calidad

APO11 Gestionar la Calidad	
<p>Descripción del Proceso Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.</p>	
<p>Declaración del Propósito del Proceso Asegurar la entrega consistente de soluciones y servicios que cumplan con los requisitos de la organización y que satisfagan las necesidades de las partes interesadas.</p>	
<p>APO11 Metas y Métricas del Proceso específicas de Seguridad</p>	
Metas del Proceso específicas de Seguridad	Métricas Relacionas
<p>Se han definido e implementado los requisitos de calidad operativos para los servicios de seguridad de la información.</p>	<p>Porcentaje, basado en encuestas, de partes interesadas satisfechas con la calidad de los servicios de seguridad de la información Número de servicios con un plan formal de seguridad de la información Frecuencia de presentación de informes (semanal, mensual, trimestral, anual) Medida en que la resolución de cuestiones de seguridad de la información (incidentes, vulnerabilidades, puntos de auditoría, etc.) queda realizada de forma oportuna Porcentaje de personal de seguridad de la información con credenciales profesionales (CISM, CISSP, etc.) Número de horas de formación profesional continua (CPE), u horas de asistencia a formación o a eventos del sector.</p>

Cuadro 24. APO11 Gestionar la Calidad. Continuación.				
APO11 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO11.01 Establecer un sistema de gestión de la calidad (SGC). Establecer y mantener un SGC que proporcione una aproximación a la gestión de la calidad de la información para la información, la tecnología y los procesos de negocio que sea continua, estandarizada, formal y que esté alineada con los requerimientos del negocio y con la gestión corporativa de la calidad.	APO01.06	Roles y responsabilidades de la seguridad de la información	Buenas prácticas y normas relevantes de seguridad de la información	APO11.02
	APO02.02	Capacidades de seguridad de la Información		
	APO02.06	Plan de seguridad de la información.		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Determinar buenas prácticas de seguridad de la información.				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO11.02 Definir y gestionar normas, prácticas y procedimientos de seguridad. Identificar y mantener re-	APO11.01	Buenas prácticas y normas relevantes para seguridad de la información	Normas de calidad dirigidas a la seguridad de la información	APO11.03 BAI03.06

Cuadro 24. APO11 Gestionar la Calidad. Continuación.				
quisitos, normas, procedimientos y prácticas para los procesos clave, a fin de guiar a la empresa hacia el cumplimiento del propósito del QMS común, consensuado. Esto debería estar en línea con los requisitos del marco de control de TI. Considerar la certificación para los procesos, unidades organizativas, productos o servicios clave.	APO11.01	Buenas prácticas y normas relevantes para seguridad de la información	Normas de calidad dirigidas a la seguridad de la información	APO11.03 BAI03.06
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Alinear las prácticas de seguridad de la información con el sistema de gestión de la calidad (SGC).				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO11.03 Enfocar la gestión de la calidad en los clientes. Enfocar la gestión de la calidad en los clientes, mediante la determinación de sus necesidades y asegurar el alineamiento con las prácticas de gestión de la calidad.	APO11.02	Normas de calidad dirigidas a la seguridad de la información	Acuerdos de nivel de servicio consensuados y cláusulas contractuales, relativos a la calidad de la seguridad de la información, cuando sea pertinente	APO11.04
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Obtener el consenso del cliente sobre los requisitos de los acuerdos de nivel de servicio de seguridad de la información.				

Cuadro 24. APO11 Gestionar la Calidad. Continuación				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO11.04 Supervisar y hacer controles y revisiones de la calidad. Supervisar la calidad de procesos y servicios de forma permanente como se defina en el SGC. Definir, planificar y aplicar medidas para supervisar la satisfacción del cliente con la calidad, así como el valor que proporciona el SGC. La información recogida debería ser utilizada por los propietarios de los procesos para mejorar la calidad.	APO11.03	Acuerdos de nivel de servicio consensuados y cláusulas contractuales, relativos a la calidad de la seguridad de la información, cuando sea pertinente	Métricas de la calidad de la seguridad de la información implementadas en línea con las buenas prácticas	APO11.05
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Definir métricas de la calidad de la seguridad de la información para medir la consecución de los requisitos de seguridad de la información y el funcionamiento eficiente de los controles de seguridad de la información.				
Supervisar las métricas de la calidad de la seguridad de la información.				
Adoptar acciones correctivas para subsanar problemas de calidad en la función de seguridad de la información.				

Cuadro 24. APO11 Gestionar la Calidad. Continuación				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
<p>APO11.05 Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.</p> <p>Incorporar prácticas pertinentes de gestión de la calidad en la definición, supervisión, notificación y gestión continua de los desarrollos de soluciones y los servicios ofrecidos.</p>	APO11.04	Métricas de la calidad de la seguridad de la información implantadas en línea con las buenas prácticas	Enlace con el proceso de comunicación de incidentes de seguridad	Interna
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Identificar, documentar y comunicar el origen de los problemas con las métricas de calidad de la seguridad de la información.				
Aplicar prácticas correctivas para solucionar los problemas de calidad.				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
<p>APO11.06 Mantener una mejora continua.</p> <p>Mantener y comunicar regularmente un plan de la calidad global que promueva la mejora continua. Éste debería incluir la necesidad y los beneficios de una mejora continua.</p>				

Cuadro 24. APO11 Gestionar la Calidad. Continuación				
Recoger y analizar datos sobre el SGC y mejorar su eficacia. Corregir las no conformidades para prevenir la recurrencia. Promover una cultura mejora continua de la calidad.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
No son necesarias guías específicas sobre seguridad de la información para esta práctica. Las actividades genéricas de COBIT 5 pueden ser utilizadas como guía adicional.				
Fuente: Cobit 5 For Information Security				

Cuadro 25. APO12 Gestionar el Riesgo

APO12 Gestionar el Riesgo	
<p>Descripción del Proceso Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.</p>	
<p>Declaración del Propósito del Proceso Integrar la gestión de riesgos empresariales relacionados con TI en la gestión general de riesgos corporativos (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI.</p>	
APO12 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	Métricas Relacionadas
1. Se dispone de un perfil de riesgo, completo y vigente, para la tecnología, las aplicaciones y la infraestructura, dentro de la empresa.	Existencia, vigencia y completitud de los perfiles de riesgo.
2. La respuesta a incidentes de seguridad de la información forma parte del proceso global de gestión del riesgo para proporcionar la capacidad de actualizar el portafolio de gestión del riesgo.	Número de incidentes con valoraciones de riesgo adecuadamente diseñadas

Cuadro 25. APO12 Gestionar el Riesgo. Continuación				
APO12 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO12.01 Recopilar datos. Identificar y recopilar datos relevantes para hacer posible una identificación, análisis y notificación efectiva de riesgos relacionados con TI.	APO01.08	Evaluación del cumplimiento de seguridad de la información	Datos sobre el riesgo de seguridad de la información	APO12.02 APO12.03
	DSS02.02	Incidentes de seguridad de la información y solicitudes de servicio, clasificados y priorizados		
Actividades específicas de Seguridad (Adicionales a las actividades de COBIT 5)				
Identificar y recopilar datos relevantes para hacer posible una eficaz identificación, análisis y entrega de informes relativos a seguridad de la información.				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO12.02 Analizar el riesgo. Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tengan en cuenta la relevancia para el negocio de los factores de riesgo.	APO12.01	Datos sobre el riesgo de	Resultados del análisis	APO12.03
	DSS05.01	Evaluación de las amenazas potenciales	Escenarios de riesgos de seguridad de la información	APO12.03
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Identificar, analizar y evaluar el riesgo de la información.				

Cuadro 25. APO12 Gestionar el Riesgo. Continuación				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO12.03 Mantener un perfil de riesgo. Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados	EDM01.01	Principios que rigen la seguridad de la información	Perfil de riesgo de seguridad de la información	APO12.04 APO12.05 BAI01.01 BAI01.11 BAI02.03
	APO12.01	Datos sobre el riesgo de seguridad de la información		
	APO12.02	Resultado del análisis de riesgo de seguridad de la información Escenarios de riesgos de seguridad de la información		
	DSS05.01	Evaluación de potenciales		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Crear un perfil de riesgo que incluya aspectos de seguridad de la información.				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO12.04 Expresar el riesgo. Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de forma oportuna a	APO12.03	Perfil de riesgo de seguridad de la información	Estrategias de respuesta a riesgos de seguridad de la información	Interna

todas las partes interesadas para una respuesta apropiada.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Definir y poner en marcha la evaluación de riesgo y las estrategias de respuesta.				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO12.05 Definir un portafolio de acciones para la gestión de riesgos. Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.	APO12.03	Perfil de riesgo de seguridad de la información	Propuestas de proyectos para reducir el riesgo de seguridad de la información	APO12.06
			Propuestas de proyectos para reducir el riesgo	APO13.02
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Supervisar continuamente los niveles de riesgo de las TI y de la información.				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO12.06 Responder al riesgo. Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida.	APO12.05	Propuestas de proyecto para reducir el riesgo de la seguridad de la información	Prácticas de reducción del riesgo de la seguridad de la información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Aplicar las prácticas seleccionadas de mitigación de riesgos de la seguridad de la información.				
Fuente: Cobit 5 For Information Security				

Cuadro 26. APO13 Gestionar de la Seguridad

APO13 Gestionar de la Seguridad				
Descripción Proceso COBIT 5				
Definir, administrar y supervisar un sistema de gestión de seguridad de la información.				
Declaración del Propósito del Proceso COBIT 5				
Mantener el impacto y la ocurrencia de incidentes de seguridad de la información dentro de los niveles de apetito al riesgo de la empresa.				
APO13 Objetivos y Métricas de Proceso específicos de seguridad				
Objetivos de Proceso específicos de Seguridad		Métricas Relacionadas		
1. Está en marcha un sistema que considera y trata efectiva mente los requerimientos de seguridad de la información de la empresa.		Número de roles de seguridad claves claramente definidos Número de incidentes relacionados con la seguridad		
2. Se ha establecido, aceptado y comunicado por toda la empresa un plan de seguridad.		Nivel de satisfacción de las partes interesadas con el plan de seguridad en toda la empresa Número de soluciones de seguridad que se desvían del plan. Número de soluciones de seguridad que se desvían de la arquitectura de empresa		
3. Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en toda la empresa.		Número de servicios con alineamiento confirmado al plan de seguridad Número de incidentes de seguridad causados por la no observancia del plan de seguridad Número de soluciones desarrolladas con alineamiento confirmado al plan de seguridad		
APO13 – Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
APO13.01 Establecer y mantener un SGSI. Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio	Fuera del ámbito de COBIT 5 para seguridad de la Información	Enfoque de seguridad de la empresa	Declaración de alcance del SGSI	DSS06.03

Cuadro 26. APO13 Gestionar de la Seguridad. Continuación				
que esté alineado con los requerimientos de negocio y la gestión de seguridad en la empresa.				
			Política de SGSI	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Definir el alcance y los límites del SGSI en términos de las características de la empresa, la organización, su localización, activos y tecnología. Incluir detalles de y justificación para, cualquier exclusión del alcance.				
Definir un SGSI de acuerdo con la política de empresa y alineado con la empresa, la organización, su localización, activos y tecnología.				
Alinear el SGSI con el enfoque global de gestión de la seguridad en la empresa.				
Obtener autorización de la dirección para implementar y operar o cambiar el SGSI.				
Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.				
Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información.				
Comunicar el enfoque del SGSI.				
Práctica de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	Desde	Descripción	Descripción	Hacia
APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información. Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en	APO02.04	Diferencias y cambios necesarios para alcanzar la capacidad objetivo	Casos de negocio de seguridad de la información	APO02.05

Cuadro 26. APO13 Gestionar de la Seguridad. Continuación.				
seguridad se basan en casos de negocios aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio.	APO12.05	Propuestas de proyectos para reducir el riesgo		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura de la empresa. Asegurar que el plan identifica las prácticas de gestión y las soluciones de seguridad apropiada y óptima, con los recursos, las responsabilidades y las prioridades asociadas para gestionar los riesgos de seguridad de información identificados.				
Mantener un inventario de componentes de la solución implementados para gestionar los riesgos relacionados con la seguridad como parte de la arquitectura de la empresa.				
Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información, sustentados en casos de negocio adecuados que incluyan la consideración de la financiación y la asignación de roles y responsabilidades.				
Proporcionar información para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas sobre la base del plan de tratamiento de riesgos de seguridad de la información.				
Definir la forma de medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizar estas mediciones para evaluar la efectividad y producir resultados reproducibles y comparables.				
Recomendar programas de formación y concienciación en seguridad de la información.				
Integrar la planificación, el diseño, la implementación y la supervisión de los procedimientos de seguridad de información y otros controles que permitan la prevención y detección temprana de eventos de seguridad, así como la respuesta a incidentes de seguridad.				

Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	Descripción	Descripción	Hacia
<p>APO13.03 Supervisar y revisar el SGSI. Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua.</p>	DSS02.02	Incidentes y requerimientos de servicios clasificados y priorizados	Recomendaciones para mejorar el SGSI	Interno
			Informes de auditoría del SGSI	MEA02.01
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
Realizar revisiones periódicas del SGSI, incluyendo aspectos de políticas, objetivos y prácticas de seguridad del SGSI. Considerar los resultados de auditorías de seguridad, incidentes, resultados de mediciones de efectividad, sugerencias y retroalimentación de todas las partes interesadas.				
Realizar auditorías internas al SGSI a intervalos planificados.				
Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se identifican mejoras en el proceso del SGSI.				
Proporcionar información para el mantenimiento de los planes de seguridad para que se incluyan las incidencias de las actividades de supervisión y revisión periódica.				
Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.				
Fuente: Cobit 5 For Information Security				

5.2.2.3 Construir, Adquirir e Implementar (BAI)

Cuadro 27. BAI01 Gestionar Programas y Proyectos

BAI01 Gestionar Programas y Proyectos				
<p>Descripción Proceso COBIT 5 Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.</p>				
<p>Declaración del Propósito del Proceso COBIT 5 Alcanzar los beneficios de negocio y reducir el riesgo de retrasos y costes inesperados y el deterioro del valor, mediante la mejora de las comunicaciones y la involucración de usuarios finales y de negocio, asegurando el valor y la calidad de los entregables del proyecto y maximizando su contribución al portafolio de servicios e inversiones.</p>				
BAI01 Objetivos y Métricas de Proceso específicos de seguridad				
Objetivos de Proceso específicos de Seguridad		Métricas Relacionadas		
Se consideran y se incorporan los requisitos de seguridad de la información en todos los programas y proyectos.		<p>Porcentaje de programas y grupos de interés del proyecto comprometidos de manera efectiva en la gestión de Seguridad de la Información</p> <p>Porcentaje de programas y proyectos que tienen un análisis de riesgos de seguridad y un plan de seguridad de la información para tratar el riesgo</p> <p>Porcentaje de expertos en temas de seguridad de la información involucrados en los proyectos</p> <p>Porcentaje de aprobaciones formales por parte de los grupos de interés de las etapas de revisión y planes de remediación</p> <p>Frecuencia de las revisiones del estado de seguridad de la información</p>		
BAI01 – Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI01.01 Mantener un enfoque estándar para la gestión de programas y proyectos. Mantener un enfoque estándar para la gestión de programas y proyectos que gobierno	APO02.02	Capacidades de seguridad de la información	Requisitos de seguridad de la información en el estudio de viabilidad	BAI01.02 BAI02.02

Cuadro 27. BAI01 Gestionar Programas y Proyectos. Continuación				
posibilite revisiones y tomas de decisión de decisión de gobierno y de gestión y actividades de gestión de la entrega enfocadas en la consecución de valor y de objetivos (requisitos, riesgos, costes, cronograma y calidad) para el negocio de una forma consistente.	APO02.02	Capacidades de seguridad de la información	Requisitos de seguridad de la información en el estudio de viabilidad	BAI01.02 BAI02.02
	APO02.06	Plan seguridad de la información		BAI03.01
	APO12.03	Perfil de riesgo de seguridad de la información		
	BAI02.01	Requerimientos de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Incorporar los requerimientos de seguridad de la información en el estudio de viabilidad para cada proyecto dentro de los programas.				
2. Establecer un proceso para asegurar que se protege toda la información que se recoge o se produce como parte del proyecto.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI01.02 Iniciar un programa. Iniciar un programa para confirmar los beneficios esperados y para obtener la autorización para proceder. Esto incluye los acuerdos sobre el patrocinio del programa, confirmar el mandato del programa a través de la aprobación del caso de negocio conceptual, designar a los consejeros o los miembros del comité del programa, generar	BAI01.01	Requisitos de seguridad de la información en el estudio de viabilidad	Caso de negocio conceptual del programa que incluye las actividades obligatorias de seguridad de la información	BAI01.04 BAI01.08

Cuadro 27. BAI01 Gestionar Programas y Proyectos. Continuación				
el expediente del programa, revisar y actualizar el caso de negocio, desarrollar un plan de realización de beneficios y obtener la aprobación de los patrocinadores para empezar.	BAI01.01	Requisitos de seguridad de la información en el estudio de viabilidad	Caso de negocio conceptual del programa que incluye las actividades obligatorias de seguridad de la información	BAI01.04 BAI01.08
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Planificar las actividades de seguridad de la información para cada proyecto dentro del programa general.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAIO01.03 Gestionar el compromiso de las partes interesadas. Gestionar el compromiso de las partes interesadas para asegurar un intercambio activo de información precisa, consistente y oportuna que llegue a todas las partes interesadas relevantes. Esto incluye la planificación, identificación y el compromiso de las partes interesadas y la gestión de sus expectativas.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				

Cuadro 27. BAI01 Gestionar Programas y Proyectos. Continuación				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI01.04 Desarrollar y mantener el plan de programa. Formular un programa para definir las bases iniciales y posicionarlo para una ejecución exitosa mediante la formalización del alcance del trabajo a ser efectuado e identificando los entregables que satisfarán sus objetivos y la entrega de valor. Mantener y actualizar el plan del programa y el caso de negocio a lo largo del ciclo de vida económico completo del programa, asegurando el alineamiento con los objetivos estratégicos y reflejando el estado actual y los conocimientos obtenidos hasta el momento.				
	APO02.06	Plan de seguridad de la información	Plan conceptual del programa incluyendo las actividades obligatorias de seguridad de la información	BAI01.08
	BAI01.02	Caso de negocio conceptual del programa que incluye las actividades obligatorias de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Desarrollar un plan de seguridad de la información que identifique el entorno y los controles de seguridad de la información que el equipo del proyecto ha de implantar para proteger los activos organizativos.				
2. Incluir los recursos necesarios en los proyectos para identificar e implementar de forma efectiva los requerimientos de seguridad de la información.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI01.05 Lanzar y ejecutar el programa.				

Cuadro 27. BAI01 Gestionar Programas y Proyectos. Continuación				
Lanzar y ejecutar el programa para adquirir y dirigir los recursos necesarios para lograr las metas y beneficios definidos en el plan del programa. De acuerdo con los criterios de revisión de lanzamiento o cambio de fase (stage-gate).				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI01.06 Supervisar, controlar e informar de los resultados del programa. Supervisar y controlar el rendimiento del programa (entrega de soluciones) y de la organización (valor/resultado) versus el plan durante el ciclo de vida económico completo de la inversión. Informar del rendimiento al comité estratégico del programa y a los patrocinadores.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				

Cuadro 27. BAI01 Gestionar Programas y Proyectos. Continuación				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI01.07. Lanzar e iniciar proyectos dentro de un programa. Definir y documentar la naturaleza y el alcance del proyecto para confirmar y desarrollar entre las partes interesadas un entendimiento común del alcance del proyecto y cómo este se relaciona con otros proyectos dentro del programa general de inversiones de TI. La definición debería estar formalmente aprobada por el patrocinador del programa y del proyecto.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI01.08. Planificar Proyectos. Establecer y mantener un plan de proyecto formal, aprobado e integrado (que cubra los recursos del negocio y de TI) para guiar la ejecución del proyec				

Cuadro 27. BAI01 Gestionar Programas y Proyectos. Continuación				
to y controlarlo duran te toda su vida. El alcance de los proyec tos debería estar claramente definido y vinculado claramente a la construcción o aumento de la capa cidad del negocio.	APO02.06	Plan de seguridad de la infor mación	Plan de proyecto inclu yendo las metas, objeti vos y requerí mientos de seguridad de la informa ción	BAI01.10
	BAI01.02	Caso de negocio conceptual del programa incluyendo las actividades obligatorias de seguridad de la información		
	BAI01.04	Plan conceptual del programa incluyendo las actividades obligatorias de seguridad de la información		
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI01.09 Gestionar la calidad de los programas y proyectos. Preparar y ejecutar un plan y procesos y prácticas de gestión de la calidad, alineadas con el SGC que describa el enfoque de calidad del programa y del proyecto y cómo será implementado. El				

Cuadro 27. BAI01 Gestionar Programas y Proyectos. Continuación				
plan debería ser formalmente revisado y acordado por todas las partes afectadas y, después, incorporado a los planes integrados del programa y los proyectos.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI01.10 Gestionar el riesgo de los programas y proyectos. Eliminar o minimizar los riesgos específicos asociados con los programas y proyectos mediante un proceso sistemático de planificación, identificación, análisis, respuesta, supervisión y control de las áreas o eventos que tienen el potencial de causar cambios no deseados. Los riesgos enfrentados por la administración del programa y los proyectos deberían ser establecidos y registrados en un único punto.	BAI01.08	Plan de proyecto incluyendo las metas, objetivos y requerimientos de seguridad de la información	Registro de riesgos de seguridad de la información incluido como parte del registro general de riesgos del proyecto	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Establecer un registro de riesgos de información y acciones correctivas para los riesgos identificados. Actualizar y revisar periódicamente el registro de riesgos.				

Cuadro 27. BAI01 Gestionar Programas y Proyectos. Continuación				
2. Integrar los proyectos de seguridad de la información en el proceso de gestión de programas y proyectos de la empresa.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI01.11 Supervisar y controlar proyectos. Medir el desempeño del proyecto versus los criterios clave de rendimiento del proyecto, tales como la planificación, la calidad, el coste y el riesgo. Evaluar el impacto de las desviaciones en el proyecto y el programa general e informar los resultados a las partes interesadas clave.	APO02.06	Plan de seguridad de la información	Informe de evaluación de proyectos de seguridad de la información identificando las debilidades de control y los planes de acciones Correctivas recomendadas	Interno
	APO12.03	Perfil de riesgo de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Realizar evaluaciones periódicas independientes de los proyectos para asegurar que los requisitos de seguridad de la información son implementados efectivamente.				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI01.12 Gestionar los recursos y los paquetes de trabajo del proyecto. Gestionar los paquetes de trabajo del proyecto mediante requerimientos formales de autorización y aceptación de los paquetes de trabajo, y asignando y coordinando los recursos de negocio y de TI adecuados.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				

Cuadro 27. BAI01 Gestionar Programas y Proyectos. Continuación				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción		De
BAI01.13 Cerrar un proyecto o iteración. Solicitar a las partes interesadas del proyecto, al final de cada proyecto, versión o iteración, que evalúen si el proyecto, la versión o la iteración entregaron los resultados y valor planeados. Identificar y comunicar cualquier actividad pendiente necesaria para lograr los resultados del proyecto y los beneficios del programa planeados, identificar y documentar las lecciones aprendidas para utilizar en futuros proyectos, versiones, iteraciones y programas.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI01.14 Cerrar un programa. Eliminar el programa del portafolio de inversiones activas cuando haya acuerdo de que el valor deseado ha sido logrado o cuando esté claro que no será logrado con los criterios de valor esta-				

Cuadro 27. BAI01 Gestionar Programas y Proyectos. Continuación				
blecidos para el programa.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
Fuente: Cobit 5 For Information Security				

Cuadro 28. BAI02 Gestionar la Definición de Requisitos

BAI02 Gestionar la Definición de Requisitos	
<p>Descripción del Proceso COBIT 5</p> <p>Identificar soluciones y analizar requisitos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocio, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costes y beneficios relacionados, análisis de riesgo y aprobación de los requisitos y soluciones propuestas.</p>	
<p>Declaración del Propósito del Proceso COBIT 5</p> <p>Crear soluciones viables y óptimas que cumplan con las necesidades de la organización mientras minimizan el riesgo.</p>	
BAI02 Objetivos y Métricas de Proceso específicos de seguridad	
Objetivos de Proceso específicos de Seguridad	Métricas Relacionadas
1. Se ha identificado e implementado todos los aspectos de seguridad de la información relevantes como requisitos técnicos y funcionales.	<p>Porcentaje de nuevos requerimientos de seguridad de la información añadidos por requerimiento del negocio</p> <p>Porcentaje de requerimientos redefinidos debido a los requerimientos de seguridad de la información</p>
2. Se ha detectado y añadido el riesgo de información asociado con requisitos técnicos y funcionales de negocio.	<p>Nuevos riesgos de seguridad de la información identificados.</p> <p>Número de incidentes de seguridad de la información que indiquen riesgos nuevos o desconocidos</p> <p>Número de incidentes de seguridad de la información basados en riesgos conocidos</p>
BAI02 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso	

Cuadro 28. BAI02 Gestionar la Definición de Requisitos. Continuación.				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI02.1 Definir y mantener los requisitos técnicos y funcionales de negocio. Basado en el modelo de negocio, identificar, priorizar, especificar y acordar los requisitos de información comercial, funcionales, técnicas y de control que cubren el alcance / comprensión de todas las iniciativas necesarias para alcanzar los resultados esperados de la solución de negocio en TI propuesto.	APO02.02	Capacidades de seguridad de la información	Requerimientos de seguridad de la información	APO02.03 APO04.04 APO08.05 APO09.05 BAI01.01 BAI02.04
	APO02.06	Plan de seguridad de la información		BAI03.01 BAI03.04 BAI03.07 BAI03.09 BAI04.03 BAI05.01 MEA01.01 MEA03.01
	MEA03.01	Requerimientos externos de cumplimiento de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Investigar, definir y documentar los requisitos de seguridad de la información p.ej. requisitos de confidencialidad, integridad y disponibilidad.				
2. Investigar y analizar los requisitos de seguridad de la información con las partes interesadas, patrocinadores de negocio y personal de implementación técnica.				
3. Asegurar que los requisitos de negocio tienen en cuenta las necesidades de protección de seguridad de la información.				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI02.02 Realizar un estudio de viabilidad y proponer soluciones alternativas. Realizar un estudio de viabilidad de las potenciales soluciones alternativas, evaluando su viabilidad y seleccionan -	BAI01.01	Requerimientos de seguridad de la información en el estudio de viabilidad	Resultados del estudio de viabilidad	Interno

Cuadro 28. BAI02 Gestionar la Definición de Requisitos. Continuación.				
do la opción preferida. Si se considera, implementar la opción seleccionada como un piloto para determinar posibles mejores.	BAI01.01	Requerimientos de seguridad de la información en el estudio de viabilidad	Resultados del estudio de viabilidad	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que los requisitos de seguridad de la información son incluidos en el estudio de viabilidad				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI02.03 Gestionar los riesgos de los requerimientos. Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos al procesamiento de la información y asociados con los requerimientos de la empresa y solución propuesta.	APO12.03	Perfil de riesgo de seguridad de la información	Acciones de mitigación del riesgo	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Realizar una evaluación de riesgos de la información para identificar los controles de seguridad de la información para las actividades relevantes del negocio (gestión del programa y proyectos incluidos).				
2. Cooperar con el responsable de riesgos para gestionar los riesgos de la				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI02.04 Obtener la aprobación de los requerimientos y soluciones. Coordinar la realimentación de las partes interesadas afectadas y, en las fases clave predeter	BAI02.01	Requerimientos de seguridad de la información	Aprobación de los requerimientos de seguridad de la información	Interno

Cuadro 28. BAI02 Gestionar la Definición de Requisitos. Continuación.				
minadas, obtener la aprobación y la firma del patrocinador o propietario del producto y cierre de los requerimientos técnicos y funcionales, de los estudios de viabilidad, de los análisis de riesgos y de las soluciones recomendadas.	BAI02.01	Requerimientos de seguridad de la información	Aprobación de los requerimientos de seguridad de la información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Validar los requerimientos de seguridad de la información con las partes interesadas, patrocinadores de negocio y personal técnico de implementación.				
Fuente: Cobit 5 For Information Security				

Cuadro 29. BAI03 Gestionar la Identificación y Construcción de Soluciones

BAI03 Gestionar la Identificación y Construcción de Soluciones	
<p>Descripción del Proceso COBIT 5 Establecer y mantener soluciones identificadas en línea con los requisitos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.</p>	
<p>Declaración del Propósito del Proceso COBIT 5 Establecer soluciones puntuales y rentables capaces de soportar los objetivos estratégicos y operativos de la empresa.</p>	
BAI03 Objetivos y Métricas de Proceso específicos de seguridad	
Objetivos de Proceso específicos de seguridad	Métricas Relacionadas
1. Las métricas de seguridad de la información se incorporan en la solución y apoyan de manera eficaz la estrategia de negocio y los objetivos operacionales.	Cantidad de diseños de la solución añadidos debido a los requerimientos de seguridad de la información Cantidad de excepciones de seguridad en el diseño y en la implementación
2. Las soluciones en seguridad de la información se aceptan y se han probado de manera satisfactoria.	Número de pruebas adicionales para la seguridad de la información

Cuadro 29. BAI03 Gestionar la Identificación y Construcción de Soluciones. Continuación.				
3. Los cambios en los requerimientos de seguridad de la información se incorporan correctamente a la solución.		Número de cambios aprobados relativos a requerimientos de seguridad de la información		
BAI03 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI03.01 Diseñar soluciones de alto nivel. Desarrollar y documentar diseños de alto nivel usando técnicas de desarrollo ágil o por fases apropiadas y acordadas. Asegurar el alineamiento con la estrategia TI y la arquitectura empresarial. Revalorar y actualizar los diseños cuando sucedan cuestiones significativas durante las fases de diseño detallado o de construcción o según la solución evolucione.	BAI01.01	Requerimientos de seguridad en el estudio de viabilidad	Especificaciones de seguridad de la información en línea con los diseños de alto nivel	BAI03.02
	BAI02.01	Requerimientos de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir las especificaciones de seguridad de la información en línea con el diseño de alto nivel.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI03.02 Diseñar los componentes detallados de la solución. Desarrollar, documentar y elaborar diseños detallados progresivamente usando técnicas de desarrollo ágiles o por fases acordadas previa -				

Cuadro 29. BAI03 Gestionar la Identificación y Construcción de Soluciones. Continuación.				
previamente considerando todos los componentes (procesos de negocio y controles automáticos o manuales relacionados, aplicaciones soporte de TI, servicios de infraestructura y productos tecnológicos y proveedores/fabricantes).				
Asegurar que el diseño detallado incluye ANSs y OLAs internos Y externos.	BAI03.01	Especificaciones de seguridad de la información en línea con los diseños de alto nivel	Diseño de la seguridad de la información en los componentes de la solución	BAI03.03
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Integrar el diseño de la seguridad de la información en los componentes de la				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI03.03 Desarrollar los componentes de la solución. Desarrollar los componentes de la solución progresivamente conforme el diseño detallado siguiendo los métodos de desarrollo, estándares de documentación, requerimientos de calidad (QA) y estándares de aprobación. Asegurar que se consideran todos los requerimientos de control en los procesos de negocio, soportando las	BAI03.02	Diseño de la seguridad de la información en los componentes de la solución	Prácticas de programación y bibliotecas de infraestructura seguras	Interno

Cuadro 29. BAI03 Gestionar la Identificación y Construcción de Soluciones. Continuación.				
aplicaciones TI y servicios de infraestructura, productos tecnológicos y servicios y proveedores/suministradores.	BAI03.02	Diseño de la seguridad de la información en los componentes de la solución	Prácticas de programación y bibliotecas de infraestructura seguras	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Verificar que todos los componentes de la solución incorporan prácticas de programación y bibliotecas de infraestructura seguras.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI03.06 Realizar controles de calidad. Desarrollar y ejecutar un plan de calidad (QA) alineado con el SGC para obtener la calidad especificada en la definición de los requerimientos y de acuerdo a las políticas y procedimientos de calidad de la empresa.	APO11.02	Estándares de calidad para la seguridad de la información	Resultados, excepciones y correcciones de la revisión de la calidad de la seguridad de información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Verificar que los aspectos de la seguridad de la información están incluidos en el aseguramiento de la calidad.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI03.07 Preparar pruebas de la solución. Establecer un plan de pruebas y entornos necesarios para probar los	BAI02.01	Requerimientos de seguridad de la información	Casos de prueba de la seguridad de la información	Interno

Cuadro 29. BAI03 Gestionar la Identificación y Construcción de Soluciones. Continuación.				
componentes individuales y de la solución integrada, incluyendo los procesos de negocio y servicios, aplicaciones e infraestructura que los soportan.	BAI02.01	Requerimientos de seguridad de la información	Casos de prueba de la seguridad de la información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Incluir los casos de prueba de seguridad de la información en los planes de pruebas.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI03.09 Gestionar cambios a los requerimientos. Hacer seguimiento del estado de los requerimientos individuales (incluyendo todos los requerimientos rechazados) a través de todo el ciclo de vida del proyecto y gestionar la aprobación de los cambios a los requerimientos.	BAI02.01	Requerimientos de seguridad de la información	Registro de todas las peticiones de cambios aprobadas y aplicadas	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Gestionar los cambios en los aspectos y requerimientos de la seguridad de la información.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI03.10 Mantener soluciones. Desarrollar y ejecutar un plan para el mantenimiento de la solución y componentes de la infraestructura. Incluir revisiones			Soluciones seguras actualizadas	Interno

Cuadro 29. BAI03 Gestionar la Identificación y Construcción de Soluciones. Continuación.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que las actualizaciones de los requerimientos de seguridad de la				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI03.11 Definir los servicios de TI y mantener el catálogo de servicios. Definir y acordar nuevos servicios TI o cambios y opciones de nivel de servicio. Documentar nuevas definiciones o cambios en los servicios y opciones de nivel de servicio que serán actualizadas en el catálogo de servicios.	Modelo de catalizado res de estructuras organizativas	Roles y responsabilidades	Servicios de seguridad de la información	APO09.03 APO09.04
	Fuera de COBIT 5 para Seguridad de la Información	Misión/ Visión de negocio Metas y objetivos de negocio		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir los servicios de seguridad de la información en concordancia con las necesidades de negocio y las necesidades de cumplimiento o normativas.				
2. Definir los procesos de seguridad de la información dentro de los servicios de TI.				
Fuente: Cobit 5 For Information Security				

Cuadro 30. BAI04 Gestionar la Disponibilidad y la Capacidad

BAI04 Gestionar la Disponibilidad y la Capacidad
<p>Descripción del Proceso COBIT 5 Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en coste. Incluir la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos de negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados.</p>
<p>Declaración del Propósito del Proceso COBIT 5 Mantener la disponibilidad del servicio, la gestión eficiente de recursos y la optimización del rendimiento de los sistemas mediante la predicción del rendimiento futuro y de los requerimientos de capacidad.</p>
BAI04 Gestionar la Disponibilidad y la Capacidad. Continuación.

Cuadro 30. BAI04 Gestionar la Disponibilidad y la Capacidad. Continuación.				
Objetivos de Proceso específicos de seguridad		Métricas Relacionadas		
1. Los requerimientos de seguridad de la información se incluyen en los planes de disponibilidad, rendimiento y gestión de la capacidad.		Porcentaje de compromisos de seguridad de la información alcanzados.		
2. Se monitoriza y optimiza el impacto de la seguridad de la información sobre la disponibilidad, el rendimiento y la capacidad.		Porcentaje de incidentes de disponibilidad, rendimiento y capacidad por año causados por los controles de seguridad de la información.		
BAI04 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia. Evaluar la disponibilidad, el rendimiento y la capacidad de los servicios y recursos para asegurar que se encuentra disponible una capacidad y un rendimiento justificables en costes para dar soporte a las necesidades del negocio y para entregar el servicio de acuerdo a los ANSs. Crear líneas de referencia para la disponibilidad, el rendimiento y la capacidad para comparaciones futuras.	APO02.02	Capacidades de seguridad de la información	Listado de problemas de seguridad de la información técnicos y procedimentales relativos a la disponibilidad, el rendimiento y la capacidad	BAI04.02
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Identificar los problemas de seguridad de la información técnica y procedimental relativa a la disponibilidad, el rendimiento y la capacidad.				

Cuadro 30. BAI04 Gestionar la Disponibilidad y la Capacidad. Continuación.

Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI04.02 Evaluar el impacto en el negocio. Identificar los servicios importantes para la empresa, mapear los servicios y recursos con los procesos de negocio e identificar las dependencias de negocio. Asegurar que el impacto de la indisponibilidad de recursos está acordado y aceptado por el cliente. Asegurar que, para las funciones vitales del negocio, los requisitos de disponibilidad definidos en el ANS pueden ser satisfechos.	BAI04.01	Listado de problemas de seguridad de la información técnicos y procedimentales relativos a la disponibilidad, el rendimiento y la capacidad	Evaluaciones del impacto de la seguridad de la información sobre la disponibilidad, el rendimiento y la capacidad	BAI04.03
	BAI04.01			BAI04.03
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Evaluar el impacto en la seguridad de la información de potenciales faltas de disponibilidad, pérdidas de rendimiento y faltas de capacidad en la seguridad de la información.				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI04.03 Planificar para requisitos de servicios nuevos o modificados. Planificar y priorizar las implicaciones en la disponibilidad, el rendi-	BAI02.01	Requerimientos de seguridad de la información	Actualizaciones en los requerimientos de seguridad de la información	Interno

Cuadro 30. BAI04 Gestionar la Disponibilidad y la Capacidad. Continuación.				
miento y la capacidad de cambios en las necesidades del negocio y en los requerimientos de servicio.	BAI04.02	Evaluaciones del impacto de la seguridad de la información sobre la disponibilidad, el rendimiento y la capacidad		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Evaluar el impacto de requerimientos nuevos o modificados en la seguridad de la información.				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI04.04 Supervisar y revisar la disponibilidad y la capacidad. Supervisar, medir, analizar, informar y revisar la disponibilidad, el rendimiento y la capacidad. Identificar desviaciones respecto a la línea base establecida. Revisar informes de análisis de tendencias identificando cualquier cuestión y variación significativa, iniciando acciones donde sea necesario y asegurando que se realiza el seguimiento de todas las cuestiones pendientes.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				

Cuadro 30. BAI04 Gestionar la Disponibilidad y la Capacidad. Continuación.				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI04.05 Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad. Abordar las desviaciones investigando y resolviendo las cuestiones identificadas relativas a disponibilidad, rendimiento y capacidad.			Actualizaciones de las acciones correctivas para resolver las cuestiones relativas a la capacidad	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Valorar e investigar cualquier cuestión relativa a la seguridad de la información que impacte en la disponibilidad, el rendimiento y la capacidad.				
Fuente: Cobit 5 For Information Security				

Cuadro 31. BAI05 Gestionar la Introducción del Cambio Organizativo

BAI05 Gestionar la Introducción del Cambio Organizativo	
Descripción del Proceso COBIT 5 Maximizar la probabilidad de la implementación exitosa en toda la empresa del cambio organizativo de forma rápida y con riesgo reducido, cubriendo el ciclo de vida completo del cambio y a todas las partes interesadas del negocio y de TI.	
Declaración del Propósito del Proceso COBIT 5 Preparar y comprometer a las partes interesadas para el cambio en el negocio y reducir el riesgo de fracaso.	
BAI05 Objetivos y Métricas de Proceso específicos de seguridad	
Objetivos de Proceso específicos de seguridad	Métricas Relacionadas
1. Las alertas y tendencias en seguridad de la información son usadas de manera eficaz para facilitar el cambio en la organización e influir sobre la cultura corporativa en relación a la seguridad de la información.	Nivel de implicación de la alta dirección en los programas y estrategias de seguridad de la información Nivel de satisfacción de los actores que operan, utilizan y mantienen el cambio Porcentaje de usuarios formados adecuadamente para los cambios en seguridad de la información como parte del cambio organizacional

Cuadro 31. BAI05 Gestionar la Introducción del Cambio Organizativo. Continuación.				
2. Los protocolos relativos a la seguridad de la información se revisan y afinan como cambios corporativos a través de procesos de concienciación en el ámbito de la seguridad de la información.		Nivel de satisfacción de los usuarios con la adopción del cambio		
BAI05 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI05.01 Establecer el deseo de cambiar. Comprender el alcance e impacto del cambio divisado y la disposición/voluntad de cambiar de las partes interesadas. Identificar las acciones para motivar a las partes interesadas para aceptar y querer que el cambio sea exitoso.	BAI02.01	Requerimientos de seguridad de la información	Plan de comunicación con la alta dirección Procesos de control del cambio acordados en línea con guías de buenas prácticas	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Establecer una cultura proactiva en seguridad de la información				
2. Identificar y comunicar los puntos críticos o débiles relativos a seguridad de la información y también los comportamientos deseables, incluyendo los cambios necesarios para abordar estos puntos.				
3. Proporcionar liderazgo visible a través del compromiso de la alta dirección (al más alto nivel, CxO) con la seguridad de la información para facilitar los cambios.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI05.02 Formar un equipo de implementación efectivo. Establecer un equipo de implemen				

Cuadro 31. BAI05 Gestionar la Introducción del Cambio Organizativo. Continuación				
tación efectivo, con miembros adecuados, creando confianza y estableciendo metas comunes y medidas efectivas.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Habilidades personales	Equipos de implementación de seguridad de la información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Designar profesionales de la seguridad de la información cualificados para servir en los equipos de implementación.				
2. Desarrollar una visión común para todo el equipo de seguridad de la información.				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI05.03 Comunicar la visión deseada. Comunicar la visión deseada para el cambio en el lenguaje de aquellos que se verán afectados. La comunicación debería ser realizada por la alta dirección e incluir la razón de ser y los beneficios del cambio, el impacto de no hacerlo y la visión, la hoja de ruta y la participación requerida de las diversas partes interesadas.	APO02.06 Fuera del ámbito de COBIT 5 para seguridad de la Información	Plan de seguridad de la información Declaración corporativas de la visión/misión	Plan de comunicación de la visión referente a seguridad de la información	BAI05.04
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Comunicar la visión relativa a seguridad de la información como apoyo a la visión corporativa.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI05.04 Facultar a los que juegan algún papel e identificar ganancias en el corto plazo.				

Cuadro 31. BAI05 Gestionar la Introducción del Cambio Organizativo. Continuación				
<p>identificar ganancias en el corto plazo. Facultar a aquellos con roles en la implementación asegurando que se han asignado las responsabilidades, se ha dado formación y se han alineado las estructuras organizativas y procesos de RRHH. Identificar y comunicar ganancias en el corto plazo que pueda ser realizadas y resulten importantes desde una perspectiva de posibilitar el cambio.</p>	APO02.05	Hoja de ruta estratégica de seguridad de la información	Lista de los beneficios potenciales a corto plazo	BAI05.05
	APO02.06	Plan de seguridad de la información		
	BAI05.03	Plan de comunicación de la visión relativa a seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Alinear las prácticas de seguridad de la para apoyar la visión.				
2. Asignar de manera clara la responsabilidad de cada persona del equipo e incluir criterios de rendimiento para a establecer quiénes son los responsables de que se lleve a cabo el proceso.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
<p>BAI05.05 Facilitar la operación y el uso. Planificar e implementar todos los aspectos técnicos, operativos y de modo de uso de forma que todos aquellos involucrados en el entorno futuro puedan ejercer sus responsabilidades.</p>				
	BAI05.04	Lista de los beneficios potenciales a corto plazo	Medidas prácticas de seguridad de la información	BAI05.06
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Desarrollar medidas prácticas de seguridad de la información.				

Cuadro 31. BAI05 Gestionar la Introducción del Cambio Organizativo. Continuación				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI05.06 Integrar nuevos enfoques. Integrar nuevos enfoques mediante el seguimiento de los cambios implementados, asegurando la efectividad del plan de operación y uso y manteniendo un plan de concienciación mediante comunicaciones regulares. Aplicar las medidas correctoras que se estime apropiado y que podrían incluir el forzar el cumplimiento.	BAI05.05	Medidas prácticas de seguridad de la información	Prácticas operativas de seguridad de la información	Interno
Security-specific Activities (in Addition to COBIT 5 Activities)				
1. Hacer seguimiento continuo de la concienciación en seguridad de la información y adaptar pertinentemente las métricas.				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI05.07 Mantener los cambios. Mantener los cambios mediante la formación eficaz del personal nuevo, campañas de comunicación periódicas, compromiso de la alta dirección, supervisión de la adopción de los cambios y divulgación a toda la empresa de las lecciones aprendidas.				
			Revisiones del uso operativo	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Informar y formar al nuevo personal y proporcionar sesiones de actualización de concienciación en seguridad de la información.				

Cuadro 32. BAI06 Gestionar los Cambios

BAI06 Gestionar los Cambios				
<p>Descripción del Proceso COBIT 5 Gestione todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, informes, cierre y documentación.</p>				
<p>Declaración del Propósito del Proceso COBIT 5 Posibilitar una entrega de los cambios rápida y fiable para el negocio, al a vez que se mitiga cualquier riesgo que impacte negativamente en la estabilidad e integridad del entorno en que se aplica el cambio.</p>				
BAI06 Objetivos y Métricas de Proceso específicas de seguridad				
Objetivos de Proceso específicos de seguridad		Métricas Relacionadas		
1. Los requerimientos de seguridad de la información se incorporan durante la evaluación del impacto del cambio en los procesos, aplicaciones e infraestructuras.		Número de cambios relevantes en cuanto a seguridad de la información y número de cambios que tengan impacto en la seguridad de la información. Número de requerimientos de seguridad de la información que no se han cumplido después del cambio.		
2. Los cambios de emergencia tienen en cuenta los requerimientos necesarios de seguridad de la información.		Número de incidentes de seguridad de la información relativos a los cambios en el entorno. Número de incidentes de seguridad de la información relativos a cambios en hardware y software.		
BAI06 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio. Evaluar todas las peticiones de cambio para determinar su impacto en los procesos de negocio y los servicios TI, y analizar si el cambio afectará negativamente al entorno operativo e introducirá un riesgo inaceptable. Asegurar que los cambios son registrados, priorizados,				

Cuadro 32. BAI05 Gestionar la Introducción del Cambio Organizativo. Continuación				
registrados, priorizados, categorizados, analizados, autorizados, planificados y programados.			Evaluaciones de impacto	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que se realiza una evaluación del impacto potencial de los cambios en seguridad de la información.				
2. Asegurar que la política de seguridad de la información se adapta a los objetivos de negocio de la empresa.				
3. Asegurar que los cambios están conformes con la política de seguridad de la información.				
4. Desarrollar prácticas que tengan en cuenta el impacto de nuevas tecnologías y tendencias en la seguridad de la información.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI06.02 Gestionar cambios de emergencia. Gestionar cuidadosamente los cambios de emergencia para minimizar futuras incidencias y asegurar que el cambio está controlado y se realiza de forma segura. Verificar que los cambios de emergencia son evaluados debidamente y autorizados de una vez hecho el cambio.			Revisión de seguridad de la información post-implementación de los cambios de emergencia	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Desarrollar medidas que contemplen los cambios de emergencia y mantenimiento sin comprometer la seguridad de la información.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI06.03 Hacer seguimiento e informar de cambios de estado. Mantener un sistema de seguimiento e informe que documente los cambios recha-				

Cuadro 32. BAI05 Gestionar la Introducción del Cambio Organizativo. Continuación				
zados, comunique el estado de cambios aprobados y en proceso y de cambios completados. Asegurar que los cambios aprobados son implementados como esté previsto.			Informes actualizados del estado de las solicitudes de cambio	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Abordar las cuestiones de rendimiento y capacidad potenciales resultantes de los cambios propuestos en seguridad de la información.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI06.04 Cerrar y documentar los cambios. Siempre que el cambio haya sido implementado, actualizar, de manera consecuente, la documentación de la solución y del usuario, así como los procedimientos a los que afecta el cambio.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
2. Para asegurar un seguimiento adecuado, mantener un registro de riesgos en la información cuando se introduzca un nuevo riesgo a raíz de un cambio de emergencia.				
Fuente: Cobit 5 For Information Security				

Cuadro 33. BAI07 Gestionar la Aceptación del Cambio y la Transición

BAI07 Gestionar la Aceptación del Cambio y la Transición
<p>Descripción del Proceso COBIT 5</p> <p>Aceptar formalmente y hacer operativas las nuevas soluciones, incluyendo la planificación de la implementación, la conversión de los datos y los sistemas, las pruebas de aceptación, la comunicación, la preparación del lanzamiento, el paso a producción de procesos de negocio o servicios TI nuevos o modificados, el soporte temprano en producción y una revisión post-implementación.</p>

Cuadro 33. BAI07 Gestionar la Aceptación del Cambio y la Transición. Continuación.				
Declaración de Propósito del Proceso COBIT 5 Implementar soluciones de forma segura y en línea con las expectativas y resultados acordados.				
BAI07 Objetivos y Métricas de Proceso específicos de Seguridad				
Objetivos de Proceso específicos de Seguridad		Métricas Relacionadas		
1. Las pruebas de seguridad de la información son parte integral de las pruebas de aceptación.		Número de cambios relacionados con la seguridad de la información que han sido fallidos o no han sido implementados Porcentaje de cambios relacionados con la seguridad de la información aceptados		
2. Las mejoras de seguridad de la información identificadas se incorporarán en futuros lanzamientos.		Número de cuestiones abiertas de seguridad de la información por lanzamiento Cambios en el número de cuestiones de seguridad de la información no resueltas por lanzamiento Porcentaje de pruebas de seguridad de la información completadas en los cambios		
BAI07 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI07.01 Establecer un plan de implementación. Establecer un plan de implementación que cubra la conversión de datos y sistemas, criterios de aceptación de las pruebas, comunicación, formación, preparación del lanzamiento, paso a producción, soporte inicial en producción, plan de marcha atrás o de contingencia y una revisión post-implantación. Obtener la aprobación de las partes relevantes.	Fuera del ámbito de COBIT 5 para seguridad de la Información	Plan de Implementación TI	Plan de Implementación TI actualizado	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Incluir aspectos de seguridad de la información en la aceptación y en el plan de implementación de la transición.				

Cuadro 33. BAI07 Gestionar la Aceptación del Cambio y la Transición. Continuación.				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI07.02 Planificar la conversión de procesos de negocio, sistemas y datos. Preparar la migración de procesos de negocio, datos de los servicios de TI e infraestructuras como parte de los mecanismos de desarrollo de la empresa, incluyendo registros de auditoría y un plan de recuperación para el caso de que la migración fallara.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI07.03 Planificar pruebas de aceptación. Establecer un plan de pruebas basado en estándares corporativos que defina roles, responsabilidades, y criterios de entrada y salida. Asegurar que el plan es aprobado por las partes relevantes.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Planes de prueba	Medidas de seguridad de la información en el entorno de prueba	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que las pruebas de aceptación de seguridad de la información son parte del plan de pruebas.				

Cuadro 33. BAI07 Gestionar la Aceptación del Cambio y la Transición. Continuación.				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI07.04 Establecer un entorno de pruebas. Definir y establecer un entorno seguro de pruebas que sea representativo del proceso de negocio y entorno de operaciones de TI planeados, en cuanto a rendimiento y capacidad, seguridad, controles internos, prácticas de operación, calidad de los datos y requisitos de privacidad y carga de trabajo.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Datos y arquitectura de entorno de pruebas	Entorno de pruebas seguro	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que existen los controles de seguridad de la información adecuados en el entorno de pruebas (p.ej. anonimato de los datos sensibles).				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI07.05 Ejecutar pruebas de aceptación. Probar los cambios independientemente, de acuerdo con el plan de pruebas definido, antes de migrar al entorno de producción.	Fuera de COBIT 5 para Seguridad de la Información	Pruebas de aceptación	Pruebas de aceptación actualizadas	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Desarrollar y ejecutar las pruebas de aceptación de seguridad de la información.				

Cuadro 33. BAI07 Gestionar la Aceptación del Cambio y la Transición. Continuación.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI07.06 Pasar a producción y gestionar los lanzamientos. Pasar la solución aceptada al negocio y las operaciones. Donde sea apropiado, ejecutar la solución como un proyecto piloto o en paralelo con la solución antigua durante un período de tiempo definido y comparar su comportamiento y resultados. Si se dieran problemas significativos, reinstaurar el entorno original de acuerdo al plan de marcha atrás o alternativo. Gestionar los lanzamientos de los componentes de la solución.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Planes de lanzamiento	Planes de lanzamiento actualizados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que la seguridad de la información es gestionada durante el paso a producción y la gestión del lanzamiento.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI07.07 Proporcionar soporte en producción desde el primer momento. Proporcionar soporte desde el primer momento a los usuarios y a las operaciones de TI durante un				

Cuadro 33. BAI07 Gestionar la Aceptación del Cambio y la Transición. Continuación.				
periodo de tiempo acordado para tratar cualquier incidencia y ayudar a estabilizar la nueva solución.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI07.08 Ejecutar una revisión post-implantación. Llevar a cabo una revisión post-implantación para confirmar salidas y resultados, identificar lecciones aprendidas y desarrollar un plan de acción. Evaluar y verificar el rendimiento actual y las salidas del servicio nuevo o modificado respecto al rendimiento y salidas previstas (es decir, el servicio esperado por el usuario o el cliente).	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Informes de la revisión post-implantación	Informes de la revisión post-implantación actualizados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que la seguridad de la información se incluye en la revisión post-implantación.				
Fuente: Cobit 5 For Information Security				

Cuadro 34. BAI08 Gestionar el Conocimiento

BAI08 Gestionar el Conocimiento				
<p>Descripción del Proceso COBIT 5 Mantener la disponibilidad de conocimiento relevante, actual, validado y fiable para dar soporte a todas las actividades de los procesos y facilitar la toma de decisiones. Planificar la identificación, recopilación, organización, mantenimiento, uso y retirada de conocimientos.</p>				
<p>Declaración de Propósito del Proceso COBIT 5 Proporcionar el conocimiento necesario para dar soporte a todo el personal en sus actividades laborales, para la toma de decisiones bien fundadas y para aumentar la productividad.</p>				
BAI08 Objetivos y Métricas de Proceso específicos de Seguridad				
Tabla 40. BAI08 Gestionar el Conocimiento				
Objetivos de Proceso específicos de Seguridad			Métricas Relacionadas	
1. Se asegura la compartición del conocimiento con las salvaguardas adecuadas.			Número de eventos de fuga de información Número de empleados formados en seguridad de la información Porcentaje de categorías de seguridad de la información cubiertas	
BAI08 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI08.01 Cultivar y facilitar una cultura de intercambio de conocimientos. Concebir e implantar un esquema para cultivar y facilitar una cultura de intercambio de conocimientos.	APO01.04	Programa de concienciación y formación en seguridad de la información	Medidas de prevención de pérdida de información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que existen medidas adecuadas de prevención de pérdida de la				
2. Proporcionar formación para la concienciación en seguridad de la información en relación al intercambio de información.				
3. Incorporar consideraciones de seguridad de la información en el ciclo de vida de la información corporativa.				

Cuadro 34. BAI08 Gestionar el Conocimiento. Continuación.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI08.02 Identificar y clasificar las fuentes de información. Identificar, validar y clasificar las diversas fuentes de información interna y externa necesarias para posibilitar el uso y la operación efectivos de los procesos de negocio y los servicios de TI.			Clasificación de fuentes de información actualizada	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Dar soporte al uso y al intercambio de información en relación a su clasificación y sensibilidad.				
Tabla 40. BAI08 Gestionar el Conocimiento				
2. Desarrollar una estructura para categorizar los sistemas.				
3. Desarrollar una estructura para clasificar la información.				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI08.03 Organizar y contextualizar la información, transformándola en conocimiento. Organizar la información basándose en criterios de clasificación. Identificar y crear relaciones significativas entre elementos de información y facilitar el uso de la información. Identificar propietarios y definir e implementar niveles de acceso a los recursos de información.			Repositorios de conocimiento publicados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Mapear roles con áreas de conocimiento y asegurar que se han establecido controles de acceso apropiados para la información relevante.				

Cuadro 34. BAI08 Gestionar el Conocimiento. Continuación.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI08.04 Utilizar y compartir el conocimiento. Difundir las fuentes de conocimiento disponibles entre las partes interesadas relevantes y comunicar cómo estos recursos pueden ser utilizados para tratar diferentes necesidades (ej. resolución de problemas, aprendizaje, planificación estratégica y toma de decisiones).			Control de acceso actualizado	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que existen medidas adecuadas para la prevención de la pérdida de información.				
2. Implementar controles de acceso mediante el uso de políticas y procesos que restrinjan el uso y el intercambio no autorizado de información.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI08.05 Evaluar y retirar la información. Medir el uso y evaluar la actualización y relevancia de la información. eliminar la información obsoleta.			Reglas actualizadas para la eliminación de la información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Deshacerse de forma segura de la información. Incluir el borrado de datos de trazabilidad (datos personales/leyes de privacidad)				
2. Mantener y documentar una pista de auditoría sólida/aceptada para la información.				
3. Alinear las medidas de seguridad de la información relevantes a la clasificación.				
4. Desarrollar políticas y procesos de destrucción segura de la información.				
Fuente: Cobit 5 For Information Security				

Cuadro 35. BAI09 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso

BAI09 Gestionar los Activos				
BAI09 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI09.01 Identificar y registrar los activos actuales. Mantener un registro actualizado y exacto de todos los activos de TI necesarios para la prestación de servicios y garantizar su alineación con la gestión de la configuración y la administración financiera	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Inventario de activos	Requerimientos de seguridad de la información para los activos TI	BAI09.02
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Identificar dependencias entre los activos.				
2. Identificar los requisitos de seguridad de la información para los activos actuales y considerar las dependencias.				
3. Abordar la seguridad de la información para los activos TI, datos y formularios, etc.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI09.02 Gestionar Activos Críticos. Identificar los activos que son críticos en la provisión de servicio y dar los pasos para maximizar su fiabilidad y disponibilidad para apoyar	BAI09.01	Requerimientos de seguridad de la información para los activos TI	Niveles de criticidad de los activos de TI	BAI09.03

Cuadro 35. BAI09 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso. Continuación.				
las necesidades del negocio.	BAI09.01			
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir los niveles de criticidad e identificar la criticidad de los activos en un registro de activos.				
2. Hacer cumplir los requisitos de seguridad de la información de los activos.				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI09.03 Gestionar el ciclo de vida de los activos Gestionar los activos desde su adquisición hasta su eliminación para asegurar que se utilizan tan eficaz y eficientemente como sea posible y son contabilizados y protegidos físicamente.	BAI09.02	Niveles de criticidad de los activos TI	Procedimientos de gestión de activos actualizados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Identificar y comunicar el riesgo de incumplimientos de seguridad de la información en relación al ciclo de vida de los activos.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI09.04 Optimizar el coste de los activos. Revisar periódicamente la base global de activos para identificar maneras de optimizar los costes y mantener el alineamiento con las necesidades del negocio.				

Cuadro 35. BAI09 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso. Continuación.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI09.05 Administrar Licencias. Administrar las licencias de software de forma que se mantenga el número óptimo de licencias para soportar los requerimientos de negocio y el número de licencias en propiedad sea suficiente para cubrir el software instalado y en uso.			Registro actualizado de licencias de software	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Establecer un procedimiento para el control de las instalaciones de software y otros activos de TI.				
2. Realizar verificaciones periódicas de la red para detectar software no autorizado.				
2. Asegurar que las medidas y los requerimientos de seguridad de la información se cumplen durante todo el ciclo de vida.				
Fuente: Cobit 5 For Information Security				

Cuadro 36. BAI10 Gestionar la Configuración

BAI10 Gestionar la Configuración
<p>Descripción del Proceso COBIT 5</p> <p>Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarias para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración.</p>

Cuadro 36. BAI10 Gestionar la Configuración. Continuación				
Declaración de Propósito del Proceso COBIT 5 Proporcionar suficiente información sobre los activos de servicio para que el servicio pueda gestionarse con eficacia, evaluar el impacto de los cambios y hacer frente a los incidentes de servicio.				
BAI10 Objetivos y Métricas de Proceso específicos de Seguridad				
Objetivos de Proceso específicos de Seguridad			Métricas Relacionadas	
1. Se aprueban, implementan y mantienen en toda la empresa líneas de referencia de configuración de seguridad de la información.			Número de veces que se han revisado y validado las líneas de referencia basado en un lapso predeterminado o cambios importantes y tiempo transcurrido Número de discrepancias entre las líneas de referencia estándar de seguridad de la información y las configuraciones reales	
BAI10 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
Práctica de Gestión	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
BAI10.01 Establecer y mantener un modelo de configuración. Establecer y mantener un modelo lógico de la infraestructura, activos y servicios y la forma de registrar los elementos de configuración (CIs del inglés, configuration items) y las relaciones entre ellos. Incluyendo los CIs considerados necesarios para gestionar eficazmente los servicios y proporcionar una sola descripción fiable de los activos en un servicio.			Alertas y eventos que sean seguridad de la información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				

Cuadro 36. BAI10 Gestionar la Configuración. Continuación				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI10.02 Establecer y mantener un repositorio de configuración y una línea de referencia Establecer y mantener un repositorio de gestión de la configuración y crear unas bases de referencia de configuración controladas.			Informe de evaluación de vulnerabilidades	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Incluir una configuración de seguridad de la información para los elementos configurables como servidores/hardware, dispositivos de red y dispositivos finales.				
2. Identificar requerimientos de seguridad de la información para los activos actuales y tener en cuenta las dependencias.				
3. Supervisar el cumplimiento con las líneas de referencia de configuración de seguridad establecida y aprobada y con sus actualizaciones.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI10.03 Mantener y controlar los elementos de configuración. Mantener un repositorio actualizado de elemento de configuración relleno con los cambios.			Plan de gestión de la configuración	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI10.04 Generar informes de estado y de configuración.				

Cuadro 36. BAI10 Gestionar la Configuración. Continuación				
Definir y elaborar informes de configuración sobre cambios en el estado de los elementos de configuración.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI10.05 Verificar y revisar la integridad del repositorio de configuración. Revisar periódicamente el repositorio de configuración y verificar la integridad y exactitud con respecto al objetivo deseado.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
Fuente: Cobit 5 For Information Security				

5.2.2.4 Entrega, Servicio y Soporte (DSS)

Cuadro 37. DSS01 Gestionar Operaciones

DSS01 Gestionar Operaciones
<p>Descripción del Proceso</p> <p>Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.</p>
<p>Declaración del Propósito del Proceso</p> <p>Entregar los resultados del servicio operativo de TI, según lo planificado.</p>
<p>DSS01 Objetivos y Métricas del Proceso específicas de Seguridad</p>

Cuadro 37. DSS01 Gestionar Operaciones. Continuación				
Objetivos de Proceso específicos de Seguridad		Métricas Relacionadas		
1. Las operaciones de seguridad de la información son realizadas de acuerdo a un plan operativo de seguridad de la información, en línea con la estrategia de seguridad de la información		Número de incidentes de seguridad de la información causados por problemas operativos		
2. Los estándares de seguridad de la información aplicables están identificados y se cumplen		Número de cuestiones de seguridad de la información no contempladas por estándares de seguridad de la información Número de estándares de seguridad de la información no abordados o satisfechos por el plan operativo de seguridad de la información.		
2. Los estándares de seguridad de la información aplicables están identificados y se cumplen		Número de cuestiones de seguridad de la información no contempladas por estándares de seguridad de la información Número de estándares de seguridad de la información no abordados o satisfechos por el plan operativo de seguridad de la información		
DSS01 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
Prácticas de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	De	Descripción	Descripción	A
DSS01.01 Ejecutar procedimientos operativos. Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.	APO03.05	Guía de implementación del servicio de arquitectura de seguridad de la información	Procedimientos operativos de seguridad de la información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Verificar que los procedimientos operativos de seguridad de la información relevantes están incluidos en los procedimientos operativos ordinarios.				
2. Asegurar que el ciclo de vida de procesamiento de la información (recepción, procesamiento, almacenamiento y salida) incorpora la política de seguridad de la información y los requerimientos regulatorios.				
3. Asegurar que las operaciones de seguridad de la información son planificadas, ejecutadas y controladas de acuerdo con el plan operativo.				
4. Aplicar seguridad de la información y derechos de acceso a todos los datos.				

Cuadro 37. DSS01 Gestionar Operaciones. Continuación				
Prácticas de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	De	Descripción	Descripción	A
DSS01.02 Gestionar servicios externalizados de TI. Gestionar la operación de servicios externalizados de TI para mantener la protección de la información empresarial y la confiabilidad de la entrega del servicio.			Planes de aseguramiento de terceros	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar y supervisar activamente el cumplimiento de terceros con las políticas, estándares y requerimientos de seguridad de la información de la empresa.				
Prácticas de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	De	Descripción	Descripción	A
DSS01.03 Supervisar la infraestructura de TI. Supervisar la infraestructura TI y los eventos relacionados con ella. Almacenar la suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias de tiempo de las operaciones y las actividades relacionadas con el soporte a esas operaciones.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Reglas de monitorización de activos y estado de eventos	Reglas de monitorización de activos actualizadas	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que TI supervisa activamente aspectos de seguridad de la información de la infraestructura de TI, tales como configuración, operaciones, acceso y uso.				

Cuadro 37. DSS01 Gestionar Operaciones. Continuación				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS01.04 Gestionar el entorno. Mantener las medidas para la protección contra factores ambientales. Instalar equipamiento y dispositivos especializados para supervisar y controlar el entorno.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Políticas de seguridad física y ambiental	Políticas de seguridad ambiental actualizadas	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que la gestión del entorno se adhiere a los requerimientos de seguridad de la información.				
Prácticas de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	De	Descripción	Descripción	A
DSS01.05 Gestionar las instalaciones. Gestionar las instalaciones, incluyendo equipos de electricidad y comunicaciones, en línea con las leyes y regulaciones,	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Informes de evaluación de instalaciones	Informes de evaluación de instalaciones actualizados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que la gestión de instalaciones se adhiere a los requerimientos de seguridad de la información.				
Fuente: Cobit 5 For Information Security				

Cuadro 38. DSS02 Gestionar Peticiones e Incidentes de Servicio.

DSS02 Gestionar Peticiones e Incidentes de Servicio				
<p>Descripción del Proceso Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.</p>				
<p>Declaración del Propósito del Proceso Lograr una mayor productividad y minimizar las interrupciones mediante la rápida resolución de consultas de usuario e incidentes.</p>				
DSS02 Objetivos y Métricas del Proceso específicas de Seguridad				
Objetivos del Proceso específicos de Seguridad		Métricas Relacionadas		
<p>1. Se ha establecido y se mantiene un programa de respuesta ante incidentes de seguridad de la información</p>		<p>Tiempo promedio de resolución de incidencias de seguridad Número y porcentaje de incidentes relacionados con seguridad de la información que causan interrupción en los procesos críticos de negocio Número de incidentes de seguridad de la información abiertos/cerrados y sus niveles de riesgo Frecuencia de pruebas del plan de respuesta ante incidentes de seguridad de la información</p>		
DSS02 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
Prácticas de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	De	Descripción	Descripción	A
DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio. Definir esquemas y modelos de clasificación de incidentes y peticiones de servicio.			Esquema de clasificación de incidentes de seguridad de la información	DSS02.02
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
<p>1. Definir y comunicar la naturaleza y las características de los potenciales incidentes relacionados con seguridad para que puedan ser fácilmente reconocidos y su impacto entendido y, así, permitir una respuesta adecuada.</p>				

Cuadro 38. DSS02 Gestionar Peticiones e Incidentes de Servicio. Continuación				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes. Identificar, registrar y clasificar peticiones de servicio e incidentes, y asignar una prioridad según la criticidad del negocio y los acuerdos de servicio.	DSS02.01	Esquema de clasificación de	Incidentes y peticiones de servicio de seguridad de la información clasificados y priorizados	APO08.03 APO12.01 APO13.03 DSS02.07
	DSS05.07	Tiques de incidentes de seguridad		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Mantener un procedimiento de investigación y respuesta de incidentes de seguridad de la información. Asegurar que se han puesto medidas para proteger la confidencialidad de la información relativa a incidentes de seguridad y que todo el personal está al corriente del procedimiento.				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS02.03 Verificar, aprobar y resolver peticiones de servicio. Seleccionar los procedimientos adecuados para peticiones y verificar que las peticiones de servicio cumplen los criterios de petición definidos				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				

Cuadro 38. DSS02 Gestionar Peticiones e Incidentes de Servicio. Continuación				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS02.04 Investigar, diagnosticar y localizar incidentes. Identificar y registrar síntomas de incidentes, determinar posibles causas y asignar recursos a su resolución.			Procedimientos de recogida de evidencias	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Mantener un procedimiento de recogida de evidencias en línea con las normas de evidencias forenses locales y asegurar que todo el personal está al corriente del procedimiento.				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS02.05 Resolver y recuperarse ante incidentes. Documentar, solicitar y probar las soluciones identificadas o temporales y ejecutar acciones de recuperación para restaurar el servicio TI relacionado.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Análisis de impacto en el negocio, política de gestión del riesgo organizativo, esquema de clasificación de incidentes	Plan de respuesta ante incidentes	DSS02.07
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir un plan de respuesta ante incidentes de seguridad de la información.				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS02.06 Cerrar peticiones de servicio				

Cuadro 38. DSS02 Gestionar Peticiones e Incidentes de Servicio. Continuación				
e incidentes. Verificar la satisfactoria resolución de incidentes y/o satisfactorio cumplimiento de peticiones, y cierre.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS02.07 Seguir el estado y emitir de informes. Hacer seguimiento, analizar e informar de incidentes y tendencias de cumplimiento de peticiones, regularmente, para proporcionar información para la mejora continua.	DSS02.02	Incidentes y peticiones de servicio de seguridad de la información clasificados y priorizados	Lecciones aprendidas	Interno
	DSS02.05	Plan de respuesta ante incidentes		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Reportar los resultados de las investigaciones de incidentes de seguridad a los grupos de interés oportunos, incluyendo informes periódicos a la dirección ejecutiva.				
2. Asegurar que los incidentes de seguridad y las acciones de seguimiento oportunas, incluyendo análisis de la causa raíz, siguen los procesos de gestión de problemas e incidentes existentes.				
Fuente: Cobit 5 For Information Security				

Cuadro 39. DSS03 Gestionar Problemas

DSS03 Gestionar Problemas				
<p>Descripción del Proceso Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.</p>				
<p>Declaración del Propósito del Proceso Incrementar la disponibilidad, mejorar los niveles de servicio, reducir costes, y mejorar la comodidad y satisfacción del cliente reduciendo el número de problemas operativos.</p>				
<p>DSS03 Objetivos y Métricas del Proceso específicas de Seguridad</p>				
Objetivos del Proceso específicos de Seguridad		Métricas Relacionadas		
<p>1. Los problemas de seguridad de la información son resueltos de una forma sostenible</p>		<p>Número de problemas de seguridad de la información recurrentes que permanecen sin resolver. Número de problemas relativos a seguridad de la información para los que se ha encontrado una solución satisfactoria que contempla cuestiones críticas de seguridad de la información</p>		
<p>DSS03 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso</p>				
Prácticas de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	De	Descripción	Descripción	A
<p>DSS03.01 Identificar y clasificar problemas. Definir e implementar criterios y procedimientos para informar de los problemas identificados, incluyendo clasificación, categorización y priorización de problemas.</p>	<p>Fuera del ámbito de COBIT 5 para Seguridad de la Información</p>	<p>Análisis de vulnerabilidades</p>	<p>Esquema de clasificación de problemas de seguridad de la información</p>	<p>DSS03.04</p>
<p>Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)</p>				
<p>1. Clasificar, categorizar y priorizar los problemas de seguridad de la información.</p>				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
<p>DSS03.02 Investigar</p>				

Cuadro 39. DSS03.02 Investigar. Continuación				
y diagnosticar problemas. Investigar y diagnosticar problemas utilizando expertos en las materias relevantes para valorar y analizar las causas raíz.			Causas raíz de los problemas actualizadas Causas raíz de los problemas actualizadas	Interno Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Investigar los problemas de seguridad de la información.				
Prácticas de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	De	Descripción	Descripción	A
DSS03.03 Levantar errores conocidos. Tan pronto como las causas raíz de los problemas se hayan identificado, crear registros de errores conocidos y una solución temporal apropiada, e identificar soluciones potenciales.			Registros de errores conocidos actualizados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Escalar los problemas de seguridad de la información cuando sea necesario.				
Prácticas de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	De	Descripción	Descripción	A
DSS03.04 Resolver y cerrar problemas. Identificar e iniciar soluciones sostenibles refiriéndose a la causa raíz, levantando peticiones de cambio a través del proceso de gestión de cambios establecido si se requiere para resolver errores.				

Cuadro 39. DSS03.02 Investigar. Continuación				
Cuadro 39. DSS03 Gestionar Problemas				
Asegurarse de que el personal afectado está al tanto de las acciones tomadas y de los planes desarrollados para prevenir que vuelvan a ocurrir futuros incidentes	DSS03.01	Esquema de clasificación de problemas de seguridad de la información	Causa raíz de los problemas	DSS03.05
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Realizar análisis de causa raíz, resolver problemas de seguridad de la información y actualizar el plan de respuesta ante incidentes. Hacer seguimiento y registrar los problemas de seguridad de la información.				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS03.05 Realizar una gestión de problemas proactiva. Recoger y analizar datos operacionales (especialmente registros de incidentes y cambios) para identificar tendencias emergentes que puedan indicar problemas. Registrar problemas para permitir la valoración.	DSS03.04	Causa raíz de problemas	Implementación de políticas y procedimientos de seguridad de la información.	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Analizar y aprovechar las lecciones aprendidas.				
Fuente: Cobit 5 For Information Security				

Cuadro 40. DSS04 Gestionar la Continuidad

DSS04 Gestionar la Continuidad				
<p>Descripción del Proceso Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.</p>				
<p>Declaración del Propósito del Proceso de COBIT 5 Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa.</p>				
DSS04 Objetivos y Métricas del Proceso específicas de Seguridad				
Objetivos del Proceso específicos de Seguridad			Métricas Relacionadas	
1. El riesgo de la información se ha identificado adecuadamente y se incluye en los planes de continuidad de las tecnologías de la información y comunicaciones (TIC)			Número de invocaciones al plan causadas por incidentes de seguridad de la información Número de incidentes de seguridad de la información escalados para la activación de la continuidad TIC	
			activación de la continuidad TIC Número de sistemas de seguridad de la información críticos cubiertos por el plan de continuidad TIC.	
DSS04 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS04.01 Definir la política de continuidad de negocio, objetivos y alcance. Definir la política y alcance de continuidad de negocio alineada con los objetivos de negocio y de las partes interesadas.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Política para la continuidad de negocio	Política para la continuidad de negocio actualizada	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que la seguridad de la información forma parte del ciclo de vida de la continuidad de negocio.				

Cuadro 40. DSS04 Gestionar la Continuidad. Continuación				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS04.02 Mantener una estrategia de continuidad. Evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Análisis de impacto en el negocio (AIN)	Análisis de impacto en el negocio (AIN) actualizado	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Incluir escenarios que tengan en cuenta la seguridad de la información.				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio. Desarrollar un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para facilitar que la empresa continúe con sus actividades críticas	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Plan de continuidad de negocio (PCN)	Plan de continuidad de negocio (PCN) actualizado	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Incluir requerimientos de seguridad de la información en el plan de continuidad de negocio (PCN)				

Cuadro 40. DSS04 Gestionar la Continuidad. Continuación				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS04.04 Ejercitar, probar y revisar el BCP. Probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS04.05 Revisar, mantener y mejorar el plan de continuidad. Realizar una revisión por la Dirección de la capacidad de continuidad a intervalos regulares para asegurar su continua idoneidad, adecuación y efectividad. Gestionar los cambios en el plan de acuerdo al proceso de control de cambios para asegurar que el plan de continuidad se mantiene actualizado y refleja continuamente los requerimientos actuales del negocio.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Plan de continuidad de negocio (PCN)	Plan de continuidad de negocio (PCN) actualizado	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				

Cuadro 40. DSS04 Gestionar la Continuidad. Continuación				
1. Considerar los incidentes de seguridad de la información como disparadores importantes para mejorar el plan de continuidad de negocio (PCN)				
Prácticas de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	De	Descripción	Descripción	A
DSS04.06 Proporcionar formación en el plan de continuidad. Proporcionar a todas las partes implicadas, internas y externas, de sesiones formativas regulares que contemplen los procedimientos y sus roles y responsabilidades en caso de interrupción.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
Prácticas de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	De	Descripción	Descripción	A
DSS04.07 Gestionar acuerdos de respaldo. Mantener la disponibilidad de la información crítica del negocio.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Resultados de pruebas de datos de respaldo	Resultados de pruebas de datos de respaldo actualizados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que los acuerdos de copia de respaldo y recuperación incluyen requerimientos de seguridad de la información.				
Prácticas de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	De	Descripción	Descripción	A
DSS04.08 Ejecutar revisiones post-reanudación. Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una interrupción.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Informes de revisión post-reanudación	Informes de revisión post-reanudación actualizados	Interno

Cuadro 40. DSS04 Gestionar la Continuidad. Continuación
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)
10. Asegurar que las revisiones pos-reanudación incluyen la seguridad de la información.
Fuente: Cobit 5 For Information Security

Cuadro 41. DSS05 Gestionar Servicios de Seguridad

DSS05 Gestionar Servicios de Seguridad	
<p>Descripción del Proceso Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.</p>	
<p>Declaración del Propósito del Proceso Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.</p>	
<p>DSS05 Objetivos y Métricas del Proceso específicas de Seguridad</p>	
Objetivos del Proceso específicos de Seguridad	Métricas Relacionadas
1. La seguridad de las redes y las comunicaciones cubre con las necesidades del negocio.	Número de vulnerabilidades descubiertas Número de rupturas (breaches) de cortafuegos
2. La información procesada, almacenada y transmitida en los dispositivos de usuario finales está protegida.	Porcentaje de individuos que reciben formación de concienciación relativa al uso de dispositivos de usuario finales Número de incidentes que impliquen dispositivos de usuario finales Número de dispositivos de usuario finales no autorizados detectados en la red o en el entorno
3. Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en el negocio.	Promedio de tiempo entre los cambios y actualizaciones de cuentas Número de cuentas (con respecto al número de usuarios/empleados autorizados)
4. Se han implantado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida.	Porcentaje de pruebas periódicas de los dispositivos de seguridad del entorno Clasificación media para las evaluaciones de seguridad física Número de incidentes relacionados con seguridad física

Cuadro 41. DSS05 Gestionar Servicios de Seguridad. Continuación.				
5. La información electrónica tiene las medidas de seguridad apropiadas mientras está almacenada, transmitida o destruida.		Número de incidentes relacionados con accesos no autorizados a la información		
DSS05 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del proceso.				
Prácticas de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	De	Descripción	Descripción	A
DSS05.01 Proteger contra software malicioso (Malware). Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía – spyware- y correo basura).			Política de prevención de software	APO01.04
			Evaluaciones de amenazas potenciales	APO12.02 APO12.03
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.				
2. Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).				
3. Distribuir todo el software de protección de forma centralizada (versión y nivel de parchado) usando una configuración centralizada y la gestión de cambios.				
4. Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).				
5. Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).				

Cuadro 41. DSS05 Gestionar Servicios de Seguridad. Continuación.				
6. Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.				
Prácticas de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	De	Descripción	Descripción	A
DSS05.02 Gestionar la seguridad de la red y las conexiones. Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.	APO01.06	Guías de clasificación de la información	Política de seguridad en la conectividad	APO01.04
	APO09.03	ANSs	Resultados de las pruebas de intrusión	MEA02.08
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones.				
2. Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña.				
3. Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y				
4. Cifrar la información en tránsito de acuerdo con su clasificación.				
5. Aplicar los protocolos de seguridad aprobados a las conexiones de red.				
6. Configurar los equipamientos de red de forma segura.				
7. Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.				
8. Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.				
9. Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS05.04 Gestionar la identidad del usuario y el acceso lógico. Asegurar que todos los				

Cuadro 41. DSS05 Gestionar Servicios de Seguridad. Continuación.				
usuarios tienen derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio.	APO03 .02	Modelo de arquitectura de la información	Resultados de las revisiones de cuentas de usuarios y privilegios de los usuarios Derechos de acceso de usuarios aprobados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menos privilegio, necesidad de tener y necesidad de conocer.				
2. Identificar unívocamente todas las actividades de proceso de la información por los roles funcionales, coordinación con las unidades de negocio y asegurando que todos los roles están definidos consistentemente, incluyendo roles definidos por el propio negocio en las aplicaciones de procesos de negocio.				
3. Autenticar todos los accesos a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación en las aplicaciones usadas en los procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.				
4. Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales				
5. Segregar y gestionar cuentas de usuarios privilegiadas.				
6. Realizar regularmente revisiones de la gestión de todas las cuentas y privilegios relacionados.				
7. Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en los sistemas TI (aplicaciones de negocio, infraestructura TI, operación, desarrollo y mantenimiento de sistemas) son identificables unívocamente. Identificar unívocamente todas las actividades de procesamiento de la información por usuario.				
8. Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible.				

Cuadro 41. DSS05 Gestionar Servicios de Seguridad. Continuación.				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS05.05 Gestionar el acceso físico a los activos de TI. Definir e implementar procedimientos para conceder, limitar y revocar el acceso a los locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, personal temporal, clientes, proveedores, visitantes o cualquier otra tercera parte.			Registros de acceso Peticiónes de acceso aprobadas	DSS0603 Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento. Las peticiones formales de acceso deberán ser completadas y autorizadas por la dirección del emplazamiento de TI, y conservarse las solicitudes registradas. Los formularios deberán identificar específicamente las áreas a las que el individuo tiene acceso concedido.				
2. Asegurar que los perfiles de acceso están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en función del trabajo y responsabilidades.				
3. Registrar y supervisar todos los puntos de entrada a los emplazamientos de TI. Registrar todos los visitantes a las dependencias, incluyendo contratistas y				
4. Instruir a todo el personal para mantener visible la identificación en todo momento. Prevenir la expedición de tarjetas o placas de identidad sin la autorización adecuada.				
5. Escortar a los visitantes en todo momento mientras estén en las dependencias. Si se encuentra a un individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, se deberá alertar al personal de seguridad.				

Cuadro 41. DSS05 Gestionar Servicios de Seguridad. Continuación.				
6. Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores. Asegurar que los dispositivos restringen el acceso y disparen una alarma en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas de acceso, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos.				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS05.06 Gestionar documentos sensibles y dispositivos de salida. Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como	APO03.02	Modelo de arquitectura de la información	Privilegios de acceso Inventario de documentos y dispositivos sensibles.	Interno
Cuadro 41. DSS05 Gestionar Servicios de Seguridad				
formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (tokens) de seguridad.	APO03.02			Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida hacia, dentro y fuera de la empresa.				
2. Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basándose en el principio del menor privilegio, equilibrando riesgo y requerimientos del negocio.				
3. Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones.				
4. Establecer salvaguardas física apropiadas sobre formularios especiales y dispositivos sensibles.				

Cuadro 41. DSS05 Gestionar Servicios de Seguridad. Continuación.				
5. Destruir la información sensible y proteger los dispositivos de salida (por ejemplo, desmagnetizando los soportes magnéticos, destruyendo físicamente los dispositivos de memoria, poniendo trituradoras o papeleras cerradas para destruir formularios especiales y otros documentos confidenciales).				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad. Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.			Tickets de incidentes de seguridad Características de Incidentes de seguridad Registros de incidentes de seguridad	DSS02.02 Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Registrar los eventos relacionados con la seguridad reportada por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo. Retenerla durante un período apropiado para ayudar en futuras investigaciones.				
Cuadro 41. DSS05 Gestionar Servicios de Seguridad				
2. Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta acorde.				
3. Revisar regularmente los registros de eventos para detectar incidentes potenciales.				
4. Mantener un procedimiento para la recopilación de evidencias en línea con las normas de evidencias forenses locales y asegurar que todos los empleados están concienciados de los requerimientos.				
5. Asegurar que los tickets de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.				
7. Realizar regularmente formación de concienciación de seguridad física.				
8. Proveer de protección física a los dispositivos de usuario finales.				
9. Deshacerse de los dispositivos de usuario finales de forma segura.				

Cuadro 42. DSS06 Gestionar Controles de Proceso de Negocio

DSS06 Gestionar Controles de Proceso de Negocio				
<p>Descripción de Proceso COBIT 5 Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Identificar los requisitos de control de la información y gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos.</p>				
<p>Declaración del Propósito del Proceso COBIT 5 Mantener la integridad de la información y la seguridad de los activos de información manejados en los procesos de negocio dentro de la empresa o externalizados.</p>				
DSS06 Objetivos y métricas de procesos específicos de seguridad				
Objetivos de Proceso específicos de seguridad		Métricas Relacionadas		
1. Se han establecido, revisado y actualizado controles apropiados sobre los procesos de seguridad de la información.		Porcentaje de las medidas de la seguridad de la información que se han implementado adecuadamente o siguen siendo válidas.		
2. Se han establecido controles adecuados para proteger la confidencialidad, integridad y disponibilidad de los procesos de negocio.		Número de incidentes relacionados con la seguridad de la información causada porque los controles de seguridad de la información establecidos no eran los adecuados.		
DSS06 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS06.01 Alinear actividades de control embebidas en los procesos de negocio con los objetivos corporativos. Evaluar y supervisar continuamente la ejecución de las actividades de los procesos de negocio y controles relaciona-			Controles de aplicación segura	Interno

Cuadro 42. DSS06 Gestionar Controles de Proceso de Negocio. Continuación				
dos, basados en el riesgo corporativo, para asegurar que el procesamiento de controles está alineado con las necesidades del negocio.			Controles de aplicación segura	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Identificar y priorizar los procesos de seguridad de la información de acuerdo con el riesgo de negocio, cumplimiento, etc.				
2. Identificar los requisitos específicos de seguridad de la información operacionales (por ejemplo, cumplimiento).				
3. Identificar e implementar los controles de aplicación necesarios.				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS06.02 Controlar el procesamiento de la información. Operar la ejecución de las actividades de proceso de negocio y controles relacionados, basados en el riesgo corporativo, para asegurar que el procesamiento de la información es válido, completo, preciso, oportuno y seguro (es decir, refleja el uso de negocio autorizado y legitimado).				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				

Cuadro 42. DSS06 Gestionar Controles de Proceso de Negocio. Continuación

Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
<p>DSS06.03 Gestionar roles, responsabilidades privilegios de acceso y niveles de autorización. Gestionar los roles de negocio, responsabilidades niveles de autoridad y segregación de tareas necesarias para apoyar los objetivos del proceso de negocio. Autorizar el acceso a cualquier activo de información relativo a los procesos de información del negocio, incluyendo aquellos bajo la custodia del negocio, de TI y de terceras partes. Esto asegura que el negocio sabe dónde están los datos y quién los está manejando en su nombre.</p>	APO13.01	Declaración de alcance del	Roles, responsabilidades, privilegios de acceso y niveles de autorización actualizados	Interno
	DSS05.05	Registro de accesos		
	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Funciones y responsabilidades asignadas		
<p>Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)</p> <p>1. Gestionar los roles, responsabilidades, privilegios de acceso y niveles de autoridad para la información.</p> <p>2. Asignar derechos de acceso basados en los principios de la necesidad de conocer, mínimo privilegio y en los requisitos de los puestos.</p> <p>3. Borrar/eliminar los derechos de acceso cuando los usuarios dejan las posiciones/unidades.</p>				

Cuadro 42. DSS06 Gestionar Controles de Proceso de Negocio. Continuación				
4. Implementar la separación de funciones de acuerdo con los procesos de negocio para evitar el fraude y accesos no autorizados.				
5. Hacer seguimiento de las autorizaciones.				
Prácticas de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	De	Descripción	Descripción	A
DSS06.04 Gestionar errores y excepciones. Gestionar las excepciones y errores de los procesos de negocio y facilitar su corrección. Incluir escalada errores y excepciones en los procesos de negocio y la ejecución de acciones correctivas definidas. Esto proporciona garantía de precisión e integridad del proceso de información del negocio.			Privilegios de acceso actualizados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asignar/retirar permisos de acceso en situaciones de emergencia.				
Prácticas de Gestión	Entradas específicas de Seguridad		Salidas específicas de Seguridad	
	De	Descripción	Descripción	A
DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades y de información. Asegurar que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan, Esto permite trazabilidad de la información a lo largo de su ciclo de vida y procesos relacionados				

Cuadro 42. DSS06 Gestionar Controles de Proceso de Negocio. Continuación				
Proporciona garantías de que la información que conduce el negocio es de confianza y ha sido procesada acorde a los objetivos definidos.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	Descripción	Descripción	A
DSS06.06 Asegurar los activos de información. Asegurar los activos de información accesibles por el negocio a través de los métodos aprobados, incluyendo la información en formato electrónico (tales como métodos para crear nuevos activos en cualquier forma, dispositivos portátiles, aplicaciones de usuario y dispositivos de almacenamiento), información en formato físico (tales como documentos fuente o informes de salida) e información en tránsito. Esto beneficia al negocio proporcionando una salvaguarda de la información de comienzo a fin.	Fuera del ámbito de COBIT 5 para seguridad de la Información	Inventario de activos		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1, Hacer cumplir la clasificación de datos, el uso aceptable y las políticas y procedimientos de seguridad para soportar la protección de los activos de información.				
Fuente: Cobit 5 For Information Security				

5.2.2.5 Supervisar, Evaluar y Valorar (MEA)

Cuadro 43. MEA01 Supervisar, evaluar y valorar el rendimiento y la conformidad

MEA01 Supervisar, evaluar y valorar el rendimiento y la conformidad				
Descripción de Proceso COBIT 5 Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.				
Declaración del Propósito del Proceso COBIT 5 Proporcionar transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos.				
MEA01 Objetivos y métricas de procesos específicos de seguridad				
Objetivos de Proceso específicos de seguridad			Métricas Relacionadas	
1. El rendimiento de la seguridad de la información es supervisado de forma continua.			Porcentaje de los procesos de negocio que satisfacen los requerimientos de seguridad de la información definidos.	
2. La seguridad de la información y las prácticas de riesgo de la información se ajustan a los requisitos de cumplimiento interno.			Porcentaje de las prácticas de seguridad de la información que satisfacen los requerimientos de cumplimiento internos.	
MEA01 Prácticas, Entradas/Salidas y Actividades de Procesos Específicos de Seguridad				
Prácticas de Gobierno	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
MEA01.01 Establecer un enfoque de la supervisión. Involucrar a las partes interesadas en el establecimiento y mantenimiento de un enfoque de supervisión que defina los objetivos, alcance y método de medición de las soluciones de negocio, la entrega del servicio y la contribución a los objetivos de negocio. Integrar este enfoque con el sistema de gestión del rendimiento de la compañía.	BAI02.01 Fuera del ámbito de COBIT 5 para seguridad de la Información	Requerimientos de seguridad de la información.	Proceso y procedimiento de supervisión de la seguridad de la información Estándares y regulaciones de seguridad de la información	MEA01.02
Actividades específicas de seguridad (Adicionales a las Entradas COBIT 5)				

Cuadro 43. MEA01 Supervisar, evaluar y valorar el rendimiento y la conformidad. Continuación				
1. Identificar y confirmar las partes interesados en seguridad de la información.				
2. Involucrar a las partes interesadas y comunicar los requisitos de la seguridad de la información y los objetivos de seguimiento y emisión de informes.				
3. Alinear y mantener continuamente el enfoque de supervisión y evaluación de la seguridad de información con los enfoques de TI y de la empresa.				
4. Establecer el proceso y el procedimiento de supervisión de la seguridad de				
5. Acordar un sistema de gestión del ciclo de vida y el proceso de control de cambios para la supervisión y emisión de informes de seguridad de información.				
6. Solicitar, priorizar y asignar recursos para supervisar la seguridad de información.				
Prácticas de Gobierno	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
MEA01.02 Establecer los objetivos de cumplimiento y rendimiento. Colaborar con las partes interesadas en la definición, revisión periódica, actualización y aprobación de los objetivos de rendimiento y cumplimiento enmarcados dentro del sistema de medida del rendimiento.	MEA01.01	Procesos y procedimiento de supervisión de seguridad de la información	Acuerdos sobre métricas y objetivos de seguridad de la información	APO07.04 MEA01.04
Actividades específicas de seguridad (Adicionales a las Entradas COBIT 5)				
1. Definir los objetivos de rendimiento de seguridad de la información de acuerdo con los estándares globales de rendimiento de TI.				
2. Comunicar el rendimiento de seguridad de información y los objetivos de conformidad a las principales partes interesadas con la debida diligencia.				
3. Evaluar si los objetivos y las métricas de seguridad de la información son adecuadas, es decir, específicas, medibles, realizables, pertinentes y de duración determinada.				
Prácticas de Gobierno	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Entradas COBIT 5)	
	De	Descripción	Descripción	A
MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento.	Fuera del ámbito de COBIT 5 para Seguridad	Regulaciones aplicables	Datos de seguimiento procesados	Interno

Cuadro 43. MEA01 Supervisar, evaluar y valorar el rendimiento y la conformidad. Continuación				
MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento.	Fuera del ámbito de COBIT 5 para Seguridad de la información	Regulaciones aplicables	Datos de seguimiento procesados	Interno
Recopilar y procesar datos oportunos y precisos de acuerdo con los enfoques del negocio.				
Actividades específicas de seguridad (Adicionales a las Entradas COBIT 5)				
1. Recopilar y analizar los datos de rendimiento y de conformidad relativos a la seguridad de la información y a la gestión de riesgos de la información (por ejemplo, métricas de seguridad de la información, informes de seguridad de la información).				
2. Valorar la eficiencia, idoneidad e integridad de los datos recogidos.				
Prácticas de Gobierno	Entradas específicas de seguridad		Salidas específicas de seguridad	
	De	Descripción	Descripción	A
MEA01.04 Analizar e informar sobre el rendimiento. Revisar e informar de forma periódica sobre el desempeño respecto de los objetivos, utilizando métodos que proporcionen una visión completa y sucinta del rendimiento de las TI y encaje con el sistema corporativo de supervisión.	MEA01.02	Acuerdo sobre métricas y objetivos de seguridad de la información	Informes de seguridad de la información y planes de acciones correctivas actualizados	APO01.07
Actividades específicas de seguridad (Adicionales a las Entradas COBIT 5)				
1. Diseñar, implementar y acordar una serie de informes de desempeño de seguridad de la información.				
2. Comparar los valores de rendimiento con los objetivos y puntos de referencia internos y, cuando sea posible, con puntos de referencia externos (industria y competidores clave).				

Cuadro 43. MEA01 Supervisar, evaluar y valorar el rendimiento y la conformidad. Continuación				
Prácticas de Gobierno	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas específicas de seguridad (Adicionales a las Entradas COBIT 5)	
	De	Descripción	Descripción	A
MEA01.05 Asegurar la implantación de medidas correctivas. Apoyar a las partes interesadas en la identificación, inicio y seguimiento de las acciones correctivas para solventar anomalías.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Guías de escalado	Proceso de seguimiento de acciones correctivas en materia de seguridad de la información	Interno
Actividades específicas de seguridad (Adicionales a las Entradas COBIT 5)				
1. Desarrollar un proceso de seguimiento para las acciones correctivas en materia de seguridad de la información.				
Fuente: Cobit 5 For Information Security				

Cuadro 44. MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno

MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno
<p>Descripción del Proceso COBIT 5</p> <p>Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.</p>
<p>Declaración del Propósito del Proceso COBIT 5</p> <p>Ofrecer transparencia a las partes interesadas claves respecto de la adecuación del sistema de control interno para generar confianza en las operaciones, en el logro de los objetivos de la compañía y un entendimiento adecuado del riesgo residual.</p>
<p>MEA02 Objetivos y Métricas de Seguridad Específicos del Proceso</p>

Cuadro 44. MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno. Continuación				
Objetivos de Seguridad Específicos del Proceso		Métricas Relacionadas		
1. Los controles de seguridad de la información están desplegados y operan eficazmente.		Porcentaje de los procesos que satisfacen los requerimientos de controlde seguridad de la información Porcentaje de controles en los que se cumplen los requisitos de controlde seguridad de la información		
2. Hay establecidos procesos de monitorización para los controles de seguridad y se informa de sus resultados.		Porcentaje de controles de seguridad de la información adecuadamente monitorizados con resultados informados y revisados		
MEA02 Prácticas de Seguridad Específicos del Proceso, Entradas/Salidas y Actividades				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas Específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA02.01 Supervisar el control interno. Realizar, de forma continua, la supervisión, los estudios comparativos y la mejora el entorno de control de TI y el marco de control para alcanzar los objetivos organizativos.	APO13.03	Informe de auditoría ISMS	Alcance para el aseguramiento de seguridad de la información y estrategia de evaluación de controles internos definidos	MEA02.03
	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Auditorías externas independientes		
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Realizar una revisión periódica de las políticas y procedimientos de seguridad de la información.				
2. Determinar el alcance del aseguramiento p.ej. controles de seguridad de la información a evaluar.				
3. Establecer un enfoque formal para el aseguramiento de seguridad de la información.				

Cuadro 44. MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno. Continuación				
Práctica de Gestión	Entradas Específicas de Seguridad		Salidas Específicas de Seguridad	
	De	Descripción	Descripción	A
MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio.				
Revisar la operación de controles, incluyendo la revisión de las evidencias de supervisión y pruebas, para asegurar que los controles incorporados en los procesos de negocio operan de manera efectiva. Incluir actividades de mantenimiento de evidencias de la operación efectiva de controles a través de mecanismos como la comprobación periódica de controles, supervisión continua de controles, evaluaciones independientes, centros de mando y control y centros de operación de red. Esto proporciona al negocio de la seguridad de la efectividad del control para satisfacer los requisitos relativos al negocio y a las responsabilidades sociales y regulatorias.			Evidencia de la efectividad de los controles de seguridad de la información	Interno
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Medir la eficacia de los controles de seguridad de la información.				

Cuadro 44. MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno. Continuación				
Práctica de Gestión	Entradas específicas de seguridad		Salidas Específicas de Seguridad	
	De	Descripción	Descripción	A
MEA02.03 Realizar autoevaluación de control. Estimular a la Dirección y a los propietarios de los procesos a tomar posesión de manera firme del procedimiento de mejora del control, a través de programas continuos de autoevaluación que valoren la completitud y efectividad del control de la Dirección sobre los procesos, políticas y contratos.	MEA02.01	Alcance para el aseguramiento de seguridad de la información y estrategia de de evaluación de controles internos definidos estrategia de evaluación de controles internos definidos	Evaluaciones de aseguramiento de seguridad de la información	MEA02.04
	MEA02.01			
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Realizar evaluaciones del aseguramiento de seguridad de la información (independientes y auto-evaluaciones) para identificar debilidades de los controles.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas Específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA02.04 Identificar y comunicar las deficiencias de control Identificar deficiencias de control y analizar e identificar las causas raíces subyacentes.	MEA02.03	Evaluaciones de aseguramiento de seguridad de la información	Resultados de la evaluación y acciones de remedio	MEA02.08

Cuadro 44. MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno. Continuación				
Escalar las deficiencias de control y comunicar las a las partes interesadas.	MEA02.03	Evaluaciones de aseguramiento de seguridad de la información	Resultados de la evaluación y acciones de remedio	MEA02.08
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Revisar los informes de incidentes de seguridad de la información para identificar deficiencias de los controles. Informar y abordar las deficiencias detectadas.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas Específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA02.05 Garantizar que los proveedores de aseguramientos sean independientes y cualificados. Asegurar que las entidades que realizan el aseguramiento sean independientes de la función, grupo u organización en el alcance. Las entidades que realizan el aseguramiento deberían demostrar una actitud y apariencia apropiadas y adecuada competencia en las habilidades y conocimientos que son necesarios para realizar el aseguramiento y la adherencia a los códigos de ética y los estándares profesionales.			Competencias en habilidades y conocimiento	Interno
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Establecer competencias y cualificaciones para el proveedor de aseguramiento.				

Cuadro 44. MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno. Continuación				
Práctica de Gestión	Entradas específicas de seguridad		Salidas Especificas de Seguridad	
	De	Descripción	Descripción	A
MEA02.06 Planificar iniciativas de aseguramiento. Planificar las iniciativas de aseguramiento basándose en los objetivos empresariales y las prioridades estratégicas, riesgo inherente, restricciones de recursos y suficiente conocimiento de la compañía.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Plan de compromiso	Plan de compromiso actualizado	Interno
Actividades Especificas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Aceptar los objetivos de la revisión de aseguramiento de seguridad de la información.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas Especificas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA02.07 Estudiar las iniciativas de aseguramiento. Definir y acordar con la dirección el ámbito de la iniciativa de aseguramiento, basándose en los objetivos de aseguramiento.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Plan de compromiso	Plan de compromiso actualizado	Interno
Actividades Especificas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Documentar los detalles del compromiso de la organización en completar la revisión.				
2. Realizar revisiones regulares de aplicaciones, sistemas y redes.				

Cuadro 44. MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno. Continuación				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas Específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA02.08 Ejecutar las iniciativas de aseguramiento. Ejecutar la iniciativa de aseguramiento planificada. Informar de los hallazgos identificados. Proveen opiniones de aseguramiento positivo, cuando sea oportuno, y recomendaciones de mejora relativas a los riesgos residuales identificados en el desempeño operacional, el cumplimiento externo y el sistema de control interno.	DSS05.02	Resultados de pruebas de intrusión	Informes y recomendaciones de auditorías externas de seguridad de la información	Interno
	MEA02.04	Resultados de la evaluación y acciones de remedio		
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Producir y emitir informes firmados sobre el aseguramiento de seguridad de la información.				
Fuente: Cobit 5 For Information Security				

Cuadro 45. MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos

MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos				
Dominio: Supervisar, Evaluar y Valorar				
Descripción del Proceso COBIT 5 Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general.				
Declaración del Propósito del Proceso COBIT 5 Asegurar que la empresa cumple con todos los requisitos externos que le sean aplicables.				
MEA03 Objetivos y Métricas de Seguridad Específicos del Proceso				
Objetivos de Seguridad Específicos del Proceso		Métricas Relacionadas		
1. Las prácticas de riesgos y seguridad de la información conformes con los requerimientos de cumplimiento de externos.		Porcentaje de prácticas de seguridad de la información que satisfacen los requerimientos externos de conformidad		
2. Se realiza una supervisión de los requisitos externos nuevos o revisados que impactan en la seguridad de la información.		Número o porcentaje de proyectos iniciados por seguridad de la información para implementar nuevos requerimientos externos		
MEA03 Prácticas de Seguridad Específicos del Proceso, Entradas/Salidas y Actividades				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas Específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA03.01 Identificar requisitos externos de cumplimiento. Identificar y supervisar, de manera continuada, cambios en las legislaciones y regulaciones tanto locales como internacionales, así como otros requisitos exter	BAI02.01	Requerimientos de seguridad de la información	Requerimientos externos de cumplimiento de seguridad de la información	BAI02.01

Cuadro 45. MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos				
nos de obligado cumplimiento en el área de TI.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Estándares y regulaciones de seguridad de la información	Requerimientos externos de cumplimiento de seguridad de la información	
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Establecer acuerdos para supervisar la conformidad de seguridad de la información con requerimientos externos.				
2. Identificar objetivos de cumplimiento de seguridad de la información con requerimientos externos.				
3. Determinar los requerimientos externos de cumplimiento que deben satisfacerse (incluyendo legales, regulatorios, de privacidad y contractuales).				
4. Identificar y comunicar las fuentes de materiales relativos a seguridad de la información que ayuden a cumplir los requerimientos de cumplimiento externos.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas Específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA03.02 Optimizar la respuesta a requisitos externos. Revisar y ajustar políticas, principios, estándares, procedimientos y metodologías para asegurar la adecuada gestión y comunicación de los requisitos legales, regulatorios y contractuales. Considerar qué estándares sectoriales, códigos de buenas prácticas y guías de mejores prácticas pueden adoptarse y adaptarse.	Fuera del ámbito de COBIT 5 para Seguridad de la Información	Regulaciones aplicables	Requerimientos externos actualizados	Interno
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				

Cuadro 45. MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos. Continuación				
1. Revisar y comunicar los requerimientos externos a todos los grupos de interés relevantes.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas Específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA03.03 Confirmar el cumplimiento de requisitos externos. Confirmar el cumplimiento de las políticas, los principios, los estándares, los procedimientos y las metodologías con los requisitos legales, regulatorios y contractuales.			Informe de conformidad de seguridad de la información	Interno
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Recopilar y analizar los datos de conformidad relacionados con la gestión de la seguridad y de los riesgos de la información.				
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas Específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA03.04 Obtener garantía del cumplimiento de requisitos externos. Obtener y notificar garantías de cumplimiento y adherencia a políticas, principios, estándares, procedimientos y metodologías. Confirmar que las acciones correctivas para tratar las diferencias en el cumplimiento son cerradas a tiempo.			Informes de aseguramiento de la conformidad	Interno

Cuadro 45. MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos. Continuación
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)
1. Obtener evidencias de las terceras partes.
Fuente: Cobit 5 For Information Security

5.2.3 Estructuras organizativas

5.2.3.1 Gerencia de Seguridad de la Información

Cuadro 46. Gerencia de la Seguridad de la Información

Gerencia de Seguridad de la Información	
Área	Característica
Mandato	La responsabilidad completa del programa de seguridad de la información de la empresa
Principios operativos	<p>Dependiendo de los factores variables en una empresa, el encargado de la Seguridad de la información puede reportar otro ejecutivo sénior o área que requiera información..</p> <p>Es el enlace entre la dirección ejecutiva y el programa de seguridad de la información. Debe también comunicar y de manera muy cercana con los grupos de interés clave del negocio para cubrir las necesidades de protección de la información.</p> <p>Debe:</p> <ul style="list-style-type: none"> Tener un entendimiento exacto de la visión estratégica del negocio Ser un comunicador efectivo Ser hábil en construir relaciones efectivas con los líderes del negocio Ser capaz de traducir los objetivos del negocio en requerimientos de seguridad de la información
Ámbito de control	<p>Es responsable de:</p> <ul style="list-style-type: none"> Establecer y mantener un sistema de gestión de seguridad de la información (SGSI) Definir y gestionar un plan de tratamiento del riesgo de la información Supervisar y revisar el SGSI
Nivel de autoridad/derechos de decisión	<p>Es responsable de implementar y mantener la estrategia de seguridad de la información.</p> <p>La responsabilidad de que se haga (y la aprobación de las decisiones importantes) reside en la función a la que él reporta, por ejemplo, un miembro de la directiva ejecutiva sénior o el ISSC.</p>
Derechos de delegación	Debe delegar las tareas a los gerentes de seguridad de la información y a personal de negocio.
Escalado	Debe escalar problemas clave relacionados con el riesgo de información a su supervisor directo y/o al ISSC.

Matriz RACI a alto nivel

Cuadro 47. Matriz RACI a Alto Nivel con Prácticas Clave

Matriz RACI a Alto Nivel con Prácticas Clave	
Práctica de Proceso	Nivel de Implicación
Identificar y comunicar amenazas para la seguridad de la información, comportamientos deseables y cambios necesarios para tratar estos puntos.	Responsable de que se haga
Asegurar que la gestión del entorno y de las instalaciones se adhiera a los requerimientos en seguridad de la información.	Responsable de que se haga
Protección contra malware.	Responsable de que se haga
Gestionar la seguridad de las redes y la conectividad.	Responsable de que se haga
Gestionar la seguridad del perímetro.	Responsable de que se haga
Gestionar la identidad de los usuarios y el acceso lógico.	Responsable de que se haga
Gestionar el acceso físico a los activos de TI.	Responsable de que se haga
Supervisar la infraestructura para identificar eventos relacionados con la seguridad.	Responsable de que se haga
Proporcionar formas de mejorar la eficiencia y la eficacia de la función de seguridad de la información (por ejemplo, mediante formación del personal de seguridad de la información; documentación de procesos, tecnología y aplicaciones; y la estandarización y automatización del proceso).	Responsable de que se haga
Supervisar la gestión del riesgo en TI.	Responsable de hacerla
Definir y comunicar la estrategia en seguridad de la información que está alineada con la estrategia del negocio.	Responsable de hacerla
Investigar, definir y documentar los requerimientos en seguridad de la información.	Responsable de hacerla
Validar los requerimientos en seguridad de la información con las partes interesadas, patrocinadores del negocio y personal de despliegue técnico.	Responsable de hacerla
Desarrollar políticas y procedimientos de seguridad de la	Responsable de
Definir e implementar estrategias de evaluación del riesgo y de respuesta y cooperar con la oficina del riesgo para gestionar el riesgo de la información.	Responsable de hacerla
Asegurar que se evalúa el impacto potencial de los cambios.	Responsable de hacerla
Recoger y analizar datos del rendimiento y de cumplimiento relativos a seguridad de la información y gestión del riesgo de la información.	Responsable de hacerla

Entradas/Salidas. Una estructura requiere entradas (normalmente información) antes de que se puedan tomar decisiones informadas, y produce salidas tales como decisiones, otra información o peticiones de información adicional.

Cuadro 48. Entradas y Salidas COBIT

Entradas y Salidas			
Entrada	De	Salida	A
Tolerancia al riesgo	Comité de Riesgo	Estrategia de seguridad de la	Empresa
Mandato regulatorio/de cumplimiento	Externo	Políticas, estándares, procedimientos	Empresa
Estrategia de negocio y de TI	Organización/TI	Plan de remediación a las recomendaciones de	Auditoría
Informes de auditoría	Auditoría		
Fuente; autores			

5.2.3.2. Comité de Dirección de Seguridad de la Información

- Composición

Cuadro 49. Comité de Dirección de Seguridad de la Información

ISSC	
Rol	Descripción
Gerente de Seguridad de la Información	<p>Presidir el ISSC y ser el enlace con el Comité de ERM</p> <p>Responsable de toda la seguridad de la información de la empresa</p> <p>Comunicación de las prácticas de diseño, implementación y monitorización</p> <p>Cuando sea aplicable, el ISSC discute las soluciones de diseño por adelantado con los arquitectos de seguridad de la información para mitigar los riesgos de la información identificados</p>

Cuadro 49. Comité de Dirección de Seguridad de la Información. Continuación.	
Custodios de la información/propietarios del negocio	A cargo de ciertos procesos o aplicaciones de negocio Responsables de comunicar tanto iniciativas de negocio que puedan impactar en la seguridad de la información o como el impacto que las prácticas de seguridad de la información puedan causar a los usuarios Pueden tener una comprensión del riesgo de negocio/operativo, costes y beneficios, así como de determinados requerimientos de seguridad de la información para su área de negocio
Gerente de TI	Informar del estado de las iniciativas de seguridad de la información relacionadas con TI
Representantes de las funciones especializadas	Aportar la opinión de los especialistas al comité cuando sea relevante, por ejemplo, de representantes de auditoría interna, RRHH, legal, riesgo, oficial de gestión de proyectos (PMO). A estas funciones se les puede pedir que se unan al ISSC en ocasiones o como miembros permanentes. Puede merecer la pena tener representantes de auditoría interna como miembros permanentes para dar consejo al comité sobre el riesgo de cumplimiento.
Fuente: Cobit 5 For Information Security	

- Mandato, Principios Operativos, Ámbito de Control y Nivel de Autoridad

Cuadro 50. Mandato, Principios Operativos, Ámbito de Control y Nivel de Autoridad

Mandato, Principios Operativos, Ámbito de Control y Nivel de Autoridad	
Área	Característica
Mandato	Asegurar que las buenas prácticas, que la seguridad de la información se aplican de forma eficaz y consistentemente en toda la empresa.

Principios operativos	<p>El ISSC se reúne de manera regular, cuando sea necesario para la empresa. Se pueden planificar reuniones másfrecuentes durante iniciativas específicas o cuando haya problemas que necesiten ser gestionados urgentemente.</p> <p>Se permiten sustitutos o representantes, pero deben limitarse. Se debe limitar la pertenencia al comité a un número pequeño de líderes estratégicos y tácticos para asegurar la comunicación bidireccional y la toma de decisiones adecuadas. Otros líderes de negocio pueden ser invitados según la necesidad.</p> <p>Todas las actas de las reuniones deben ser aprobadas y retenidas por un determinado periodo de tiempo.</p> <p>El Gerente De Seguridad De La Información preside las reuniones del ISSC.</p>
Ámbito de control	El ISSC es responsable en la toma de decisiones de seguridad de la información para toda la empresa.
Nivel de autoridad/derechos de decisión	El ISSC es responsable de las decisiones de seguridad de la información de la empresa en apoyo a las decisiones estratégicas del comité de ERM.
Derechos de delegación	El ISSC es el último responsable de la estrategia de diseño e implementación del programa de seguridad de la información y esta responsabilidad no se puede delegar a otros roles miembros.
Escalado	<p>Todos los problemas deben ser escalados al miembro responsable de seguridad de la información pertinente de la dirección ejecutiva.</p> <p>Las estrategias del riesgo de la información de la empresa deben ser escaladas para su aprobación al comité de ERM.</p>
Fuente: Cobit 5 For Information Security	

Matriz RACI a Alto Nivel

Cuadro 51. ISSC: Matriz RACI a Alto Nivel

Práctica de Proceso	Nivel de Implicación (RACI)
Definir y comunicar la estrategia de seguridad de la información que está alineada con la estrategia del negocio.	Responsable de que se haga
Investigar, definir y documentar los requerimientos en seguridad de la información.	Responsable de que se haga
Validar los requerimientos en seguridad de la información con las partes interesadas, patrocinadores del negocio y personal de despliegue técnico.	Responsable de que se haga
Desarrollar políticas y procedimientos de seguridad de la información.	Responsable de que se haga
Desarrollar un plan de seguridad de la información que identifique el entorno de seguridad de la información y las actividades a ser implementadas por el equipo de proyecto para proteger los activos de la organización.	Responsable de que se haga
Asegurar que se evalúa el impacto potencial de los cambios.	Responsable de que se haga
Recoger y analizar datos del rendimiento y de cumplimiento relativos a seguridad de la información y gestión del riesgo de la información.	Responsable de que se haga
Establecer, acordar y comunicar el rol del GERENTE DE SEGURIDAD DE LA INFORMACIÓN y el ISM.	Responsable de hacerla
Aumentar el perfil de la función de seguridad de la información dentro de la empresa y potencialmente fuera de ella.	Responsable de hacerla
Contribuir al esfuerzo en la gestión de la continuidad de negocio de toda la empresa.	Responsable de hacerla
Fuente: Cobit 5 For Information Security	

Entradas/Salidas

Cuadro 52. ISSC: Entradas y Salidas

Entradas y Salidas			
Entrada	De	Salida	A
Estrategia de negocio	Consejo de Administración	Programa y estrategia de seguridad de la información	Comité de ERM, ISMs, custodios de la Información/dueños del negocio
Niveles de aceptación del riesgo	Comité de ERM	Perfil del riesgo de la información	Comité de ERM
Estrategia de TI	TI		
Listado de proyectos de la empresa	Custodios de la información/ propietarios del negocio, PMO		
Informes de auditoría interna	Auditoría interna		
Fuente: Cobit 5 For Information Security			

5.2.3.3 Comité de Gestión de Riesgo Empresarial. El comité de ERM es responsable de todas la toma de decisiones de la empresa relativas a la evaluación, control, optimización, financiación y monitorización de todas las fuentes de riesgo, con el propósito de incrementar el valor de la empresa a a corto y largo plazo para todas sus partes interesadas.

- Composición

Cuadro 53. Comité de Gestión de Riesgo Empresarial (ERM)

Comité de ERM	
Rol	Descripción
Gerente de seguridad de la Información	En un escenario óptimo, el Gerente de seguridad de la Información es miembro del comité de ERM, para proporcionar al comité asesoramiento sobre riesgos específicos de la información.
Gerencias.	Representante de la alta dirección ejecutiva.
Propietarios de los procesos clave para el negocio	A cargo de ciertos procesos o aplicaciones de negocio Responsables de comunicar tanto iniciativas de negocio que puedan impactar en la seguridad de la información como el impacto que las prácticas de seguridad de la información puedan causar a los usuarios Pueden tener una comprensión del riesgo de negocio/operativo, costes y beneficios, así como de determinados requerimientos de seguridad de la información para su área de negocio
Auditoría/cumplimiento	Proporciona información especializada cuando sea relevante. Se les puede pedir su incorporación al comité de ERM de manera ocasional o como miembro permanente. Por ejemplo, puede merecer la pena tener representantes de la auditoría interna como miembros permanentes con objeto de asesorar al comité en materia de riesgo de cumplimiento.
Representante legal	Proporciona asesoramiento legal. Se le puede pedir su incorporación al comité de ERM de manera ocasional o como miembro permanente.
Fuente: Cobit 5 For Information Security	

Matriz RACI de Alto Nivel

Cuadro 54. Comité de ERM: Matriz RACI de Alto Nivel

Comité de ERM: Matriz RACI de Alto Nivel	
Práctica del Proceso	Nivel de
Asesorar sobre la estrategia de seguridad de la información definida por el ISSC.	Responsable de hacerla
Establecer los niveles de tolerancia al riesgo de la empresa.	Responsable de que se haga
Definir e implementar las estrategias de evaluación y de respuesta al riesgo.	Responsable de que se haga
Revisar las evaluaciones de riesgos de la información y los perfiles de riesgos.	Responsable de que se haga
Fuente: Cobit 5 For Information Security	

5.2.3.4. Custodios de la Información/ Propietarios de Negocio

Composición

Los custodios de la información o los propietarios de negocio actúan como enlaces entre las funciones de negocio y de seguridad de la información. Pueden ser asociados con tipos de información, aplicaciones específicas, o unidades de negocio dentro de una empresa. La persona que desempeñe este rol debe poseer un buen conocimiento tanto del negocio como de los tipos de información que son procesados y que requieren protección. Actúan como asesores de confianza y agentes de supervisión en cuestiones relativas a la información dentro del negocio.

Este rol debería equilibrar el riesgo de negocio y el de información de modo que las decisiones del negocio o prevalezcan siempre sobre las decisiones de la seguridad de la información.

Matriz RACI de Alto Nivel

Cuadro 55. Custodios de la Información/Propietarios de Negocio: Matriz RACI de Alto Nivel

Custodios de la Información/Propietarios de Negocio: Matriz RACI de Alto Nivel	
Práctica del Proceso	Nivel de
Comunicar, coordinar y asesorar a los gestores de negocio sobre los esfuerzos en gestión de riesgos de la información.	Responsable de hacerla
Informar al ISSC sobre cambios en los procesos de negocio y/o en las estrategias (por ejemplo, nuevos productos o servicios).	Responsable de hacerla
Elevar el perfil de la función de seguridad de la información y de las políticas y procedimientos de seguridad de la información dentro de la empresa.	Responsable de hacerla
Fuente: Cobit 5 For Information Security	

6. RESULTADOS

De acuerdo a lo planteado en este documento y a lo evaluado en SONDA Coombia, se obtiene un modelo de seguridad, fundamentado en dos buenas practicas de gestión y gobernabilidad; donde es posible medir y controlar los aspectos mas relevantes de seguridad para la compañía.

7. APORTES

Se obtuvo un modelo de seguridad el cual podría servir como estandar para los demás Datacenter de Sonda, al igual que para Datacenters que posean características generales.

8. CONCLUSIONES

La implantación de un Sistema de Gestión de la Seguridad de la Información proporciona a SONDA Colombia los siguientes beneficios:

- Un análisis de riesgos de sus Sistemas de Información.
- Una gestión adecuada de los riesgos según su modelo de empresa.
- Una mejora continua de su gestión de la seguridad.
- El cumplimiento de la legislación vigente sobre protección de datos de carácter personal, comercio electrónico, propiedad intelectual, etc.
- Facilita el logro de los objetivos de la organización.
- Hace a la organización más segura y consciente de sus riesgos.
- Mejoramiento continuo del Sistema de Control Interno.
- Optimiza la asignación de recursos.
- Aprovechamiento de oportunidades de negocio.
- Fortalece la cultura de autocontrol.
- Mayor estabilidad ante cambios del entorno.
- Conocer y Analizar sus riesgos, identificando amenazas, vulnerabilidades e impactos en su empresa.
- Reducir eficazmente el nivel de riesgo mediante los controles adecuados
- Organizar los recursos de la seguridad.
- Integra la Gestión de la Seguridad SI.
- Aporta confianza a los sistemas de información

Y en definitiva, establece una cultura de la seguridad y una excelencia en el tratamiento de la información en todos sus procesos de negocio. Así, aporta un valor añadido de reconocido prestigio, en la calidad de los servicios que ofrece a sus clientes

9. RECOMENDACIONES

El presente modelo podría ser adoptado por aquellas organizaciones que busquen una integración entre la norma ISO 27001 y Cobit 5 For information Security, por ello, sería aconsejable continuar con futuras investigaciones que permitan la elaboración de un modelo general el cual pueda ser fácilmente aplicado a las mismas.

10. IMPLICACIONES

Para SONDA, la elaboración del presente modelo representa un paso muy importante en la definición del modelo de seguridad a implementar en el Datacenter, teniendo en cuenta que hace poco obtuvo su certificación ISO20000 y que se encuentra próximo a iniciar el proceso de certificación en ISO27001.

BIBLIOGRAFÍA

AENOR. Comprehensive Performance Assessment for local government. [en línea], [consultado el 2 de agosto de 2014]. Disponible en: [http://www.en.aenor.es/aenor/normas/fichanorma.asp?tipo=N&codigo=N0044393 &PDF=Si](http://www.en.aenor.es/aenor/normas/fichanorma.asp?tipo=N&codigo=N0044393&PDF=Si)

BSIGROUP. ISO 27001: Código de conducta para los controles de gestión de seguridad de la información. [en línea], [consultado el 2 de agosto de 2014]. Disponible en: <http://www.bsigroup.com/en-GB/iso-27001-information-security/ISOIEC-27001-Revision/>

_____. Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013. 2013. [en línea], [consultado el 2 de agosto de 2014]. Disponible en: <http://www.bsigroup.com/Documents/iso-27001/resources/BSI-ISO27001-mapping-guide-UK-EN.pdf>

COBIT USER GROUP. Historia del Cobit. [en línea], [consultado el 2 de agosto de 2014]. Disponible en: <http://www.pc-history.org/cob.htm>

ESPAÑA. Comisaria General de Policía Judicial U.D.E.F.; Central Brigada De Investigación Tecnológica. Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. [en línea], [consultado el 2 de agosto de 2014]. Disponible en: http://www.fsc.ccoo.es/comunes/recursos/99922/doc28596_Seguridad_informatica.pdf

ESTÁNDAR. ISO/IEC. INTERNACIONAL. 17799. Tecnología de información Beta. [en línea], [consultado el 2 de agosto de 2014]. Disponible en: <http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf>

FEDERACIÓN DE SERVICIOS A LA CIUDADANÍA. Seguridad informática. ? [en línea], [consultado el 2 de agosto de 2014]. Disponible en: http://www.fsc.ccoo.es/comunes/recursos/99922/doc28596_Seguridad_informatica.pdf

IS&BCA, Information Security & Business Continuity Academy. Checklist of Mandatory Documentation Required by ISO/IEC 27001 (2013 Revision). 2013. [en línea], [consultado el 2 de agosto de 2014]. Disponible en: http://www.iso27001standard.com/downloads/Checklist_of_Mandatory_Documentation_Required_by_ISO_27001_2013.pdf

ISACA. COBIT 5 Enabling Processes. 2012. [en línea], [consultado el 2 de agosto de 2014]. Disponible en: www.isaca.org/COBIT/Documents/COBIT5-Ver2-enabling.pdf

_____. _____. Enabling Implementation. 2012. [en línea], [consultado el 2 de agosto de 2014]. Disponible en: <<http://www.isaca.org/COBIT/Documents/COBIT5-Ver2-Implementation.pdf>>

_____. _____. for Information Security. 2012. [en línea], [consultado el 2 de agosto de 2014]. Disponible en: <http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf>

ITERA, IT & Business process. ¿Qué es COBIT? [en línea], [consultado el 2 de agosto de 2014]. Disponible en: <http://www.itera.com.mx/it institute/ mails/ chile/cobit.htm>

QUICK LINK. ISO 27001: Information technology — Security techniques — Code of practice for information security controls. [en línea], [consultado el 2 de agosto de 2014]. Disponible en: <http://www.iso27001security.com/html/27002.html>

STANDARD.COM. Iso 2700. Informe de ISO 27001: Lista de documentación obligatoria requerida por ISO 27001 (Revisión 2013) (PDF). [en línea], [consultado el 2 de agosto de 2014]. Disponible en: http://www.iso27001standard.com/downloads/ Checklist_of_ Mandatory_ Documentation _ Required_by_ISO_ 27001_2013.pdf

UNIVERSIDAD AUTÓNOMA DE MÉXICO: The History Of ISO 17799 And ISO 27001. [en línea], [consultado el 2 de agosto de 2014]. Disponible en <http://www.pc-history.org/17799.htm>

DESARROLLO DEL MODELO DE INTEGRACIÓN DE LAS NORMAS ISO/IEC 27001:2013, ISO/IEC 27002:2013 Y COBIT V5 FOR INFORMATION SECURITY PARA LA DEFINICIÓN, DISEÑO Y MODELAMIENTO DE LAS POLÍTICAS DE SEGURIDAD APLICADO AL DATACENTER DE SONDA COLOMBIA.

Alba, Mario, Beltran, John y Esguerra, Mauricio.
{mario-alba, John-beltran, mauricio-esguerra}@upc.edu.co
Universidad Piloto de Colombia

Abstract— The following document presents the approach to define an optimal security model for the datacenter owned by the company Sonda Colombia, which integrates the best practices of management in ISO/IEC 27001:2013 and ISO/IEC 27002:2013, and governance offered by COBIT 5 FOR INFORMATION SECURITY.

This company aims to provide IT services to various types of clients, who are worried about the security of the information in its infrastructure, requiring models to ensure the safety of it.

ISO / IEC 27001:2013 and ISO / IEC 27002:2013 guarantee all types of controls that should be implemented to ensure that the risks could be managed, controlled and mitigated.

COBIT 5 FOR INFORMATION SECURITY with its wide range of governance processes ensure all aspects of the security model, helping to continuously improve them and defining all monitoring protocols.

Resumen— El siguiente documento es una presentación del planteamiento para definir un modelo de seguridad óptimo para el Datacenter de Sonda Colombia, el cual integrara las buenas prácticas de gestión de seguridad de la información establecidas en ISO/IEC 27001:2013 y ISO/IEC 27002:2013, y las de gobernabilidad ofrecidas por COBIT 5 FOR INFORMATION SECURITY.

Sonda de Colombia tiene como objetivo ofrecer servicios de TI a varios tipos de clientes, los cuales preocupados por la seguridad de la información consignada en su infraestructura exigen modelos para garantizar la seguridad de esta.

ISO/IEC 27001:2013 y ISO/IEC 27002:2013 regirán los tipos de controles que se deben implementar para garantizar que los riesgos existentes puedan ser manejados, controlados y mitigados apropiadamente.

COBIT 5 FOR INFORMATION SECURITY con su amplia gama de procesos garantizara la gobernabilidad de todos los aspectos del modelo de seguridad

Índice de Términos— Framework de Seguridad de la Información, COBIT 5 For Information Security, ISO 27001 e ISO 27002, Catalizadores.

I. INTRODUCCIÓN

La elaboración de modelos de Seguridad que integran varios estándares se ha convertido en una práctica cada vez más común en las empresas Colombianas.

La iniciativa del proyecto surge de la necesidad que tiene Sonda Colombia en ser una compañía competitiva en el mercado y de mejorar su imagen ante sus clientes, así como de generar un modelo de

Seguridad que permita obtener los beneficios de incluir tres normas en un mismo modelo de seguridad y brinde un diseño acoplado a las necesidades de la empresa.

La nueva versión de la ISO 27001 está basada en la experiencia obtenida con el uso del estándar ISO 27001:2005, además facilita la integración con otras normas ISO gracias a sus nuevas directivas y se encuentra alineada con la norma ISO 31000 para gestión de riesgos. Por otro lado, se elimina la sección referente al proceso de PHVA y se permite a la organización elegir otro modelo de mejora continua. Dado que la norma está basada en la experiencia obtenida de la norma anterior, es posible mapear el contenido de la norma del 2013 en la norma del 2005.¹ A su vez, COBIT 5 For Information Security es un framework para gestión de la seguridad de la información. SONDA como empresa proveedora de servicios de TI, pretende a mediano plazo la expansión de los servicios prestados a sus actuales y futuros clientes con el montaje de un Datacenter que ofrezca servicios Cloud. Adicionalmente pretende garantizar la seguridad de la información que será consignada en dichos servicios; en contraste, la empresa debe estar en capacidad de responder de manera correcta ante cualquier requerimiento de seguridad.

COBIT es un marco de trabajo aceptado mundialmente para el adecuado control de proyectos de tecnología, los flujos de información y los riesgos que éstas implican. COBIT se utiliza para planear, implementar, controlar y evaluar el gobierno sobre TIC incorporando objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez. Además contribuye a reducir las brechas existentes entre los objetivos de negocio, y los beneficios, riesgos, necesidades de control y aspectos técnicos propios de un proyecto TIC; proporcionando un Marco Referencial Lógico para su dirección efectiva.

¹<http://www.bsigroup.com/en-GB/iso-27001-information-security/ISOIEC-27001-Revision/>

II. DISEÑO PROPUESTO

A. CATALIZADORES

Las políticas, los principios y los marcos de referencia son los medios que usara SONDA para definir el camino a seguir, el comportamiento deseado de cada una de los actores involucrados y que traducidos en guías formales, serán los mecanismos para llegar a establecer los comportamientos deseados.



PRINCIPIOS DE COBIT

Aprovechando la facilidad de aplicación de los principios de Cobit a cualquier modelo de negocio, estos serán tomados por SONDA como base para su operación.

Dar Soporte al negocio: El modelo debe enfocarse al negocio teniendo en cuenta las partes interesadas, requisitos legales, requisitos del negocio y gestión del riesgo, amenazas actuales y futuras y la mejora continua de la seguridad de la información.

Defender el Negocio: Adoptar una estrategia basada en el riesgo, proteger la confidencialidad de la información clasificada, centrarse en aplicaciones críticas para el negocio y desarrollo seguro de sistemas.

Promover un comportamiento responsable en la seguridad de la información: Actuar de manera profesional y ética y fomentar una cultura positiva de la seguridad de la información que permita hacer

un seguimiento oportuno a los incidentes presentados.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La alta dirección de SONDA, teniendo en cuenta que la información es un factor de alta importancia y criticidad en el desarrollo de los negocios actuales y un activo fundamental para el normal desarrollo de las actividades comerciales y operativas de la compañía, establece políticas, normas, planes de mejoramiento continuo y actividades de capacitación y sensibilización como parte integral de la gobernabilidad corporativa, ofreciendo a los usuarios, clientes, proveedores y demás entidades y personas relacionadas con la empresa niveles apropiados de integridad, disponibilidad y confidencialidad de la información de propiedad y/o administrada por SONDA, dando cumplimiento a los requisitos legales.

Basados en que SONDA ya ha implementado la norma ISO20000 y que algunos de sus procesos son compatibles con ISO27001, las siguientes políticas ya están siendo aplicadas:

- GESTIÓN DE INCIDENTES DE SEGURIDAD
- RECURSOS HUMANOS
- GESTIÓN DE ACTIVOS
- RELACIÓN CON LOS PROVEEDORES
- CONTINUIDAD DEL NEGOCIO

El planteamiento de las Políticas de Seguridad de la Información de la compañía toma como referencia los dominios de las normas ISO27001: 2013 e ISO27001:2013. De acuerdo a la clasificación de Cobit 5 For Information Security, las políticas fueron planteadas bajo el esquema mostrado a continuación, estableciendo para cada una de ellas una descripción, unos objetivos y un alcance.

Políticas específicas de la seguridad de la información dirigidas por función de la seguridad de la información

- POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

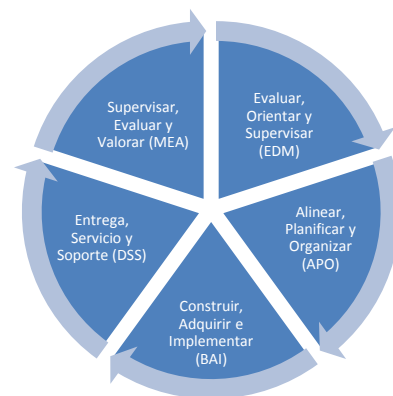
- CONTROL DE ACCESO
- SEGURIDAD FÍSICA Y AMBIENTAL
- MANTENCIÓN, DESARROLLO Y ADQUISICIÓN DE SISTEMAS INFORMÁTICOS
- GESTIÓN DE INCIDENTES DE SEGURIDAD
- CONTROL DE CRIPTOGRAFÍA
- SEGURIDAD EN LAS OPERACIONES

Políticas específicas de la seguridad de la información dirigidas por otras áreas dentro de la empresa

- ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
- RECURSOS HUMANOS
- GESTIÓN DE ACTIVOS
- SEGURIDAD DE LAS COMUNICACIONES
- RELACIÓN CON LOS PROVEEDORES
- CONTINUIDAD DEL NEGOCIO
- CUMPLIMIENTO

PROCESOS

Para cada uno de los procesos aplicados al modelo de negocio SONDA, se representan tanto las necesidades del mismo como los objetivos y las métricas de medición de estos. El siguiente esquema muestra la subdivisión de estos procesos de acuerdo al marco de referencia COBIT 5 For Information security.



Evaluar, Orientar y Supervisar

- Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno
- Asegurar la Entrega de Beneficios
- Asegurar la Optimización del Riesgo
- Asegurar la Optimización de Recursos
- Asegurar la Transparencia hacia las Partes Interesadas

Alinear, Planificar y Organizar

- Gestionar el Marco de Gestión de TI
- Gestionar la Estrategia
- Gestionar la Arquitectura Empresarial
- Gestionar la Innovación
- Gestionar el Portafolio
- Gestionar el Presupuesto y los Costes
- Gestionar los Recursos Humanos
- Gestionar las Relaciones
- Gestionar los Acuerdos de Servicio
- Gestionar los Proveedores
- Gestionar la Calidad
- Gestionar el Riesgo
- Gestionar de la Seguridad

Construir, Adquirir e Implementar

- Gestionar Programas y Proyectos
- Gestionar la Definición de Requisitos
- Gestionar la Identificación y Construcción de Soluciones
- Gestionar la Disponibilidad y la Capacidad
- Gestionar la Introducción del Cambio Organizativo
- Gestionar los Cambios
- Gestionar la Aceptación del Cambio y la Transición
- Gestionar el Conocimiento
- Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso
- Gestionar la Configuración

Entrega, Servicio y Soporte

- Gestionar Operaciones
- Gestionar Peticiones e Incidentes de Servicio
- Gestionar Problemas
- Gestionar la Continuidad
- Gestionar Servicios de Seguridad
- Gestionar Controles de Proceso de Negocio

Supervisar, Evaluar y Valorar

- Supervisar, evaluar y valorar el rendimiento y la conformidad
- Supervisar, Evaluar y Valorar el Sistema de Control Interno
- Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos

III. ESTRUCTURA ORGANIZATIVA

Se identifican las estructuras organizativas de la seguridad de la información:

- Gerencia de la seguridad de la información
- Comité de dirección de la seguridad de la información
- Comité de Gestión de riesgo empresarial
- Custodios de la Información/Propietarios de negocio

Para cada una de ellas se identifican:

- Areas y Características
- Matriz Razi de Alto nivel: Esta incluye Prácticas Clave asociadas a la gestión y Gobierno de la Seguridad de la Información y el nivel de implicación de la estructura organizativa.
- Esquema de entradas y salidas de las estructuras organizativas.

IV. RESULTADOS

De acuerdo a lo planteado en este documento y a lo evaluado en SONDA Colombia, se obtiene un modelo de seguridad, fundamentado en dos buenas practicas de gestión y gobernabilidad; donde es posible medir y controlar los aspectos mas relevantes de seguridad para la compañía.

V. APORTES

Se obtuvo un modelo de seguridad el cual podría servir como estandar para los demás Datacenter de Sonda, al igual que para Datacenters que posean características generales.

VI. CONCLUSIONES

La implantación de un Sistema de Gestión de la Seguridad de la Información proporciona a SONDA Colombia los siguientes beneficios:

- Un análisis de riesgos de sus Sistemas de Información.
- Una gestión adecuada de los riesgos según su modelo de empresa.
- Una mejora continua de su gestión de la seguridad.
- El cumplimiento de la legislación vigente sobre protección de datos de carácter personal, comercio electrónico, propiedad intelectual, etc.
- Facilita el logro de los objetivos de la organización.
- Hace a la organización más segura y consciente de sus riesgos.
- Mejoramiento continuo del Sistema de Control Interno.
- Optimiza la asignación de recursos.
- Aprovechamiento de oportunidades de negocio.
- Fortalece la cultura de autocontrol.
- Mayor estabilidad ante cambios del entorno.
- Conocer y Analizar sus riesgos, identificando amenazas, vulnerabilidades e impactos en su empresa.

- Reducir eficazmente el nivel de riesgo mediante los controles adecuados
- Organizar los recursos de la seguridad.
- Integra la Gestión de la Seguridad SI.
- Aporta confianza a los sistemas de información

Y en definitiva, establece una cultura de la seguridad y una excelencia en el tratamiento de la información en todos sus procesos de negocio. Así, aporta un valor añadido de reconocido prestigio, en la calidad de los servicios que ofrece a sus clientes.

VII. RECOMENDACIONES

El presente modelo podría ser adoptado por aquellas organizaciones que busquen una integración entre la norma ISO 27001 y Cobit 5 For information Security, por ello, sería aconsejable continuar con futuras investigaciones que permitan la elaboración de un modelo general el cual pueda ser fácilmente aplicado a las mismas.

REFERENCIAS

- [1] The History Of ISO 17799 And ISO 27001. Disponible en la web: <<http://www.pc-history.org/17799.htm>>.
- [2] ISO. Estándar internacional ISO/IEC 27001 Disponible en la web: <<http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf>>.
- [3] BSI Group. The new version of ISO/IEC 27001:2013 is here. Disponible en la web: <<http://www.bsigroup.com/en-GB/iso-27001-information-security/ISOIEC-27001-Revision/>>
- [4] BSI Group. Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013. 2013. Disponible en la web: <<http://www.bsigroup.com/Documents/iso-27001/resources/BSI-ISO27001-mapping-guide-UK-EN.pdf>>.
- [5] IS&BCA, Information Security & Business Continuity Academy. Checklist of Mandatory Documentation Required by ISO/IEC 27001 (2013 Revision). 2013. Disponible en la web: <http://www.iso27001standard.com/downloads/Checklist_of_Mandatory_Documentation_Required_by_ISO_27001_2013.pdf>.
- [6] ITERA, IT & Business process. ¿Qué es COBIT? Disponible en la web: <http://www.itera.com.mx/itainstitute/emails/chile/cobit.htm>.

- [7] ESPAÑA. COMISARIA GENERAL DE POLICÍA JUDICIAL U.D.E.F. CENTRAL BRIGADA DE INVESTIGACIÓN TECNOLÓGICA. Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. Disponible en la web: <http://www.fsc.ccoo.es/comunes/recursos/99922/doc28596_Seguridad_informatica.pdf>.
- [8] ISACA. COBIT 5 Enabling Processes. 2012. Disponible en la web: < www.isaca.org/COBIT/Documents/COBIT5-Ver2-enabling.pdf>.
- [9] ISACA. COBIT 5 Enabling Implementation. 2012. Disponible en la web: <<http://www.isaca.org/COBIT/Documents/COBIT5-Ver2-Implementation.pdf>>.
- [10] ISACA. COBIT 5 for Information Security. 2012. Disponible en la web: < <http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf>>.

Autores

Breve referencias sobre la formación académica del autor y su experiencia.