

UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE INGENIERIA

Escuela Profesional de Ingeniería de Sistemas e Informática



“Aplicación de COBIT para la gestión de riesgos de TI en las aulas multimedia de la Universidad Nacional del Santa”

**Tesis para optar el Título Profesional de Ingeniero de Sistemas e
Informática**

TESISTAS:

- Bach: Avila Rodriguez, Denis Walter
- Bach: Román Savas, Sandy Shuley

ASESORA:

- Dra. Briones Pereyra, Lizbeth Dora

NUEVO CHIMBOTE, PERÚ

2025

UNIVERSIDAD NACIONAL DEL SANTA
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E
INFORMÁTICA



CONFORMIDAD DEL ASESOR

La presente Tesis ha sido revisada y desarrollada en cumplimiento del objetivo propuesto y reúne las condiciones formales y metodológicas, estando en cuadrado dentro de las áreas y líneas de investigación conforme al reglamento general para obtener el Título Profesional en la Universidad Nacional del Santa de acuerdo a la denominación siguiente:

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO EN
SISTEMAS E INFORMÁTICA

“APLICACIÓN DE COBIT PARA LA GESTIÓN DE RIESGOS DE TI EN LAS
AULAS MULTIMEDIA DE LA UNIVERSIDAD NACIONAL DEL SANTA”

AUTORES: Bach. DENIS WALTER AVILA RODRIGUEZ
Bach. SANDY SHULEY ROMÁN SAVAS



LIZBETH DORA BRIONES PEREYRA
DNI 32960646
CÓD. ORCID 0000-0003-0626-7227

UNIVERSIDAD NACIONAL DEL SANTA
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E
INFORMÁTICA



CONFORMIDAD DEL JURADO EVALUADOR

El presente Jurado Evaluador da la conformidad del presente informe, desarrollado en cumplimiento del objetivo propuesto y presentado con forme al Reglamento General para obtener el Título Profesional en la Universidad Nacional del Santa, titulado:

“APLICACIÓN DE COBIT PARA LA GESTIÓN DE RIESGOS DE TI EN LAS AULAS MULTIMEDIA DE LA UNIVERSIDAD NACIONAL DEL SANTA”

AUTORES: Bach. DENIS WALTER AVILA RODRIGUEZ
Bach. SANDY SHULEY ROMÁN SAVAS

Revisado y evaluado por el siguiente Jurado Evaluador:

CARLOS ALFREDO GIL NARVÁEZ
PRESIDENTE
DNI: 32970648
CÓD. ORCID: 0000-0003-0137-9545

PEDRO GLICERIO MANCO PULIDO
SECRETARIO
DNI: 32953190
CÓD. ORCID: 0000-0002-8542-2119

LIZBETH DORA BRIONES PEREYRA
INTEGRANTE
DNI: 32960646
CÓD. ORCID: 0000-0003-0626-7227



UNS
UNIVERSIDAD
NACIONAL DEL SANTA

FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ACTA DE EVALUACIÓN PARA SUSTENTACIÓN DE TESIS

En el Campus Universitario de la Universidad Nacional del Santa, siendo las 12:00 p.m. del día lunes 13 de julio de 2026, en el Pabellón de CECOMP, Aula S6, y en cumplimiento de lo dispuesto mediante Resolución Decanal N° 347-2026-UNS-FI, que declara expedito el presente acto académico con fecha 13 de julio de 2026, se procedió a la instalación del Jurado Evaluador, designado por Resolución N° 191-2026-UNS-CFI de fecha 03 de junio de 2026. Dicho Jurado se encuentra integrado por el Ms. Carlos Alfredo Gil Narvéz (Presidente), el Ms. Pedro Glicerio Manco Pulido (Secretario) y la Dra. Lizbeth Dora Briones Pereyra (Integrante), con la finalidad de dar inicio a la sustentación del Informe Final de Tesis titulado: "APLICACIÓN DE COBIT PARA LA GESTIÓN DE RIESGOS DE TI EN LAS AULAS MULTIMEDIA DE LA UNIVERSIDAD NACIONAL DEL SANTA", presentado por los Bachilleres ROMÁN SAVAS SANDY SHULEY, con código de matrícula N° 0201814016, y ÁVILA RODRÍGUEZ DENIS WALTER, con código de matrícula N° 0201814038, quienes cuentan con la asesoría de la Dra. Lizbeth Dora Briones Pereyra, designado mediante Resolución N° 862-2023-UNS-FI, de fecha 13 de diciembre de 2023.

Concluida la exposición, los sustentantes absolvieron las preguntas, observaciones y comentarios formulados por los miembros del Jurado Evaluador, así como por el público asistente.

Luego de una deliberación exhaustiva sobre el contenido del trabajo, la calidad de la exposición y las respuestas brindadas, así como las sugerencias pertinentes, y en concordancia con lo estipulado en los artículos 71° y 111° del Reglamento General de Grados y Títulos vigente de la Universidad Nacional del Santa (aprobado mediante Resolución N° 337-2024-CU-R-UNS del 12 de abril de 2024), el Jurado acuerda otorgar la siguiente nota final de Evaluación:

BACHILLER	CALIFICACIÓN	CONDICIÓN
ÁVILA RODRÍGUEZ DENIS WALTER	17	BUENO

Siendo las 12:40 p.m. se dio por terminado el acto de sustentación y, en señal de conformidad, los miembros del Jurado firman la presente Acta.

Ms. Carlos Alfredo Gil Narvéz
Presidente

Ms. Pedro Glicerio Manco Pulido
Secretario

Dra. Lizbeth Dora Briones Pereyra
Integrante



UNS
UNIVERSIDAD
NACIONAL DEL SANTA

FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ACTA DE EVALUACIÓN PARA SUSTENTACIÓN DE TESIS

En el Campus Universitario de la Universidad Nacional del Santa, siendo las 12:00 p.m. del día lunes 13 de julio de 2026, en el Pabellón de CECOMP, Aula S6, y en cumplimiento de lo dispuesto mediante Resolución Decanal N° 347-2026-UNS-FI, que declara expedito el presente acto académico con fecha 13 de julio de 2026, se procedió a la instalación del Jurado Evaluador, designado por Resolución N° 191-2026-UNS-CFI de fecha 03 de junio de 2026. Dicho Jurado se encuentra integrado por el Ms. Carlos Alfredo Gil Narvéz (Presidente), el Ms. Pedro Glicerio Manco Pulido (Secretario) y la Dra. Lizbeth Dora Briones Pereyra (Integrante), con la finalidad de dar inicio a la sustentación del Informe Final de Tesis titulado: "APLICACIÓN DE COBIT PARA LA GESTIÓN DE RIESGOS DE TI EN LAS AULAS MULTIMEDIA DE LA UNIVERSIDAD NACIONAL DEL SANTA", presentado por los Bachilleres ROMÁN SAVAS SANDY SHULEY, con código de matrícula N° 0201814016, y ÁVILA RODRÍGUEZ DENIS WALTER, con código de matrícula N° 0201814038, quienes cuentan con la asesoría de la Dra. Lizbeth Dora Briones Pereyra, designado mediante Resolución N° 862-2023-UNS-FI, de fecha 13 de diciembre de 2023.

Concluida la exposición, los sustentantes absolvieron las preguntas, observaciones y comentarios formulados por los miembros del Jurado Evaluador, así como por el público asistente.

Luego de una deliberación exhaustiva sobre el contenido del trabajo, la calidad de la exposición y las respuestas brindadas, así como las sugerencias pertinentes, y en concordancia con lo estipulado en los artículos 71° y 111° del Reglamento General de Grados y Títulos vigente de la Universidad Nacional del Santa (aprobado mediante Resolución N° 337-2024-CU-R-UNS del 12 de abril de 2024), el Jurado acuerda otorgar la siguiente nota final de Evaluación:

BACHILLER	CALIFICACIÓN	CONDICIÓN
ROMÁN SAVAS SANDY SHULEY	17	Bueno

Siendo las 12:40 p.m. se dio por terminado el acto de sustentación y, en señal de conformidad, los miembros del Jurado firman la presente Acta.

Ms. Carlos Alfredo Gil Narvéz
Presidente

Ms. Pedro Glicerio Manco Pulido
Secretario

Dra. Lizbeth Dora Briones Pereyra
Integrante



Recibo digital

Este recibo confirma que su trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega: Lizbeth Briones
Título del ejercicio: APLICACIÓN DE COBIT PARA LA GESTIÓN DE RIESGOS DE TI E...
Título de la entrega: COBIT_AVILA_ROMAN.pdf
Nombre del archivo: COBIT_AVILA_ROMAN.pdf
Tamaño del archivo: 2.14M
Total páginas: 109
Total de palabras: 18,996
Total de caracteres: 110,441
Fecha de entrega: 21-oct-2026 10:54p. m. (UTC-0500)
Identificador de la entrega: 3066859716



COBIT_AVILA_ROMAN.pdf

INFORME DE ORIGINALIDAD

14%	13%	3%	14%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	estrategiasdetiitch.blogspot.com	7%
	Fuente de Internet	
2	marcosdegobiernoyreferenci.blogspot.com	3%
	Fuente de Internet	
3	www.scribd.com	2%
	Fuente de Internet	
4	Submitted to Universidad del Istmo de Panamá	2%
	Trabajo del estudiante	
5	Submitted to Universidad Internacional de la Rioja	1%
	Trabajo del estudiante	

Excluir citas

Activo

Exclude assignment template

Activo

Excluir bibliografía

Activo

Excluir coincidencias

< 15 words

DEDICATORIA

*Esta tesis es dedicada a nuestras familias
que siempre confiaron en nosotros, por
formarnos con buenos hábitos y valores, y
por enseñarnos a perseverar en los
momentos difíciles.*

Denis Walter Avila Rodriguez

Sandy Shuley Román Savas

AGRADECIMIENTO

En primer lugar, dar gracias a Dios por acompañarnos en todo momento de nuestras vidas y guiarnos por el camino correcto.

Agradecemos a la Universidad Nacional Del Santa por permitirnos formar parte de ella y brindarnos los conocimientos necesarios para nuestra preparación profesional.

A nuestros padres por el apoyo incondicional en las decisiones tomadas en este largo camino universitario.

Queremos agradecer también a la Dra. Lizbeth Dora Briones Pereyra, por guiarnos en todo este tiempo en el desarrollo de nuestra tesis y dar respuestas a nuestras dudas.

Denis Walter Avila Rodriguez

Sandy Shuley Román Savas

PRESENTACIÓN

Señores miembros del jurado evaluador:

De acuerdo con lo dispuesto en el Reglamento General de Grados y Títulos de la Universidad Nacional del Santa, presentamos ante ustedes el Informe de Tesis titulada: **“APLICACIÓN DE COBIT PARA LA GESTIÓN DE RIESGOS DE TI EN LAS AULAS MULTIMEDIA DE LA UNIVERSIDAD NACIONAL DEL SANTA”** la cual dejamos a disposición de ustedes y esperamos cumpla con los requisitos de aprobación para optar el Título Profesional de Ingeniería de Sistemas e Informática.

En esta investigación se dará lugar al sector de educación en la ciudad de Nuevo Chimbote, el cual se tiene como propósito realizar la aplicación de COBIT para permitir la gestión de riesgos de las aulas multimedia en la Universidad Nacional del Santa.

Después de haber expuesto lo siguiente ante ustedes señores miembros del jurado evaluador, ponemos a su disposición este informe de tesis, con el objetivo de cumplir los requisitos para su aprobación.

INDICE

DEDICATORIA.....	VIII
AGRADECIMIENTO	IX
PRESENTACIÓN.....	X
INDICE	XI
INDICE DE TABLAS	XIV
INDICE DE FIGURAS	XVIII
RESUMEN	XX
ABSTRACT.....	XXI
INTRODUCCIÓN	XXII
DATOS GENERALES DEL ESTUDIO	24
TITULO DEL PROYECTO	24
TESISTAS	24
ASESORA	24
TIPO DE INVESTIGACIÓN	24
DELIMITACION DEL ESTUDIO	24
METODO DE INVESTIGACION.....	24
REGIMEN DE INVESTIGACION.....	25
AREA DE DESARROLLO DEL PROYECTO.....	25
LUGAR DE INVESTIGACION.....	25
CAPITULO I.....	26
INTRODUCCIÓN	26
1.1. DESCRIPCION Y FORMULACIÓN DEL PROBLEMA.....	27
1.1.1. RAZÓN SOCIAL.....	27
1.1.2. DOMICILIO LEGAL	27
1.1.3. RUC.....	27
1.1.4. ACTIVIDAD DE LA EMPRESA.....	27
1.1.5. LOGOTIPO.....	27
1.1.6. DIRECCIONAMIENTO ESTRATÉGICO DE LA EMPRESA.....	27
VISIÓN	27
MISIÓN	27
VALORES	28
1.1.7. FORMULACIÓN DEL PROBLEMA	28
1.2. OBJETIVOS.....	28

1.2.1.	OBJETIVO GENERAL	28
1.2.2.	OBJETIVOS ESPECÍFICOS	29
1.3.	FORMULACIÓN DE LA HIPÓTESIS	29
1.4.	JUSTIFICACIÓN E IMPORTANCIA	29
1.4.1.	JUSTIFICACIÓN SOCIAL	29
1.4.2.	JUSTIFICACIÓN OPERATIVA	29
1.4.3.	JUSTIFICACIÓN TECNOLÓGICA	29
1.4.4.	JUSTIFICACIÓN METODOLÓGICA	30
1.4.5.	JUSTIFICACIÓN ECONÓMICA	30
1.4.6.	JUSTIFICACIÓN PRÁCTICA	30
1.4.7.	IMPORTANCIA DE LA INVESTIGACIÓN	30
CAPITULO II		31
MARCO TEÓRICO		31
2.1.	ANTECEDENTES DEL PROBLEMA	32
2.1.1.	NIVEL INTERNACIONALES	32
2.1.2.	NIVEL NACIONAL	32
2.1.3.	NIVEL LOCAL	35
2.2.	MARCO TEÓRICO Y CONCEPTUAL	35
2.2.1.	APLICACIÓN	35
2.2.2.	GESTIÓN	35
2.2.3.	AULAS MULTIMEDIA	36
2.2.4.	UNIVERSIDAD	36
2.2.5.	ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	36
2.2.6.	GESTIÓN DE RIESGOS	36
2.2.7.	ISO 31000	37
2.2.8.	COBIT	¡Error! Marcador no definido.
2.2.9.	PRINCIPIOS COBIT	39
2.2.10.	COMPONENTES	40
2.2.11.	DOMINIOS	40
2.2.12.	OBJETIVOS	41
2.2.13.	GOBIERNO	42
2.3.	GESTION COBIT	42
2.3.1.	NIVELES	42
2.4.	PROCESOS APO	42
2.5.	PROCESOS EDM	45
2.6.	PROCESOS BAI	46

2.7. PROCESOS DSS.....	48
2.8. PROCESOS MEA.....	49
CAPITULO III.....	51
MATERIALES Y MÉTODOS	51
3.1. DISEÑO DE CONTRASTACIÓN DE LA HIPÓTESIS.....	51
3.2. POBLACIÓN.....	52
3.3. MUESTRA.....	52
3.4. OPERACIONALIZACIÓN DE LAS VARIABLES.....	53
3.5. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS	53
3.5.1. TÉCNICAS.....	53
3.5.2. INSTRUMENTOS	53
3.5.3. VALIDEZ Y CONFIABILIDAD DE LOS INSTRUMENTOS.....	54
3.5.4. METODOLOGÍA PARA EL DESARROLLO DEL ESTUDIO	54
CAPITULO IV.....	58
RESULTADOS Y DISCUSIÓN	58
4.1. APLICACION DEL MARCO COBIT E ISO 31000.....	59
4.1.1. DIAGNOSTICO DEL CONTEXTO TECNOLÓGICO DE LAS AULAS MULTIMEDIA	59
4.1.2. ALINEAMIENTO COBIT: OBJETIVOS INSTITUCIONALES, OBJETIVOS DE TI Y PROCESOS PRIORIZADOS	59
4.1.3. EVALUACIÓN DE CAPACIDAD Y BRECHAS DE GOBIERNO DE TI	66
4.1.4. GESTIÓN DE RIESGOS SEGÚN ISO 31000	92
4.2. ANÁLISIS DE RESULTADOS	113
4.3. DISCUSIÓN.....	116
CAPITULO V	117
CONCLUSIONES Y RECOMENDACIONES.....	117
5.1. CONCLUSIONES.....	118
5.2. RECOMENDACIONES.....	119
Referencias Bibliográficas.....	120

INDICE DE TABLAS

Tabla 1	53
Operacionalización de las variables	53
Tabla 2	60
Ponderación de Objetivos Empresariales según COBIT	60
Tabla 3	60
Valoración realizada en la UNS para los objetivos corporativos.....	60
Tabla 4	61
Resultados de objetivos de la empresa con mayor ponderación	61
Tabla 5	62
Cruce de los alcances de la institución seleccionados con las finalidades TI	62
Tabla 6	63
Resultados de los objetivos de la institución seleccionados con los objetivos TI	63
Tabla 7	64
Ponderación de Objetivos Empresariales según COBIT	64
Tabla 9	65
Valoración de Procesos Facilitadores.....	65
Tabla 10	66
Resultados de Ponderación de Procesos Facilitadores.....	66
Tabla 11	67
EDM03	67
Tabla 12	67
EDM04	67
Tabla 13	68
APO01.....	68
Tabla 14	68
APO12.....	68
Tabla 15	69
APO13.....	69
Tabla 16	69
BAI01	69
Tabla 17	70
BAI09	70
Tabla 18	70
BAI10	70

Tabla 19	70
DSS02	70
Tabla 20	71
DSS03	71
Tabla 21	71
DSS04	71
Tabla 22	71
DSS05	71
Tabla 23	72
MEA02	72
Tabla 24	72
EDM03	72
Tabla 25	73
Valoración de nivel de capacidad EDM03	73
Tabla 26	73
EDM04	73
Tabla 27	75
Valoración de nivel de capacidad EDM04	75
Tabla 28	75
APO01	75
Tabla 29	76
Valoración de nivel de capacidad APO01	76
Tabla 30	77
APO12	77
Tabla 31	77
Valoración de nivel de capacidad APO12	77
Tabla 32	78
APO13	78
Tabla 33	79
Valoración de nivel de capacidad APO13	79
Tabla 34	80
BAI01	80
Tabla 35	81
Valoración de nivel de capacidad BAI01	81
Tabla 36	82

BAI09	82
Tabla 37	84
Valoración de nivel de capacidad BAI09	84
Tabla 38	84
BAI10	84
Tabla 39	85
Valoración de nivel de capacidad BAI10	85
Tabla 40	85
DSS02	85
Tabla 41	86
Valoración de nivel de capacidad DSS02	86
Tabla 42	86
DSS03	86
Tabla 43	87
Valoración de nivel de capacidad DSS03	87
Tabla 44	87
DSS04	87
Tabla 45	88
Valoración de nivel de capacidad DSS04	88
Tabla 46	88
DSS05	88
Tabla 47	90
Valoración de nivel de capacidad DSS05	90
Tabla 48	90
MEA02	90
Tabla 49	91
Valoración de nivel de capacidad MEA02	91
Tabla 50	91
Evaluación consolidada de capacidad y brechas COBIT	91
Tabla 51	97
Identificación de los riesgos	97
Tabla 52	98
Niveles de probabilidad de riesgo	98
Tabla 53	99
Niveles de impacto de riesgo	99

Tabla 54	99
Esquema de Probabilidad e Impacto	99
Tabla 55	100
Niveles de riesgo cualitativo	100
Tabla 56	100
Niveles de riesgo cuantitativos	100
Tabla 57	101
Matriz de análisis de probabilidad por impacto	101
Tabla 58	101
Impacto Cuantitativo del Riesgo	101
Tabla 59	104
Evaluación de riesgos.....	104
Tabla 60	106
Tratamiento de riesgos	106
Tabla 61	109
Esquema técnico de monitoreo, revisión y comunicación de riesgos	109
Tabla 62	110
Criterios de aceptabilidad y respuesta al riesgo.....	110
Tabla 63	111
Matriz consolidada de riesgos y niveles de exposición.....	111
Tabla 64	112
Plan de tratamiento, control y mitigación de riesgos.....	112
Tabla 65	114
Resultados de procesos alcanzados.....	114

INDICE DE FIGURAS

Figura 1.....	37
Proceso ISO 31000	37
Figura 2.....	38
Principios de COBIT	38
Figura 3.....	39
Procesos de COBIT 5.....	39
Figura 4.....	73
Radar de atributos de capacidad EDM03.....	73
Figura 5.....	74
Radar de atributos de capacidad EDM04.01	74
Figura 6.....	74
Radar de atributos de capacidad EDM04.02	74
Figura 7.....	75
Radar de atributos de capacidad EDM04.03	75
Figura 8.....	76
Radar de atributos de capacidad APO01.02	76
Figura 9.....	76
Radar de atributos de capacidad APO01	76
Figura 10.....	77
Radar de atributos de capacidad APO12	77
Figura 11.....	78
Radar de atributos de capacidad APO13.01	78
Figura 12.....	79
Radar de atributos de capacidad APO13.02	79
Figura 13.....	79
Radar de atributos de capacidad APO13.03	79
Figura 14.....	80
Radar de atributos de capacidad BAI01.02.....	80
Figura 15.....	81
Radar de atributos de capacidad BAI01.07.....	81
Figura 16.....	81
Radar de atributos de capacidad BAI01.....	81
Figura 17.....	82
Radar de atributos de capacidad BAI09.01.....	82

Figura 18.....	83
Radar de atributos de capacidad BAI09.02.....	83
Figura 19.....	83
Radar de atributos de capacidad BAI09.....	83
Figura 20.....	84
Radar de atributos de capacidad BAI10.1.....	84
Figura 21.....	85
Radar de atributos de capacidad BAI10.....	85
Figura 22.....	86
Radar de atributos de capacidad DSS02	86
Figura 23.....	87
Radar de atributos de capacidad DSS03	87
Figura 24.....	88
Radar de atributos de capacidad DSS04	88
Figura 25.....	89
Radar de atributos de capacidad DSS05.04	89
Figura 26.....	89
Radar de atributos de capacidad DSS05	89
Figura 27.....	90
Radar de atributos de capacidad MEA02	90
Figura 28.....	115
Resultados de evaluación COBIT en la UNS.....	115

RESUMEN

En esta investigación se desea aplicar COBIT para evaluar la Gestión de Riesgos de TI en las Aulas Multimedia de la Universidad Nacional del Santa. Ya que esta metodología, permite realizar un análisis profundo de lo que se desea, en empresas pequeñas, medianas y grandes. Además, como principal interés en que el servicio de enseñanza no se vea perjudicado frente a la falta de gestión de riesgos para los recursos tecnológicos.

En nuestro estudio se hizo uso del tipo descriptiva-aplicada, es así como para el desarrollo se usó el marco de trabajo COBIT y la ISO 31000, lo que permitió mantener un orden y control de todos los procedimientos y evaluaciones que se realizaron en la gestión de riesgos. Este análisis que se realizó permitió lograr los objetivos establecidos, demostrando que en la universidad nacional del santa es necesario implementar una correcta gestión de los recursos de TI debido al poco alcance que se observó con respecto a los procesos y subprocesos evaluados, además, después de identificar los riesgos se halló que están en un nivel muy alto y con impactos catastróficos para la institución y su servicio de enseñanza, además, para la seguridad de los estudiantes y docentes que usan las aulas multimedia.

Palabras clave: COBIT, aulas multimedia, riesgos

Autores:

Bach. Denis Walter Avila Rodriguez

Bach. Sandy Shuley Román Savas

Asesora:

Dra. Lizbeth Dora Briones Pereira

ABSTRACT

In this research we want to apply COBIT to evaluate IT Risk Management in the Multimedia Classrooms of the National University of Santa. Since this methodology allows for a deep analysis of what is desired, in small, medium and large companies. Furthermore, the main interest is that the teaching service is not harmed by the lack of risk management for technological resources.

Our study employed a descriptive-applied approach, utilizing the COBIT framework and the ISO 31000 standard. This ensured order and control throughout the procedures and assessments conducted as part of the risk management process. The analysis enabled the achievement of the established objectives, demonstrating that the Universidad Nacional del Santa needs to implement proper IT resource management—a necessity highlighted by the limited scope observed in the processes and sub-processes evaluated. Furthermore, the identified risks were found to be at a very high level, posing potentially catastrophic impacts on the institution and its educational services, as well as on the safety of the students and faculty who use the multimedia classrooms.

Keywords: COBIT, multimedia classrooms, risks

Authors:

Bach. Denis Walter Avila Rodriguez

Bach. Sandy Shuley Román Savas

Advisor:

Dra. Lizbeth Dora Briones Pereira

INTRODUCCIÓN

En esta investigación se presenta las necesidades de la UNS que se encuentra ubicada en Nuevo Chimbote, en base a la Gestión de Riesgos en sus aulas multimedia para ofrecer a la población estudiantil el mejor servicio de enseñanza. Se logró identificar potenciales riesgos que desatarían consecuencias graves e Inadmisibles, lo que significa que la aplicación de una metodología como COBIT se presenta como una estrategia para su identificación y toma de decisiones con respecto a los riesgos a los que se expone a todos los recursos de TI y sobre todo la calidad del servicio de enseñanza que se brinda en la institución, lo cual es primordial para posicionarse dentro de las mejores instituciones nacionales de enseñanza superior.

Nuestro objetivo principal es aplicar COBIT para lograr Evaluar la Gestión de Riesgos de TI en las Aulas Multimedia de la Universidad Nacional del Santa, lo cual nos permite alcanzar las metas detalladas como aplicar la matriz COBIT, identificar y describir los riesgos en las TI, realizar un análisis del riesgo de ti, obtener el impacto de cada riesgo y proponer su mitigación, crear la matriz de riesgos para la toma de decisiones y opciones de tratamiento, proponer una mejora para la optimización de activos, recursos y capacidades de las TI.

La hipótesis que se formuló para nuestra investigación es: “La aplicación de COBIT permite evaluar la gestión de riesgos de TI en las aulas multimedia de la Universidad Nacional del Santa”.

El estudio desarrollado contiene:

CAPITULO I: LA EMPRESA. En esta parte de la investigación se observan datos principales de la UNS como su actividad principal, donde se ubica, misión, visión, y valores de la universidad en la que estamos realizando el análisis.

CAPITULO II: PLANTEAMIENTO DEL PROBLEMA. Para este capítulo se realiza el planteamiento de la realidad problemática, análisis del problema, formulación del problema, importancia de la investigación, justificación, hipótesis y objetivos.

CAPITULO III: MARCO TEÓRICO. En la presente sección se abordan los antecedentes del tema de investigación en el aspectos internacional, nacional y local, además, se plantea las teorías y conceptos relacionados con el tema de investigación que dan sustento a las variables de estudio.

CAPITULO IV: METODOLOGÍA DEL DESARROLLO DE LA VARIABLE INDEPENDIENTE. En este apartado describimos el enfoque metodológico para la aplicación de la metodología COBIT, incluyendo la matriz con procesos y subprocesos, además, la identificación de riesgos.

CAPITULO V: MATERIALES Y MÉTODOS. En esta sección se detalla el diseño de contrastación de la hipótesis, tomamos los siguientes puntos como la población, muestra, técnicas y la metodología de validación de la metodología.

CAPITULO VI: RESULTADOS Y DISCUSIÓN. En este capítulo se presentan los resultados obtenidos tras la implementación de la metodología.

CAPITULO VII: CONCLUSIONES Y RECOMENDACIONES. Para esta sección se desarrollan las conclusiones y recomendaciones finales en base a lo que ha planteado en la ejecución del trabajo de investigación.

DATOS GENERALES DEL ESTUDIO

TITULO DEL PROYECTO

“APLICACIÓN DE COBIT PARA LA GESTIÓN DE RIESGOS DE TI EN LAS AULAS MULTIMEDIA DE LA UNIVERSIDAD NACIONAL DEL SANTA”

TESISTAS

Bach. Denis Walter Avila Rodriguez

Bach. Sandy Shuley Román Savas

ASESORA

Dra. Lizbeth Dora Briones Pereyra

TIPO DE INVESTIGACIÓN

Según su Naturaleza es de tipo **Descriptiva** porque debido a la auditoría que se realiza se describe, identifica y evalúa el estado en el que se encuentran las aulas multimedia, como consecuencia de la descripción y evaluación del estado real se llega a plantear hipótesis a fin de optimizar los procedimientos aplicados.

Según su fin o propósito es de tipo **Aplicada** debido a que se genera una solución en base a la problemática planteada en las aulas multimedia de la Universidad Nacional del Santa, donde se realiza una auditoría con la finalidad de analizar, evaluar los riesgos y los servicios informáticos y promover el cumplimiento de la normativa ISO.

DELIMITACION DEL ESTUDIO

En nuestro proyecto se realiza la aplicación del marco de referencia COBIT, centrándose en el área de la Gestión de Riesgos de TI, lo cual nos lleva a poder diagnosticar, actuar y prevenir para brindar un servicio de calidad.

METODO DE INVESTIGACION

Es **Inductivo – Deductivo** ya que se realiza la definición de la problemática y es una investigación aplicada en la cual se planteará la hipótesis para hacer uso de

indicadores de la variable independiente para la observación y percepción de las consecuencias de la hipótesis son viables con respecto a los resultados de la aplicación de COBIT para la gestión de riesgos de TI en las aulas multimedia de la UNS, con la finalidad de una correcta aplicación en la institución, se propondrá la aplicación de una serie de buenas prácticas para lograr la determinación de la viabilidad que permitirá a los trabajadores y a la institución a contar con una mejor gestión de la seguridad de todos los implementos y ambientes tecnológicos

REGIMEN DE INVESTIGACION

La investigación es libre, ya que se da por iniciativa de los investigadores, y poder evaluar correctamente la gestión del riesgo con el uso de COBIT.

AREA DE DESARROLLO DEL PROYECTO

LOCALIDAD

Departamento: Ancash

Provincia : Santa

Distrito : Nuevo Chimbote

LUGAR DE INVESTIGACION

Universidad Nacional del Santa

Escuela Profesional de Ingeniería de Sistemas e Informática

Nuevo Chimbote – Ancash – Perú

CAPITULO I

INTRODUCCIÓN

1.1. DESCRIPCION Y FORMULACIÓN DEL PROBLEMA

1.1.1. RAZÓN SOCIAL

UNIVERSIDAD NACIONAL DEL SANTA

1.1.2. DOMICILIO LEGAL

Av. Pacifico Nro. 508 Urb. Buenos Aires

1.1.3. RUC

20148309109

1.1.4. ACTIVIDAD DE LA EMPRESA

Enseñanza Superior

1.1.5. LOGOTIPO



1.1.6. DIRECCIONAMIENTO ESTRATÉGICO DE LA EMPRESA

- **VISIÓN**

La visión de la Universidad hace referencia al desarrollo del potencial desde la infancia temprana, acceden al ámbito de la lectoescritura, resuelven problemas, ejercen valores y saben seguir aprendiendo, se asumen ciudadanos con derechos y obligaciones que contribuyen al desarrollo de sus comunidades y del país combinado su capital cultural y natural con avances mundiales.

- **MISIÓN**

Brindar formación profesional humanística, científica y tecnológica a los estudiantes, con calidad y responsabilidad social y ambiental.

- **VALORES**

- ✓ **Respeto:** Los trabajadores de la universidad ponen en práctica ese valor para llevar una buena convivencia y la fluida comunicación en todas las áreas.
- ✓ **Compromiso con la calidad:** La calidad en la enseñanza es lo que caracteriza a nuestro lugar de estudio, todo ello se ve reflejado en los grandes profesionales formados.
- ✓ **Innovación:** Proyectos de gran alcance son los que han ayudado a nuestra alma mater a resaltar frente a las demás instituciones.
- ✓ **Creatividad:** Un gran valor que caracteriza a todo alumno de la UNS, gracias a la gran enseñanza de sus docentes que ayudan con la creación de nuevos proyectos.
- ✓ **Libertad de Pensamiento:** Todos los que pertenecemos a la UNS sabemos y expresamos con total libertad nuestros deseos por mejorar la institución, así como la plana docente con el objetivo de contar con la mejor universidad local y/o nacional.
- ✓ **Crítica:** Es un valor característico de la institución ya que ello es por lo que se ha llegado lejos y contamos con una enseñanza y plana docente de calidad.
- ✓ **Solidaridad:** Valorar nuestros conocimientos, así como mostrárselo a los demás con los proyectos puestos en marcha.

1.1.7. FORMULACIÓN DEL PROBLEMA

¿De qué manera la Aplicación de COBIT contribuye a la evaluación de la Gestión de Riesgos de Ti en las Aulas Multimedia, estableciendo mecanismos de control y mitigación de los niveles de exposición al riesgo en la Universidad Nacional Del Santa?

1.2. OBJETIVOS

1.2.1. OBJETIVO GENERAL

Evaluar la gestión de riesgos de TI mediante la aplicación del marco COBIT en las Aulas Multimedia de la Universidad Nacional del Santa.

1.2.2. OBJETIVOS ESPECÍFICOS

- Identificar riesgos en las TI, así como, amenazas que nos acercarán a la concertación como tal del riesgo.
- Realizar un análisis adecuado y profundo del riesgo de ti.
- Obtener el impacto de cada riesgo y proponer su mitigación.
- Crear la matriz de riesgos para la toma de decisiones, y opciones de tratamiento.
- Proponer mejoras para la optimización de activos, recursos y capacidades de las TI

1.3. FORMULACIÓN DE LA HIPÓTESIS

La aplicación de COBIT contribuye a fortalecer la gestión de riesgos de TI en las aulas multimedia de la Universidad Nacional del Santa, mediante la identificación y análisis de los riesgos, el establecimiento de mecanismos de control y mitigación orientados a reducir los niveles de exposición al riesgo.

1.4. JUSTIFICACIÓN E IMPORTANCIA

1.4.1. JUSTIFICACIÓN SOCIAL

Cuando se cuenta con ambientes seguros, los docentes y alumnos se sentirán más seguros del lugar donde están aprendiendo, lo cual mejorará el servicio de enseñanza que se brinda, así como el producto observado en proyectos de investigación.

1.4.2. JUSTIFICACIÓN OPERATIVA

Con un mejor manejo de los procesos permite trabajar con una mayor competencia en el desarrollo de las labores lectivas, ya que se dispondrá de ambientes más seguros y mejor equipados.

1.4.3. JUSTIFICACIÓN TECNOLÓGICA

Permite organizar y controlar la gestión de TI en las aulas multimedia de la UNS, identificando procesos críticos, brechas de control y riesgos que pueden afectar la continuidad del servicio educativo. Además, facilita la definición de mecanismos de control y mitigación orientados a reducir los niveles de exposición al riesgo y

fortalecer la seguridad, disponibilidad y administración de los recursos tecnológicos.

1.4.4. JUSTIFICACIÓN METODOLÓGICA

Se justifica metodológicamente en base a la aplicación de un proceso estructurado que permita una correcta trazabilidad de la gestión de riesgos de TI en las aulas multimedia. Además, la integración del marco COBIT con ISO 31000 nos permite vincular los objetivos de la universidad con los procesos de gobierno y gestión de TI, identificar y analizar bajo los criterios estándares establecidos.

1.4.5. JUSTIFICACIÓN ECONÓMICA

La reducción de costos es una oportunidad significativa frente a las fallas tecnológicas, pérdidas, robos o deterioros de los equipos, permite optimizar los recursos para tecnología e inversiones a largo plazo.

1.4.6. JUSTIFICACIÓN PRÁCTICA

Permite ser la base para una mejor administración operativa de las aulas multimedia, además, prioriza acciones de mantenimiento, actualización, control y seguimiento, promoviendo la continuidad del servicio educativo.

1.4.7. IMPORTANCIA DE LA INVESTIGACIÓN

Al aplicarse una auditoria basada en COBIT será de gran importancia para identificar las deficiencias de las aulas multimedia y posterior a eso obtener resultados óptimos teniendo como base las normativas ISO 31000 para el incremento del grado de protección de la información, servicios y equipos informáticos.

CAPITULO II

MARCO TEÓRICO

2.1. ANTECEDENTES DEL PROBLEMA

2.1.1. NIVEL INTERNACIONALES

Tesis 01

Título: “Verificación De La Seguridad En La Aplicación Del Estándar COBIT Para La Evaluación De La Administración De Las Tecnologías De La Información En El Servicio Nacional De Aprendizaje (Sena Regional Magdalena)”

Autores: José Alfonso Castro Cantillo y Juliette Katherine Paredes Acevedo

Año: 2023

Lugar: Santa Marta/Colombia

Resumen ejecutivo:

La tesis lleva por título “VERIFICACIÓN DE LA SEGURIDAD EN LA APLICACIÓN DEL ESTÁNDAR COBIT PARA LA EVALUACIÓN DE LA ADMINISTRACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN EL SERVICIO NACIONAL DE APRENDIZAJE (SENA REGIONAL MAGDALENA)”, tiene como objetivo la evaluación de un área de sistemas de una organización mediante el estándar de seguridad COBIT, para determinar si los pasos ejecutados en el estudio fueron los requeridos para el estudio y así poder determinar las recomendaciones dadas a la oficina de sistemas del Servicio de Aprendizaje, fueron las más óptimas para el manejo de toda su información interna y externa que esta maneja para su buen funcionamiento.

Relación con el estudio:

Este estudio se relaciona con nuestra investigación ya que aplica COBIT como una propuesta de solución frente a la problemática que hallan en el estudio de la organización y frente a la idea global de cómo se encuentra conformada y con las políticas que rigen su funcionamiento.

2.1.2. NIVEL NACIONAL

Tesis 02

Título: “Aplicación De La Metodología COBIT 5 Para La Mejora De Procesos De Auditoria Y Seguridad Informática En La Empresa DATCO S&H, Huaraz”

Autor: Emerson Elí Chavez Angeles

Año: 2020

Lugar: Huaraz/Perú

Resumen ejecutivo:

La tesis titulada, “APLICACIÓN DE LA METODOLOGIA COBIT 5 PARA LA MEJORA DE PROCESOS DE AUDITORIA Y SEGURIDAD INFORMÁTICA EN LA EMPRESA DATCO S&H, HUARAZ”, tiene como objetivo informar los hallazgos de la aplicación de la norma COBIT5 en el transcurso de transferencias de información contable, financiera y administrativa del área de Gerencia General de la Empresa DATCO S&H.

Relación con el estudio:

La relación que tiene con el estudio se da ya que en esta tesis también se hace uso de COBIT para brindar una mejor auditoría, logrando evaluaciones más acertadas y que contribuyan con los objetivos organizacionales. La escogen debido a que es una metodología aprobada en empresas de seguros más importantes del Perú, haciéndola muy confiable para la mejora de una gestión informática en organizaciones.

Tesis 03

Título: “COBIT y la infraestructura tecnológica de la empresa AGB Soluciones SAC, 2019”

Autores: Axel Jussiefp Lezcano Figueroa y Omar José Sevilla Ochoa

Año: 2019

Lugar: Lima/Perú

Resumen ejecutivo:

La tesis que tiene de título “COBIT Y LA INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA AGB SOLUCIONES SAC, 2019”, tiene como finalidad establecer la corelación que existe entre COBIT y la infraestructura tecnológica de la empresa AGB soluciones. La investigación que se realiza es de no experimental en la cual aplican el método científico, y

finalmente usan COBIT para proteger los datos de la corporación y su aseguramiento.

Relación con el estudio:

Está relacionado con nuestra investigación debido a que también se hace uso de COBIT en una investigación no experimental, así como también se hace uso de dicha metodología para la infraestructura tecnológica. Esta metodología ayudará con sus lineamientos de buenas prácticas para el control de las TI de la empresa, también para mejorar el acatamiento regulatorio y el crecimiento de valor alineando los objetivos del negocio.

Tesis 04

Título: “Auditoría de Sistemas Informáticos”

Autor: Jose Omar Saenz Flores

Año: 2019

Lugar: Moquegua/Perú

Resumen ejecutivo:

La tesis tiene por título “AUDITORIA DE SISTEMAS INFORMÁTICOS”, la cual tiene como meta un mejoramiento en las etapas de TI de la librería sagrado corazón de Jesús utilizando COBIT 5. Y se pudo identificar procesos diferentes tanto de gobierno como de gestión de TI, los cuales fueron para proteger la optimización del riesgo, la eficientización de los recursos, la transparencia hacia las partes interesadas, dirigir las estrategias y desarrollar la aceptación del cambio y de la transición.

Relación con el estudio:

La tesis se relaciona con la investigación ya que se hace uso de la metodología COBIT, para poder responder a preguntas de que es lo que se quiere hacer, lograr, donde se quiere llegar, teniendo en cuenta la potenciación de riesgos y de recursos. Al igual que nuestra investigación inicializamos con la identificación de las metas para finalmente obteniendo metas y procesos de mayor importancia y mejorarlos.

2.1.3. NIVEL LOCAL

Tesis 05

Título: “Diagnóstico y propuesta de mejora del nivel de gestión de adquisición e implementación de las tecnologías de información y comunicación (tic) en el Hospital Regional Eleazar guzmán barrón del distrito de nuevo Chimbote 2015”

Autor: Giancarlo Giovannini Calderón Velásquez

Año: 2020

Lugar: Chimbote / Perú

Resumen ejecutivo:

La tesis relacionada con una propuesta para mejorar la gestión de adquisición en un hospital tiene como objetivo la gestión en el abastecimiento y sostenimiento de infraestructura y tecnologías en el soporte de gestión administrativa y médica del hospital, después de aplicar COBIT se pudo realizar las sugerencias a la gestión de la tecnología informática que conlleven a lograr mejores resultados.

Relación con el estudio:

Está relacionado con el estudio ya que se aplica COBIT, luego de realizar entrevistas para poder seleccionar los procesos que sean necesarios, ya que no se podría aplicar toda la auditoria, luego de seleccionar los procesos se analizaron los hallazgos.

2.2. MARCO TEÓRICO Y CONCEPTUAL

2.2.1. APLICACIÓN

Es la acción de hacer uso, empleo o utilidad de algo. En nuestro proyecto se pondrá en práctica todas las actividades que conllevan al modelo COBIT para la gestión de riesgos. (Real Academia Española, 2023)

2.2.2. GESTIÓN

Esta palabra nos hace referencia a cumplir con la ejecución de un conjunto de actividades, las cuales nos llevarán a un fin en común. También se puede hacer

uso de la palabra diligencias para hacer referencia a que estamos realizando una gestión para cumplir con un deseo. (Martínez, 2024)

2.2.3. AULAS MULTIMEDIA

Se trata de una sala o un espacio habilitado y preparado para albergar recursos para actividades de aprendizaje utilizando ordenadores y herramientas audiovisuales. Las aulas están especialmente preparadas y equipadas con las medidas de conectividad y seguridad adecuadas para acceder a internet y visualizar archivos audiovisuales. (Fombona & Pascual, 2020)

2.2.4. UNIVERSIDAD

Es una institución de enseñanza superior, la cual se divide en grupos denominados facultades además cada grupo contiene especialidades de enseñanza. Este concepto también es usado para la infraestructura que se destina a la enseñanza superior. (Osteicoechea, 2023)

2.2.5. ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN

El área de TI tiene como propósito principal: el estudio, diseño, desarrollo, e implementación de las herramientas informáticas que son utilizados para la manipulación de datos e información de una empresa u organización.

En esta oficina no solo se encargan del análisis, diseño y desarrollo de las soluciones informáticas internas, además, del soporte técnico de los usuarios, de entregar los recursos tales como PC's, programas, etc. (Pachón, 2024)

2.2.6. GESTIÓN DE RIESGOS

Conlleva un conjunto de actividades que se formulan con la meta de poder identificar, evaluar y finalmente lograr el objetivo el cual es disminuir el impacto del riesgo, así podremos prevenir de posibles amenazas y evitar una falla en el funcionamiento continuo. Con ello se hará visibles las amenazas para poder tomar medidas de mitigar las posibilidades de que suceda. (2024)

Comprende a personas, flujos y tecnología con el fin de establecer objetivos acordes o alineados a los valores de la empresa. Algunos puntos a favor para una empresa que aplique esta gestión de riesgos son las de reducción de costos, baja incertidumbre y se verá en aumento la probabilidad de éxito en la organización. (IBM, s.f.)

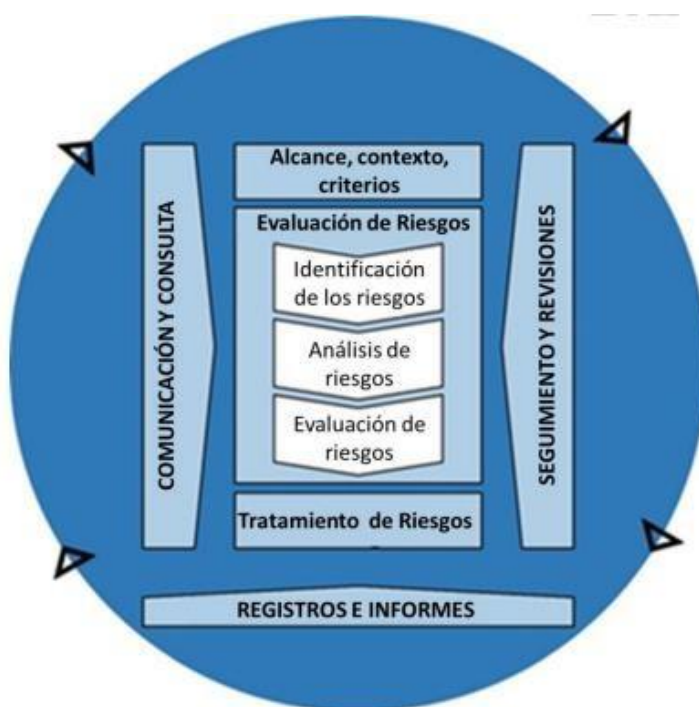
2.2.7. ISO 31000

Esta norma es fundamental cuando hablamos de Gestión de Riesgos, ya que es un estándar internacional que nos proporciona las directrices para que una institución o en una empresa se pueda contemplar el riesgo como un elemento que genere valor para la misma (Riveros, 2020).

“El proceso de aplicación de esta normativa se basa en un conjunto de directrices, procedimientos y prácticas a las actividades de notificación y consulta, estableciendo del contexto y evaluación, tratamiento, seguimiento, revisión, registros y reportes del riesgo” (Rama Judicial, 2018). Tal y como lo vemos posteriormente en la imagen.

Figura 1

Proceso ISO 31000



2.2.8. COBIT

Es un marco de trabajo que se aplica para un buen y mejor gobierno, así como, la adecuada gestión de las ti. Lo que busca esta metodología es ayudar a prosperar y evolucionar para aprovechar las oportunidades tecnológicas, trayendo consigo ventajas como:

- **Alinea la TI con los objetivos de la empresa.**

Este punto es muy importante debido a que se necesitan objetivos que estén alineados a las estrategias de la empresa. Para ello COBIT proporcionará controles y herramientas para contar con dichos objetivos, así maximizar el valor de los equipos y sistemas de TI.

- **Mejora la gestión del desempeño.**

Para tener una mejora se debe realizar una evaluación del rendimiento de todas las partes, con ello se podrá identificar lo que funciona y lo que no, con el objetivo de actuar lo más pronto posible para obtener una mejora.

- **Incrementa el valor y la confianza en los sistemas de información de la empresa.**

Los principios y prácticas que nos proporciona esta metodología nos permiten aumentar el rendimiento y productividad en el área de TI, reduciendo riesgos en los tiempos de entrega y/o en la seguridad de la información.

- **Proporciona un prototipo de código abierto.**

Esta característica nos permitirá brindar adaptabilidad y estar capacitados para todas las innovaciones que surjan en el mercado. (Conexión Esan, 2021)

Figura 2

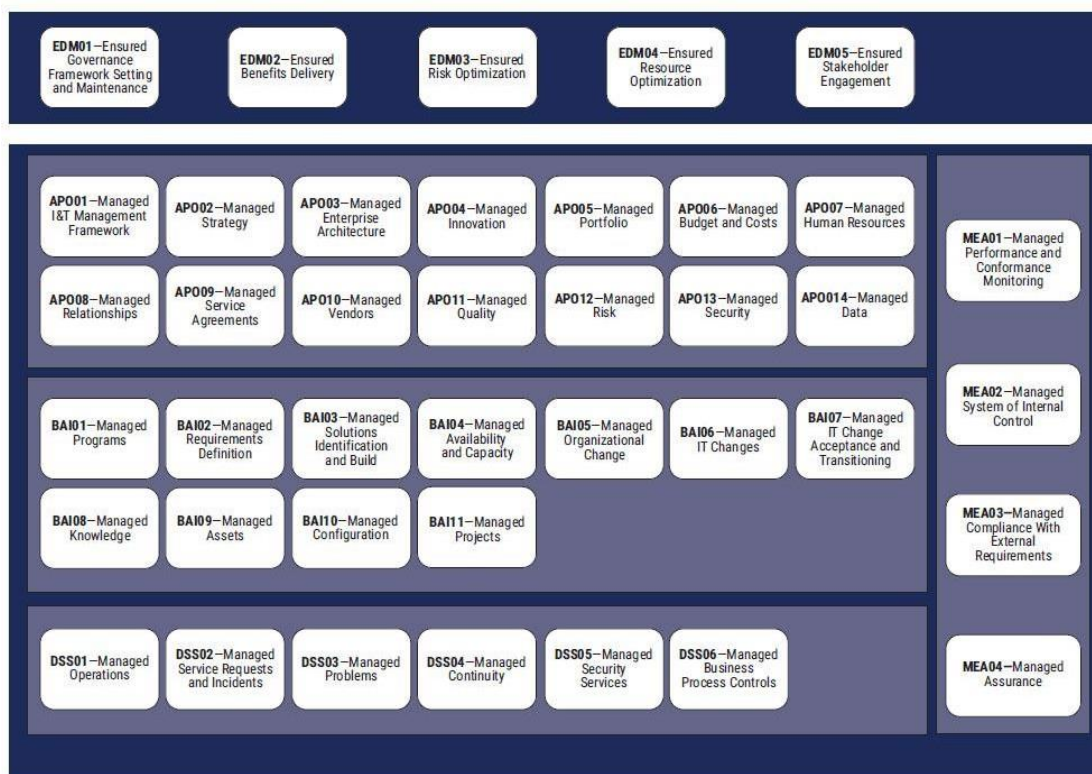
Principios de COBIT



El marco de referencia COBIT presenta los siguientes procesos de Gobierno de TI Empresarial:

Figura 3

Procesos de COBIT



2.2.9. PRINCIPIOS COBIT

El sistema COBIT se articula en torno a un conjunto de principios que permiten crear valor para la empresa a través de una gobernanza de TI sólida. Estos principios orientan tanto el diseño del sistema de gobierno como su operación cotidiana.

En COBIT 5, los seis principios rectores son:

Satisfacer las necesidades de las partes interesadas: el gobierno de TI existe para generar valor para accionistas, clientes, empleados y reguladores.

Cubrir la organización de forma integral: el marco no se limita a la función de TI; afecta a toda la empresa de extremo a extremo.

Aplicar un único marco integrado: COBIT se alinea con otras normas y marcos relevantes (ISO 27001, ITIL, PMBOK) en lugar de sustituirlos.

Habilitar un enfoque holístico: se definen siete categorías de habilitadores (principios y políticas, procesos, estructuras organizativas, cultura, información, servicios e infraestructura, personas y competencias) que deben funcionar de forma coordinada.

Separar la gobernanza de la gestión: la gobernanza evalúa, dirige y supervisa; la gestión planifica, construye, ejecuta y supervisa la operación.

2.2.10. COMPONENTES

Los componentes de COBIT incluyen:

Marco de trabajo. Organizar y categorizar los objetivos de gobernanza de TI y las buenas prácticas por dominios y procesos de TI antes de asociarlos con sus respectivos requisitos de negocio.

Descripciones de procesos. Un modelo de proceso de referencia y un lenguaje común para todos en una empresa.

Objetivos de control. Utilice este conjunto completo de requisitos de alto nivel para un control eficaz de cada proceso de TI.

Directrices de gestión. Asignar responsabilidades, acordar objetivos, medir el desempeño e ilustrar la interrelación con otros procesos.

Modelos de madurez. Evalúan la madurez y la capacidad de cada proceso y ayudan a abordar las deficiencias.

2.2.11. DOMINIOS

El modelo COBIT organiza sus procesos en cinco dominios principales, tanto en COBIT 5 como en COBIT 2019. Cada dominio agrupa los procesos relacionados con una fase del ciclo de vida de la gobernanza y la gestión de TI:

EDM (Evaluar, Dirigir y Supervisar): es el dominio de gobernanza propiamente dicho. La dirección evalúa opciones estratégicas, dirige la TI hacia los objetivos y supervisa el rendimiento y el cumplimiento.

APO (Alinear, Planificar y Organizar): abarca la estrategia, la arquitectura empresarial, la innovación, la gestión de riesgos y la gestión de recursos humanos de TI.

BAI (Construir, Adquirir e Implementar): gestiona los programas de cambio, la adquisición de soluciones y la gestión del conocimiento organizativo.

DSS (Entregar, Dar Servicio y Soporte): cubre las operaciones de TI, la gestión de servicios, la seguridad y la continuidad del negocio.

MEA (Supervisar, Evaluar y Valorar): asegura el seguimiento del rendimiento, el cumplimiento normativo y la evaluación del sistema de control interno.

En total, COBIT 2019 define 40 objetivos de gobierno y gestión distribuidos en estos cinco dominios, frente a los 37 de COBIT 5.

2.2.12. OBJETIVOS

Objetivos del marco COBIT

Intercambio de información simplificado

COBIT simplifica el proceso de compartir información entre gerentes de TI, trabajadores y partes interesadas clave. De esta manera, la administración y gobernanza de TI es más eficiente porque no se ve obstaculizada por las malas comunicaciones.

Combinación equilibrada de estrategias de TI y comerciales para lograr los objetivos

Mediante el uso de marcos de trabajo COBIT, se combinan estrategias comerciales y metodologías de TI, trabajando en conjunto en lugar de por separado. Esto limita el riesgo de que las medidas de TI entren en conflicto con los objetivos comerciales de la organización y unifica el pensamiento en torno a abordar los desafíos.

Optimización de costos

Los marcos COBIT pueden optimizar los costos al reducir la redundancia en los sistemas y el capital humano.

2.2.13. GOBIERNO

La gobernanza de TI (IT governance) engloba las estrategias, procesos y estructuras organizativas que permiten a las empresas dirigir sus sistemas de información. COBIT ocupa dentro de ese ámbito el papel de marco integrador: relaciona los objetivos de negocio con los objetivos de TI y estos, a su vez, con los procesos y controles concretos que deben existir en la organización.

2.3. GESTION COBIT

2.3.1. NIVELES

El modelo de madurez COBIT ayuda a las organizaciones a evaluar la capacidad y el rendimiento de sus procesos de TI. Proporciona una escala del 0 al 5, lo que permite a las empresas identificar deficiencias y mejorar la eficacia de la gobernanza.

Nivel 0 – Incompleto: Los procesos no se implementan o no logran alcanzar los objetivos.

Nivel 1 – Realizado: Los procesos se ejecutan, pero pueden ser inconsistentes.

Nivel 2 – Gestionado: Los procesos se planifican, supervisan y controlan.

Nivel 3 – Establecido: Se implementan procesos estandarizados en toda la organización.

Nivel 4 – Predecible: Los procesos se miden y operan dentro de límites definidos.

Nivel 5 – Optimización: La mejora continua y la innovación están integradas.

2.4. PROCESOS APO

Procesos:

APO01. Gestionar el Marco de Gestión de TI: Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.

APO02. Gestionar la Estrategia: Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos.

APO03. Gestionar la Arquitectura Empresarial: Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Define los requisitos para la taxonomía, las normas, las directrices, los procedimientos, as plantillas y las herramientas y proporcionar un vínculo para estos componentes.

APO04. Gestionar la Innovación: 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.

APO05. Gestionar el Portafolio: Ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación. Evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos, así como en su valor y riesgo corporativo. 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.

APO06 Gestionar el Presupuesto y los Costes: Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuesto, coste y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costes a la empresa.

APO07. Gestionar los Recursos Humanos: Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.

APO08. Gestionar las relaciones: Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándolas hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usando términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves.

APO09. Gestionar los acuerdos de servicio: Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la empresa, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento.

APO10. Gestionar los Proveedores: Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.

APO11. Gestionar la Calidad: Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.

APO12 Gestionar el Riesgo: Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa. Propósito del Proceso. Integrar la gestión de riesgos empresariales relacionados

APO13. Gestionar la Seguridad: Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.

2.5. PROCESOS EDM

Evaluate, Direct and Monitor

EDM01 – Asegurar el marco de gobierno

Establece y mantiene el sistema de gobierno de TI de la organización, asegurando que exista una estructura clara para tomar decisiones, asignar responsabilidades y supervisar el desempeño tecnológico, es así como, este proceso define principios, políticas, roles y mecanismos de control que permiten alinear TI con la estrategia institucional, en la práctica, ayuda a que la alta dirección tenga visibilidad sobre cómo se gobiernan los recursos tecnológicos, quién toma decisiones clave y cómo se controla el cumplimiento de los objetivos.

EDM02 – Asegurar la entrega de beneficios

Garantiza que las inversiones, proyectos y servicios de TI generen beneficios reales para la organización y contribuyan al logro de sus objetivos estratégicos, este proceso permite evaluar si las iniciativas tecnológicas entregan valor, optimizan costos, mejoran procesos o incrementan la satisfacción de los usuarios, también implica hacer seguimiento a los beneficios esperados, medir resultados y tomar decisiones cuando una inversión no está generando el impacto previsto.

EDM03 – Asegurar la optimización del riesgo

Busca que los riesgos relacionados con TI sean identificados, evaluados, priorizados y gestionados dentro de los niveles aceptables definidos por la organización, dicho proceso considera riesgos como fallas de sistemas, pérdida de información, ciberataques, indisponibilidad de servicios, incumplimientos normativos o dependencia de proveedores, es así que su finalidad es asegurar que la dirección conozca los riesgos críticos y tome decisiones oportunas para reducir su impacto en la continuidad operativa.

EDM04 – Asegurar la optimización de recursos

Asegura que los recursos tecnológicos, humanos, financieros y de información sean utilizados de manera eficiente, suficiente y sostenible, por ello permite evaluar si la organización cuenta con infraestructura, personal, presupuesto, herramientas y capacidades adecuadas para cumplir sus objetivos, además, ayuda a evitar desperdicios, duplicidad de recursos o limitaciones que puedan afectar la calidad de los servicios de TI.

EDM05 – Asegurar la participación de las partes interesadas

Promueve una comunicación efectiva entre TI, la alta dirección, usuarios, proveedores y demás partes interesadas, permite asegurar las necesidades, expectativas y preocupaciones de los stakeholders para que sean identificadas, comprendidas y consideradas en la toma de decisiones tecnológicas y facilita la transparencia mediante reportes, reuniones, indicadores y canales de comunicación que permiten fortalecer la confianza en la gestión de TI.

2.6. PROCESOS BAI

Build, Acquire and Implement (Construir, Adquirir e Implementar)

BAI01 – Gestionar programas

Administra programas estratégicos compuestos por varios proyectos relacionados, asegurando que se ejecuten de forma coordinada y entreguen los beneficios esperados contemplando la definición de objetivos, alcance, recursos, cronogramas, riesgos, responsables e indicadores de avance manteniendo el control de iniciativas complejas de TI y asegurar que cada proyecto contribuya al resultado global del programa.

BAI02 – Gestionar la definición de requisitos

Garantiza que los requisitos funcionales y no funcionales de una solución tecnológica sean identificados, analizados, documentados y validados con los usuarios y áreas involucradas, comprende qué necesita realmente la organización antes de diseñar o adquirir una solución incluyendo aspectos como funcionalidades esperadas, seguridad, rendimiento, disponibilidad, facilidad de uso, integración con otros sistemas y cumplimiento normativo.

BAI03 – Gestionar la identificación y construcción de soluciones

Permite diseñar, desarrollar, adquirir o configurar soluciones tecnológicas que respondan a las necesidades del negocio incluyendo la evaluación de alternativas, selección de herramientas, diseño técnico, construcción, pruebas y validación de la solución asegurando que la tecnología implementada sea funcional, segura, escalable y alineada con los requisitos previamente definidos.

BAI04 – Gestionar disponibilidad y capacidad

Asegura que los servicios, aplicaciones, infraestructura y recursos tecnológicos tengan la capacidad y disponibilidad necesarias para soportar las operaciones de la organización monitoreando el uso de recursos, anticipar crecimiento de demanda, planificar ampliaciones y prevenir interrupciones garantizando que los usuarios accedan a los servicios tecnológicos cuando los necesitan y con un nivel de rendimiento adecuado.

BAI05 – Gestionar la habilitación del cambio organizacional

Facilita la adopción de nuevas soluciones tecnológicas mediante acciones de comunicación, capacitación, gestión de impactos y acompañamiento a los usuarios ayudando a reducir la resistencia al cambio y mejorar la transición organizacional.

BAI06 – Gestionar cambios de TI

Controla los cambios realizados en infraestructura, aplicaciones, configuraciones y servicios de TI para reducir riesgos e interrupciones, además, establece mecanismos de solicitud, evaluación, aprobación, planificación, ejecución y revisión de cambios para asegurar que toda modificación sea analizada antes de implementarse, cuente con responsables claros y tenga planes de reversión en caso de fallas.

BAI07 – Gestionar aceptación y transición del cambio

Garantiza que las soluciones implementadas sean probadas, aceptadas y transferidas adecuadamente al entorno operativo, es así que incluye pruebas funcionales, validación con usuarios, capacitación, documentación, preparación del soporte y cierre de la transición con lo que se asegura que el cambio pueda operar de manera estable y que los usuarios cuenten con las condiciones necesarias para utilizarlo correctamente.

BAI08 – Gestionar conocimiento

Asegura que el conocimiento relacionado con TI sea capturado, organizado, compartido y reutilizado por la organización incluyendo la creación de manuales, bases de conocimiento, procedimientos, lecciones aprendidas y documentación técnica para evitar la dependencia de personas específicas, acelerar la atención de incidentes y facilitar la continuidad del servicio ante rotación de personal o cambios operativos.

BAI09 – Gestionar activos

Administra el ciclo de vida de los activos tecnológicos desde su adquisición hasta su retiro o disposición final y permite registrar, controlar y optimizar equipos, licencias, software, dispositivos, contratos y otros recursos de TI, ayuda a reducir costos, prevenir pérdidas,

asegurar el cumplimiento de licencias y conocer con precisión qué activos existen, dónde se encuentran y quién los utiliza.

BAI10 – Gestionar configuración

Mantiene información confiable y actualizada sobre los componentes tecnológicos y sus relaciones, tales como servidores, aplicaciones, redes, equipos, servicios y dependencias permitiendo conocer cómo está compuesta la infraestructura de TI y cómo un cambio o falla puede afectar otros elementos y facilita la resolución de incidentes, la planificación de cambios y el control de la arquitectura tecnológica.

BAI11 – Gestionar proyectos

Aplica prácticas de dirección, seguimiento y control de proyectos para asegurar el cumplimiento del alcance, tiempo, costo, calidad y beneficios esperados, incluye la planificación del proyecto, asignación de responsabilidades, gestión de riesgos, control de avances, comunicación con interesados y cierre formal garantizando que las iniciativas de TI se ejecuten de manera ordenada y generen resultados medibles para la organización.

2.7. PROCESOS DSS

Deliver, Service and Support (Entregar, Dar Servicio y Soporte)

DSS01 – Gestionar operaciones

Coordina y ejecuta las actividades operativas diarias de TI necesarias para brindar servicios estables, seguros y eficientes, su finalidad es asegurar que los servicios tecnológicos funcionen de manera continua y soporten adecuadamente las actividades del negocio.

DSS02 – Gestionar solicitudes de servicio e incidentes

Permite atender solicitudes de servicio de los usuarios y resolver incidentes que afectan la operación normal de TI, por ello abarca el registro, clasificación, priorización, asignación, atención, escalamiento y cierre de tickets, buscando la restauración los servicios en el menor tiempo posible, mejorar la experiencia del usuario y mantener trazabilidad sobre las atenciones realizadas.

DSS03 – Gestionar problemas

Identifica y elimina las causas raíz de incidentes recurrentes o significativos para mejorar la estabilidad de los servicios de TI analizando patrones, investigar causas, proponer soluciones definitivas y prevenir que el problema vuelva a ocurrir, es así como permite reducir interrupciones, mejorar la calidad del servicio y fortalecer la gestión preventiva.

DSS04 – Gestionar continuidad

Asegura que los servicios críticos de TI puedan mantenerse o recuperarse ante interrupciones, fallas graves, desastres o eventos imprevistos con la identificación de servicios críticos, análisis de impacto, definición de planes de continuidad, estrategias de recuperación, pruebas periódicas y actualización de procedimientos para minimizar el impacto operativo y garantizar la continuidad del negocio.

DSS05 – Gestionar servicios de seguridad

Protege la información, infraestructura, aplicaciones y servicios tecnológicos contra amenazas internas y externas, para ello incluye controles de acceso, monitoreo de seguridad, gestión de vulnerabilidades, protección contra malware, respuesta ante incidentes de seguridad y concientización de usuarios contribuyendo a preservar la confidencialidad, integridad y disponibilidad de la información institucional.

DSS06 – Gestionar controles de procesos de negocio

Implementa y supervisa controles que aseguran la integridad, confiabilidad y seguridad de los procesos de negocio soportados por TI reduciendo errores, fraudes, accesos indebidos o inconsistencias en la información utilizada por la organización.

2.8. PROCESOS MEA

Monitor, Evaluate and Assess (Monitorear, Evaluar y Valorar)

MEA01 – Monitorear, evaluar y valorar el desempeño y la conformidad

Mide el desempeño de TI y verifica que los procesos, servicios e iniciativas cumplan con los objetivos establecidos con el uso de indicadores, reportes, auditorías internas, revisiones periódicas y análisis de cumplimiento para identificar desviaciones y oportunidades de mejora para así permitir la tomar decisiones basadas en evidencia y demostrar el aporte de TI a los resultados institucionales.

MEA02 – Monitorear, evaluar y valorar el sistema de control interno

Evalúa la efectividad del sistema de control interno de TI para identificar debilidades, brechas y riesgos que puedan afectar la operación o la seguridad de la información con la ayuda de controles diseñados realmente funcionan, si se aplican de forma consistente y si requieren ajustes logrando fortalecer la gobernanza, reducir riesgos y asegurar mayor confiabilidad en los procesos tecnológicos.

MEA03 – Monitorear, evaluar y valorar el cumplimiento de requisitos externos

Verifica que la organización cumpla con leyes, regulaciones, normas, políticas externas y obligaciones contractuales relacionadas con TI, buscando la identificación de requisitos aplicables, evaluar el nivel de cumplimiento, documentar evidencias y proponer acciones correctivas cuando existan brechas logrando la reducción de riesgos legales, sanciones, incumplimientos contractuales y afectaciones reputacionales.

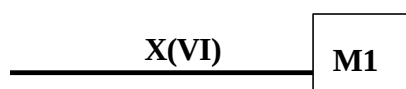
CAPITULO III

MATERIALES Y MÉTODOS

3.1. DISEÑO DE CONTRASTACIÓN DE LA HIPÓTESIS

El diseño de la investigación es no experimental de grupo único y de tipo descriptiva.

Esquema del Diseño No Experimental



Grupo único

Donde,

X: COBIT

M1: Descripción de la problemática en las aulas multimedia de la UNS después de aplicar la (VI)

3.2. POBLACIÓN

En el presente proyecto tendrá una población finita que está constituida por 22 trabajadores encargados de los equipos y/o ambientes tecnológicos de la UNS, los cuales pertenecen a la oficina de TI (9). Así como los miembros de consejo universitario (13) ya que es el órgano superior de gestión, ejecución académica y administrativa de la Universidad.

3.3. MUESTRA

La muestra fue seleccionada mediante un muestreo no probabilístico intencional, considerando como criterio principal la participación directa de los trabajadores en la administración, soporte y control de los recursos tecnológicos de las aulas multimedia de la UNS. Dicha selección se justifica en base a que los participantes poseen información técnica relevante sobre los procesos de TI, los riesgos existentes y las acciones necesarias para establecer mecanismos de control y mitigación. Por ello, el estudio no busca generalizar estadísticamente los resultados, sino realizar un diagnóstico aplicado del contexto evaluado.

La muestra con la que se desarrollará la investigación está conformada por 9 trabajadores pertenecientes a la Oficina de Tecnologías de la Información, distribuidos de la siguiente manera: Jefatura de OTIC (1), Servicios Académicos (2), UICESI (2) y UDEMSI (4).

En consecuencia, la contrastación de la hipótesis se sustenta en la coherencia entre el diagnóstico realizado, la evaluación de los procesos de TI mediante COBIT, la identificación de riesgos y la propuesta de mecanismos de control y mitigación, más que en una validación estadística inferencial.

3.4. OPERACIONALIZACIÓN DE LAS VARIABLES

Tabla 1

Operacionalización de las variables

VARIABLES	DIMENSIONES	INDICADORES	TIPO	TÉCNICA
INDEPENDIENTE (VI): Aplicación de COBIT	Gobierno y gestión de TI	- Porcentaje de procesos priorizados COBIT	Cuantitativa	Análisis documental
	Evaluación de procesos	- Nivel de capacidad de los procesos COBIT evaluados	Ordinal	Checklist COBIT
	Control interno de TI	- Porcentaje de cumplimiento de prácticas COBIT	Cuantitativa	Observación
	Brechas de gestión	- Número de brechas identificadas en procesos COBIT	Cuantitativa	Análisis de observación
DEPENDIENTE (VD): Gestión de Riesgos de TI en las aulas multimedia	Identificación de Riesgos	- Número y porcentaje de riesgos identificados	Cuantitativa	Observación
	Análisis y Evaluación de Riesgos	- Nivel de impacto de riesgos identificados	Cuantitativa	Matriz de riesgos
	Tratamiento de Riesgos	- Número de riesgos con acciones de tratamiento definidas	Cualitativa	Matriz de tratamiento
	Monitoreo y Revisión	- Número de controles propuestos con responsable	Cuantitativa	Análisis documental

Fuente: Elaboración propia

3.5. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

3.5.1. TÉCNICAS

- **Observación:** Para recolectar información de manera directa sobre el funcionamiento y las deficiencias de las aulas multimedia.
- **Checklist:** A fin de tener una lista con las deficiencias de las aulas multimedia

3.5.2. INSTRUMENTOS

- **Inventarios:** Con la finalidad de saber lo que se tiene, ver el estado de estos mismos y concluir con lo que se necesita.

3.5.3. VALIDEZ Y CONFIABILIDAD DE LOS INSTRUMENTOS

La validez de los instrumentos se sustenta en su alineación con las variables, dimensiones e indicadores definidos en la operacionalización del estudio. Asimismo, los instrumentos fueron elaborados considerando los procesos priorizados de COBIT y las etapas de gestión de riesgos establecidas por ISO 31000, con el propósito de asegurar coherencia entre el objetivo de la investigación, la recolección de datos y el análisis de resultados.

Los instrumentos utilizados, como la de observación, el checklist, el inventario y las matrices de análisis, responden a criterios técnicos verificables relacionados con la gestión de riesgos de TI en las aulas multimedia. Entre dichos criterios se consideran el estado de los equipos, existencia de controles, evidencias documentales, cumplimiento de prácticas COBIT, probabilidad, impacto, nivel de exposición al riesgo y acciones de tratamiento propuestas.

La confiabilidad se garantiza mediante la aplicación uniforme de los instrumentos bajo los mismos criterios de evaluación en el entorno analizado. Para ello, se establecieron parámetros comunes de registro, valoración y análisis, permitiendo mantener consistencia en la información recolectada y trazabilidad entre los riesgos identificados, los procesos COBIT asociados, los controles existentes y las acciones de mitigación planteadas.

3.5.4. METODOLOGÍA PARA EL DESARROLLO DEL ESTUDIO

- **IDENTIFICACIÓN DEL PROBLEMA**

Se realizó un análisis previo de los procesos institucionales y de TI dentro de la institución. Se pudo identificar necesidades de mejora en los flujos de seguridad y gestión de riesgos de la oficina de informática, mediante observación directa y entrevista con el personal comprometido en OTIC.

Para este caso, hallamos limitaciones tales como, la falta de procesos y estrategias para gestionar los riesgos, sin hacer nada al respecto, como prevenirlos o mitigarlos. Además, de la falta de infraestructura, equipos y dispositivos en correcto estado para asegurar su integridad. Todo ello afecta directamente a la integridad de la información de los estudiantes, y a la calidad educativa.

- **DEFINICIÓN DE LOS OBJETIVOS**

En base a la problemática y las limitaciones, establecimos un objetivo general, del cual se despliegan los específicos, los cuales están guiados a una implementación de la metodología en mención enfocada en gestionar los riesgos.

- **REVISIÓN DE LA LITERATURA**

Se realizaron revisiones a investigaciones de tipo local, nacional e internacional que estén basadas o haciendo uso de la metodología COBIT, en diferentes ámbitos, tales como la Gestión de Riesgos. Así, tener en cuenta el proceso de implementación y los hallazgos en base a esta experiencia de mejora en la organización.

- **DISEÑO DEL ESTUDIO**

Se hizo uso de un diseño no experimental descriptivo, para validar los riesgos a los que está expuesta la institución.

- **RECOLECCIÓN DE DATOS**

Consideramos una muestra compuesta por 9 trabajadores de la institución encargados del área responsable.

- **DESARROLLO**

La metodología se desarrolló en fases secuenciales y relacionadas entre sí, con el propósito de pasar de un diagnóstico inicial hacia una propuesta de control y mitigación de riesgos. Estas fases permiten que COBIT sea utilizado como un marco para orientar decisiones de gobierno y gestión de TI.

- **Establecimiento del contexto institucional y tecnológico**

Se identificó el contexto de las aulas multimedia, los recursos tecnológicos disponibles, los actores involucrados, las condiciones operativas y las principales limitaciones que afectan la continuidad, seguridad y disponibilidad del servicio educativo.

- **Alineamiento de objetivos institucionales, objetivos de TI y procesos COBIT**

Se realizó el alineamiento entre los objetivos institucionales, los objetivos relacionados con TI y los procesos de COBIT vinculados con la optimización del riesgo, la gestión de recursos, la seguridad de la

información, la continuidad del servicio y el monitoreo de controles. Esta fase permite estructurar un mapping entre las necesidades de la institución, los objetivos de TI y los procesos priorizados.

- **Priorización de procesos de gobierno y gestión de TI**

A partir del alineamiento realizado, se seleccionaron los procesos COBIT más relevantes para el estudio, considerando su relación con la gestión de riesgos de TI en las aulas multimedia. Se priorizaron procesos asociados a la optimización del riesgo, gestión de recursos, seguridad, continuidad, atención de incidentes, control interno y monitoreo.

- **Evaluación de capacidad y brechas de control**

Se evaluó el nivel de capacidad de los procesos seleccionados, identificando brechas entre el estado actual y las prácticas esperadas de gobierno y gestión de TI. Esta evaluación permite determinar si existen políticas, responsables, controles, evidencias, indicadores y mecanismos de supervisión suficientes para gestionar los riesgos identificados.

- **Gestión formal de riesgos según ISO 31000**

La gestión de riesgos se estructuró siguiendo las etapas de ISO 31000: establecimiento del contexto, identificación de riesgos, análisis de probabilidad e impacto, evaluación de los niveles de exposición, tratamiento del riesgo, monitoreo y comunicación.

- **Definición de criterios de aceptabilidad y tolerancia al riesgo**

Se definieron criterios para clasificar los riesgos según su nivel de exposición: permitido, admisible, limitado, relevante e inadmisible. La tolerancia al riesgo se entiende como el nivel máximo de exposición que puede aceptarse sin comprometer la continuidad del servicio educativo, la seguridad de los usuarios, la disponibilidad de los recursos tecnológicos o la integridad de la información.

- **Tratamiento, control y mitigación de riesgos**

Para cada riesgo evaluado se plantearon respuestas orientadas a evitar, reducir, transferir o aceptar el riesgo, según su nivel de exposición y su impacto sobre los objetivos institucionales. Asimismo, se definieron

mecanismos de control y mitigación vinculados con los procesos COBIT priorizados.

- **Monitoreo, revisión y mejora continua**

Finalmente, se consideró el seguimiento de los riesgos, controles e indicadores asociados, con el fin de revisar periódicamente la efectividad de las acciones propuestas y promover la mejora continua de la gestión de TI en las aulas multimedia.

- **ANÁLISIS DE DATOS**

Esta información se analizó con herramientas y cuadros propuestos por la metodología COBIT, con el objetivo de evaluar el impacto de los riesgos identificados con sus indicadores definidos.

- **INTERPRETACIÓN Y DISCUSIÓN DE RESULTADOS**

Se interpretaron los datos obtenidos para identificar las amenazas y áreas críticas que prevalecen. Se realizó una contrastación de los resultados con los objetivos planteados y con el marco teórico revisado.

- **CONCLUSIONES Y RECOMENDACIONES**

Las conclusiones fueron formuladas en base al análisis previo y a las observaciones. Las recomendaciones se plantearon en base a los objetivos formulados.

- **REDACCIÓN DEL INFORME FINAL**

El informe final de tesis fue estructurado según las normas académicas de la Universidad Nacional del Santa, incluyendo las secciones con respecto a las metodológicas detalladas, anexos y bibliografía actualizada.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1. APLICACION DEL MARCO COBIT E ISO 31000

Este capítulo presenta los resultados de la aplicación integrada de COBIT e ISO 31000 para la gestión de riesgos de TI en las aulas multimedia de la Universidad Nacional del Santa. El estudio se centra en un diagnóstico técnico-aplicado, la evaluación de procesos de gobierno y gestión de TI. Es así como los resultados evidencian la trazabilidad entre contexto tecnológico, procesos COBIT priorizados, riesgos identificados, niveles de exposición y acciones de control o mitigación.

4.1.1. DIAGNOSTICO DEL CONTEXTO TECNOLÓGICO DE LAS AULAS MULTIMEDIA

El diagnóstico del contexto tecnológico constituye la primera etapa del proceso de gestión de riesgos, ya que permite delimitar el entorno donde se identifican y evalúan los riesgos. En el caso de la Universidad Nacional del Santa, el estudio se centra en las aulas multimedia, los equipos tecnológicos, los sistemas, la conectividad, las condiciones físicas de infraestructura y los procesos de soporte asociados a la continuidad del servicio educativo.

Se identifican como elementos críticos los equipos de cómputo, proyectores, equipos de sonido, puntos de red, tomacorrientes, software instalado, controles de acceso físico, mantenimiento preventivo, licencias, antivirus y mecanismos de respaldo ante interrupciones del servicio. Estos elementos son relevantes porque soportan directamente las actividades académicas y, en caso de fallas, pueden afectar la disponibilidad del servicio, la seguridad de los usuarios y la integridad de la información.

Los actores involucrados corresponden principalmente al personal de la Oficina de Tecnologías de la Información, quienes participan en la administración, soporte, mantenimiento y control de los recursos tecnológicos. La información proporcionada por estos responsables permite sustentar el diagnóstico aplicado y orientar la propuesta de mecanismos de control y mitigación.

4.1.2. ALINEAMIENTO COBIT: OBJETIVOS INSTITUCIONALES, OBJETIVOS DE TI Y PROCESOS PRIORIZADOS

La metodología COBIT nos proporciona 17 metas corporativas que se encuentran alineados a la empresa, los cuales se van a ajustar a la Universidad Nacional del

Santa, se realizará una ponderación dividiendo los objetivos en Primarios (P) y Secundarios (S) con la siguiente escala:

Tabla 2

Ponderación de Objetivos Empresariales según COBIT

Valoración	
3	Alta
2	Media
1	Baja

Fuente. Elaboración propia

Tabla 3

Valoración realizada en la UNS para los objetivos corporativos

Dimensiones	Objetivos Corporativos	Relación con los ideales del Gobierno			Ponderación
		Realización de Beneficios	Optimización de Riesgos	Optimización de Recursos	
Financiera	1.- Generación de retorno para las partes interesadas de las asignaciones de recursos de Negocios	S			1
	2.- Portafolio de servicios de enseñanza competitivos			S	1
	3.- Exposición de negocio controlados		P		3
	4.- Acato de leyes y normativas externas		P		3
	5.- Integridad financiera			P	3
Cliente	6.- Filosofía de servicio enfocada en el alumnado	S			1
	7.- Persistencia y accesibilidad del servicio de enseñanza		P	S	2
	8.- Acciones ágiles a un entorno de servicio variable		S		1
	9.- Elección estratégica de decisiones basada en los datos		P	S	2
	10.- Maximización de costos de entrega de los servicios		S		1
Interna	11.- Mejora de la funcionalidad de los procesos de negocio		P		3

	12.- Eficacia de los costos de los procesos de los servicios	S			1
	13.- Planes administrados de cambio en el servicio educativo	S	S		2
	14.- Rendimiento operativo, de la plana docente y administrativa		P		3
	15.- Acatamiento de las normativas internas		P		3
Aprendizaje y Crecimiento	16.- Plana docente capacitada e impulsada			S	1
	17.- Tradición de innovación de servicios de enseñanza			S	1

Fuente. Elaboración propia

Tabla 4

Resultados de objetivos de la empresa con mayor ponderación

Dimensiones	Objetivos Corporativos	Relación con los objetivos del Gobierno			Ponderación
		Realización de Beneficios	Optimización de Riesgos	Optimización de Recursos	
Financiera	3.- Exposición de negocio controlados		P		3
	4.- Acato de leyes y normativas externas		P		3
	5.- Integridad financiera			P	3
Interna	11.- Mejora de la funcionalidad de los procesos de negocio		P		3
	14.- Rendimiento operativo, de la plana docente y administrativa		P		3
	15.- Acatamiento de las normativas internas		P		3

Fuente. Elaboración propia

Realizamos la ponderación teniendo como referencia las metas institucionales, lo que se obtuvo en los hallazgos son 6 metas con mayor evaluación, con importancia Alta según la escala establecida. Posterior a la ponderación de los objetivos de la institución, se realizó el contraste de los alcances de la institución con las finalidades de TI, de la siguiente manera:

Tabla 5

Cruce de los alcances de la institución seleccionados con las finalidades TI

			Meta Corporativa						Ponderación
			3.- Exposición de negocio controlados	4.- Acato de leyes y normativas externas	5.- Integridad financiera	11.- Mejora de la funcionalidad de los procesos de negocio	14.- Rendimiento operativo, de la plana docente y administrativa	15.- Acatamiento de las normativas internas	
Meta Relacionada con las TI			Financiera		Interna				
Financiera	1	Integración de TI y la estrategia de la institución	P			S			2
	2	Acato de leyes y normativas externas	S	P			S	P	2
	3	Responsabilidad de los administrativos para tomar decisiones relacionadas con TI				P	S	S	2
	4	Vulnerabilidades de la institución en relación con las TI	P			P	S	P	3
	5	Desarrollo de los aportes de servicios relacionados con la TI		S		S			1
	6	Integridad de los costos, rentabilidad y amenazas de las TI	P						2
Cliente	7	Provisión de servicio de TI de acuerdo a los requerimientos de la institución	S			S	S	P	2
	8	Incorporación adecuada de aplicaciones, data y mejoras informáticas	P	P		S	P	P	3
Interna	9	Adaptabilidad de las TI	P			P	S	P	3
	10	Resguardo de la información, infraestructura de procesamiento y aplicativos	P	S					3
	11	Maximización de activos, recursos y competencias de las TI				S	S	P	2

Aprendizaje y Crecimiento	12	Formación y soporte de procesos de la institución unificando aplicativos y tecnología en procesos de la institución	S		S	P	P		2
	13	Suministro de planes que faciliten beneficios de forma oportuna			S				1
	14	Accesibilidad de información útil y significativa para la toma de decisiones			S	S	P	P	3
	15	Realización de las normativas internas por parte de las TI	S		P		P		3
	16	Recurso humano de la institución y de las TI capacitado e impulsado	P		P	S	P	P	3
	17	Percepción, trayectoria y acciones estratégicas para la institución			S	P	P		3

Tabla 6

Resultados de los objetivos de la institución seleccionados con los objetivos TI

Meta Corporativa									
				3.- Exposición de negocio controlados	4.- Acato de leyes y normativas externas	5.- Integridad financiera	11.- Mejora de la funcionalidad de los procesos de negocio	14.- Rendimiento operativo, de la planta docente y administrativa	15.- Acatamiento de las normativas internas
Meta Relacionada con las TI				Financiera			Interna		
Categoría	Objetivo	Descripción	Impacto						
									Ponderación
Financiera	4	Vulnerabilidades de la institución en relación con las TI	P		P	S		P	3
Cliente	8	Incorporación adecuada de aplicaciones, data y mejoras informáticas	P		P	S	P		3
Interna	9	Adaptabilidad de las TI	P		P		S		3
	10	Resguardo de la información, infraestructura de procesamiento y aplicativos	P					P	3
	14	Accesibilidad de información útil y significativa para la toma de decisiones			S	S	P	P	3
	15	Realización de las normativas internas por parte de las TI	S		P		P		3

Aprendizaje y	16	Recurso humano de la institución y de las TI capacitado e impulsado	P	P	S	P	P	3
	17	Percepción, trayectoria y acciones estratégicas para la institución		S	P	P		3

En la Tabla 32 se realizó la correlación de los alcances de la Empresa con los objetivos de TI; de los 17 objetivos empresariales sólo obtuvieron ponderación alta 6 objetivos, lo cual representa el 35.30% del total.

Posteriormente en la Tabla 27 podemos apreciar que de los 17 objetivos de TI sólo obtuvieron ponderación alta 8 objetivos de TI, lo cual se traduce en el 47.06%.

El propósito de la selección de los ideales de la empresa y las relacionadas con las TI es para mostrar la gran relevancia que tienen las ti para la toma de decisiones y conformidad de los ideales de la UNS.

SELECCIÓN DE PROCESOS FACILITADORES Y PRÁCTICAS DE GOBIERNO

Para la realización de la auditoría en la Oficina de Tecnología e Información de la UNS se seleccionó los procesos facilitadores según COBIT, del Prototipo de Referencia de Procesos de C.

Para evaluar los procesos que se ajustan a la Universidad Nacional del Santa realizaremos una ponderación donde los objetivos de dividirá en:

P = Primarios S = Secundarios,

Es así que se determina la ponderación en escala:

Tabla 7

Ponderación de Objetivos Empresariales según COBIT

Valoración	
3	Alta
2	Media
1	Baja

Fuente. Elaboración propia

Tabla 9

Valoración de Procesos Facilitadores

			Meta Corporativa							Ponderación
			3.- Exposición de	4.- Acato de leyes y	5.- Integridad	11.- Mejora de la	14.- Rendimiento	15.- Acatamiento		
Meta Relacionada con las TI			Financiera			Interna				
Evaluar, Orientar y Supervisar	EDM01	Mantenimiento del Marco de Gobierno	S				S		2	
	EDM02	Asegurar la Entrega de Beneficios	S	S					2	
	EDM03	Asegurar la Optimización del Riesgo	P	S		P	P	S	3	
	EDM04	Asegurar la Optimización de los Recursos	P		S	P	P		3	
	EDM05	Asegurar la Transparencia hacia las partes interesadas		S	S	S		S	2	
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI	P	S			P	S	3	
	APO02	Gestionar la Estrategia			S	S			2	
	APO03	Gestionar la Arquitectura Empresarial				S	S	S	2	
	APO04	Gestionar la Innovación			P			S	2	
	APO05	Gestionar el portafolio	S	S			S		2	
	APO06	Gestionar el Presupuesto y los Costes			P	S			2	
	APO07	Gestionar los Recursos Humanos					S		1	
	APO08	Gestionar las Relaciones					S		1	
	APO09	Gestionar los Acuerdos de Servicio	S	S	S	S			2	
	APO10	Gestionar los Proveedores			P		S	S	2	
	APO11	Gestionar la Calidad		P				S	2	
	APO12	Gestionar el Riesgo	P	S		P	P	S	3	
	APO13	Gestionar la Seguridad	P				P	S	3	
Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos	P		P	S	P		3	
	BAI02	Gestionar la Definición de Requisitos		P					2	
	BAI03	Gestionar la Identificación y la Construcción de Soluciones	S			S			2	
	BAI04	Gestionar la Disponibilidad y la Capacidad			S	S			2	
	BAI05	Gestionar la introducción de Cambios Organizativos				S	S		2	
	BAI06	Gestionar los Cambios	S	S	S				2	
	BAI07	Gestionar la Aceptación del Cambio y de la Transición			S				2	
	BAI08	Gestionar el Conocimiento					S		1	
	BAI09	Gestionar los Activos	P	S			P		3	
	BAI10	Gestionar la Configuración	P			P	P		3	
Entregar, dar Servicio y Soporte	DSS01	Gestionar las Operaciones		S				S	2	
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio	P			P	P		3	
	DSS03	Gestionar los Problemas	P			P	P	S	3	
	DSS04	Gestionar la Continuidad	P			S	P		3	
	DSS05	Gestionar los Servicios de Seguridad	P	S			P		3	
	DSS06	Gestionar los Controles de los Procesos del Negocio				S			1	
Supervisión, Evaluación y Seguimiento	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S				S		2	
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno	P		P		P	P	3	
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos		P				S	2	

Fuente. Elaboración propia

Tabla 10

Resultados de Ponderación de Procesos Facilitadores

			Meta Corporativa						
									
			3.- Exención de 4.- Acato de leyes y 5.- Integridad 11.- Mejora de la 14.- Rendimiento 15.- Acatamiento de Ponderación						
			Meta Relacionada con las TI						
			Financiera Interna						
Ori enta s y	EDM03	Asegurar la Optimización del Riesgo	P	S		P	P	S	3
	EDM04	Asegurar la Optimización de los Recursos	P		S	P	P		3
Aline ar, i	PO01	Gestionar el Marco de Gestión de TI	P	S			P	S	3
	PO12	Gestionar el Riesgo	P	S		P	P	S	3
	PO13	Gestionar la Seguridad	P				P	S	3
Const rucció n	BAI01	Gestionar los Programas y Proyectos	P		P	S	P		3
	BAI09	Gestionar los Activos	P	S			P		3
	BAI10	Gestionar la Configuración	P			P	P		3
Entregar, dar Servicio y Soporte	DSS02	Gestionar las Peticiones y los Incidentes del Servicio	P			P	P		3
	DSS03	Gestionar los Problemas	P			P	P	S	3
	DSS04	Gestionar la Continuidad	P			S	P		3
	DSS05	Gestionar los Servicios de Seguridad	P	S			P		3
Sa pa re si	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno	P		P		P	P	3

Fuente. Elaboración propia

Después de realizar la ponderación de los Procesos Facilitadores se seleccionaron 13 procesos relacionados con la Gestión de Riesgos de TI y la empresa, la cual corresponde a la Universidad Nacional del Santa. De cada proceso se seleccionaron las prácticas de Gobierno a ser aplicadas en la auditoría.

4.1.3. EVALUACIÓN DE CAPACIDAD Y BRECHAS DE GOBIERNO DE TI

Anteriormente se realizó la selección de los procesos y prácticas de gobierno, es así que, llega el momento de realizar el desarrollo de cada uno de los procesos y analizar en qué medida se está dando cumplimiento a las prácticas de Gobierno.

Tabla 11

EDM03

Subproceso	Documentos COBIT	Dispone
EDM03.01 Evaluar la gestión del riesgo	• Perfil de riesgo empresarial • Apetito y tolerancia al riesgo • Reporte de evaluación de riesgos	NO
EDM03.02 Orientar la gestión del riesgo	• Principios de gestión del riesgo • Directrices de respuesta al riesgo	NO
EDM03.03 Supervisar la gestión del riesgo	• Reportes de riesgo consolidados • Indicadores clave de riesgo (KRI)	NO

Fuente. Elaboración propia

Tabla 12

EDM04

Subproceso	Documentos COBIT	Dispone
EDM04.01 Evaluar la gestión de recursos	• Evaluación de capacidad de recursos • Reporte de utilización de recursos TI	SI
EDM04.02 Orientar la gestión de recursos	• Principios de asignación de recursos • Directrices de optimización	SI
EDM04.03 Supervisar la gestión de recursos	• Reportes de desempeño de recursos • Indicadores de eficiencia	NO

Fuente. Elaboración propia

Tabla 13

APO01

Subproceso	Documentos COBIT	Dispone
APO01.01 Definir el marco de gestión	• Marco de gobierno y gestión de TI	NO
APO01.02 Establecer roles y responsabilidades	• Principios de gobierno TI • Estructura organizacional de TI • Matriz RACI	SI
APO01.03 Mantener el marco de gestión	• Procedimiento de revisión del marco	NO
APO01.04 Mejorar continuamente	• Evaluaciones de desempeño del marco • Plan de mejora continua	NO

Fuente. Elaboración propia

Tabla 14

APO12

Subproceso	Documentos COBIT	Dispone
APO12.01 Recopilar datos de riesgo	• Registro de eventos de riesgo • Catálogo de riesgos TI	NO
APO12.02 Analizar riesgos	• Evaluación de impacto y probabilidad • Matriz de riesgos	NO
APO12.03 Mantener perfil de riesgo	• Perfil de riesgo TI • Mapa de riesgos	NO
APO12.04 Articular el riesgo	• Reportes de riesgo integrados	NO
APO12.05 Responder al riesgo	• Plan de respuesta al riesgo • Acciones de mitigación	NO

Fuente. Elaboración propia

Tabla 15

APO13

Subproceso	Documentos COBIT	Dispone
APO13.01 Establecer SGSI	• Política de seguridad de la información • Alcance del SGSI	SI
APO13.02 Gestionar la seguridad	• Normas y procedimientos de seguridad	SI
APO13.03 Monitorear la seguridad	• Reportes de incidentes de seguridad • Métricas de seguridad	NO

Fuente. Elaboración propia

Tabla 16

BAI01

Subproceso	Documentos 8	Dispone
BAI01.01 Enfoque estándar	• Metodología de gestión de proyectos	NO
BAI01.02 Iniciar programas	• Caso de negocio • Acta de inicio	SI
BAI01.03 Gestionar interesados	• Registro de interesados • Plan de comunicaciones	NO
BAI01.04 Planificar	• Plan del proyecto • Cronograma	NO
BAI01.05 Ejecutar	• Informes de avance	NO
BAI01.06 Monitorear	• Indicadores de desempeño	NO
BAI01.07 Cerrar	• Informe de cierre • Lecciones aprendidas	SI

Fuente. Elaboración propia

Tabla 17*BAI09*

Subproceso	Documentos COBIT	Dispone
BAI09.01 Identificar activos	• Inventario de activos TI	SI
BAI09.02 Gestionar activos	• Registros de control de activos	SI
BAI09.03 Ciclo de vida	• Procedimientos de alta y baja	NO

Fuente. Elaboración propia

Tabla 18*BAI10*

Subproceso	Documentos COBIT	Dispone
BAI10.01 Establecer configuración	• Base de datos de configuración (CMDB)	SI
BAI10.02 Mantener configuración	• Registros de configuración	NO
BAI10.03 Controlar cambios	• Solicitudes y registros de cambios	NO

Fuente. Elaboración propia

Tabla 19*DSS02*

Subproceso	Documentos COBIT	Dispone
DSS02.01 Clasificar solicitudes	• Catálogo de servicios	NO
DSS02.02 Registrar incidentes	• Registro de incidentes	NO
DSS02.03 Resolver incidentes	• Reportes de resolución	NO
DSS02.04 Monitorear atención	• Indicadores de nivel de servicio	NO

Fuente. Elaboración propia

Tabla 20*DSS03*

Subproceso	Documentos COBIT	Dispone
DSS03.01 Identificar problemas	• Registro de problemas	NO
DSS03.02 Diagnosticar	• Análisis de causa raíz	NO
DSS03.03 Resolver	• Acciones correctivas	NO
DSS03.04 Cerrar	• Informe de cierre	NO

Fuente. Elaboración propia

Tabla 21*DSS04*

Subproceso	Documentos COBIT	Dispone
DSS04.01 Definir política	• Política de continuidad de TI	NO
DSS04.02 Mantener planes	• Plan de continuidad de TI	NO
DSS04.03 Probar planes	• Resultados de pruebas	NO
DSS04.04 Gestionar incidentes	• Reportes de continuidad	NO

Fuente. Elaboración propia

Tabla 22*DSS05*

Subproceso	Documentos COBIT	Dispone
DSS05.01 Protección	• Controles de seguridad definidos	NO
DSS05.02 Accesos	• Registros de control de acceso	NO
DSS05.03 Identidades	• Registros de identidades	NO
DSS05.04 Red	• Controles de seguridad de red	SI
DSS05.05 Eventos	• Registros de eventos de seguridad	NO
DSS05.06 Incidentes	• Registro de incidentes de seguridad	NO

Fuente. Elaboración propia

Tabla 23*MEA02*

Subproceso	Documentos COBIT	Dispone
MEA02.01 Supervisar controles	• Matriz de controles internos	NO
MEA02.02 Evaluar controles	• Informes de auditoría interna	NO
MEA02.03 Tratar deficiencias	• Planes de acción correctiva	NO

Fuente. Elaboración propia

4.1.3.1. Evaluación de Niveles de Capacidad

Con respecto al análisis de los niveles de capacidad se observan los procesos seleccionados, los cuales cuentan con documentación, para lo cual se mostrarán los resultados a través de gráficos de radar, así se apreciará el avance del proceso.

Tabla 24*EDM03*

Atributos de Capacidad del Proceso										
Proceso	Práctica de Gobierno	Modelado del Proceso	Ejecución de Proceso	Gestión de Proceso	Monitoreo de Procesos	Eficiencia del Proceso	Gestión del Rendimiento	Gestión de los Resultados	Mejora de Proceso	Optimización de Procesos
EDM03	EDM03.01	0	0	0	0	0	0	0	0	0
	EDM03.02	0	0	0	0	0	0	0	0	0
	EDM03.03	0	0	0	0	0	0	0	0	0

Figura 4

Radar de atributos de capacidad EDM03

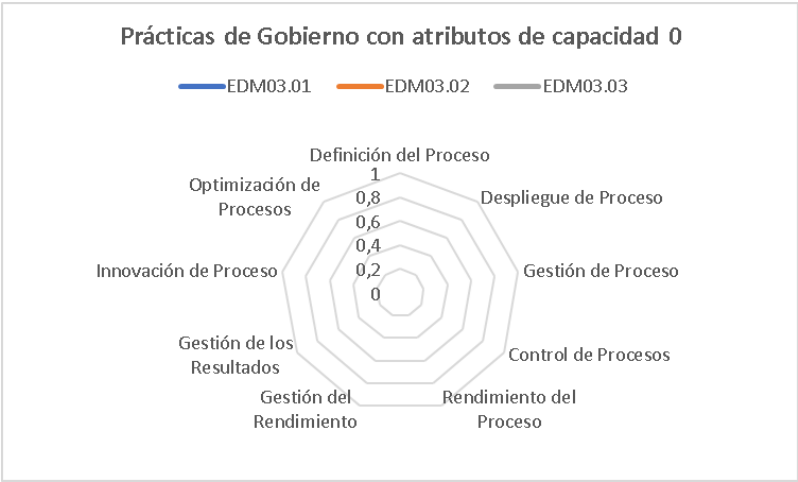


Tabla 25

Valoración de nivel de capacidad EDM03

Descripción	Valor
Valor Óptima	27
Valor Obtenido	0
% alcanzado	0.00
Escala	N

Tabla 26

EDM04

Atributos de Capacidad del Proceso										
Proceso	Práctica de Gobierno	Modelado del Proceso	Ejecución de Proceso	Gestión de Proceso	Monitoreo de Procesos	Eficiencia del Proceso	Gestión del Rendimiento	Gestión de los Resultados	Mejora de Proceso	Optimización de Procesos
EDM04	EDM04.01	1	1	1	1	1	1	1	1	1
	EDM04.02	1	1	1	1	1	1	1	1	1
	EDM04.03	0	0	0	0	0	0	0	0	0

Figura 5

Radar de atributos de capacidad EDM04.01

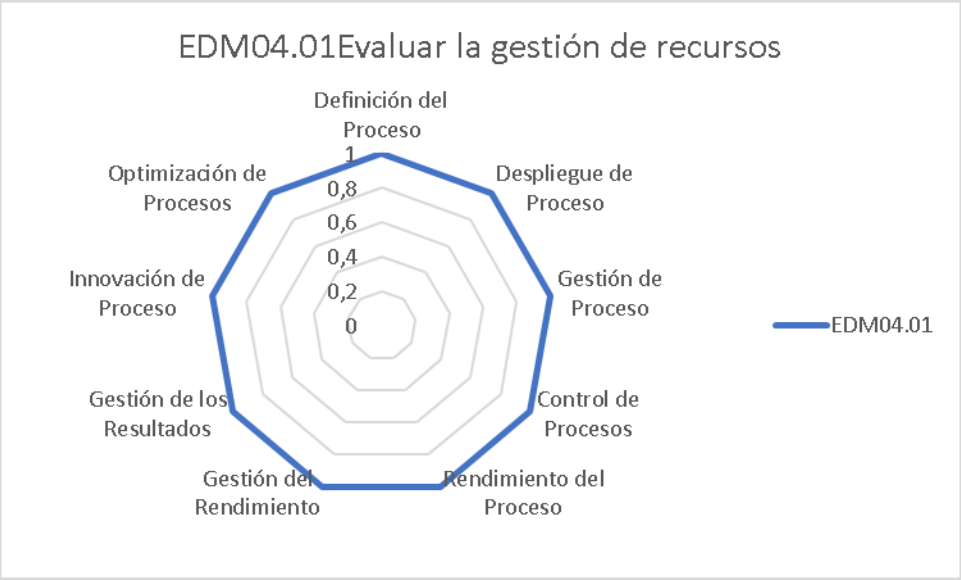


Figura 6

Radar de atributos de capacidad EDM04.02

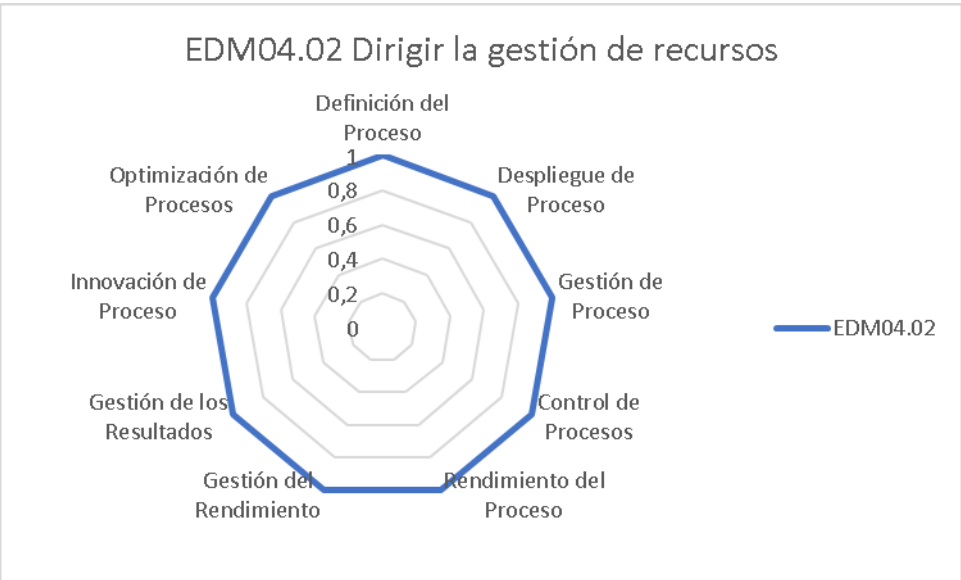


Figura 7

Radar de atributos de capacidad EDM04.03

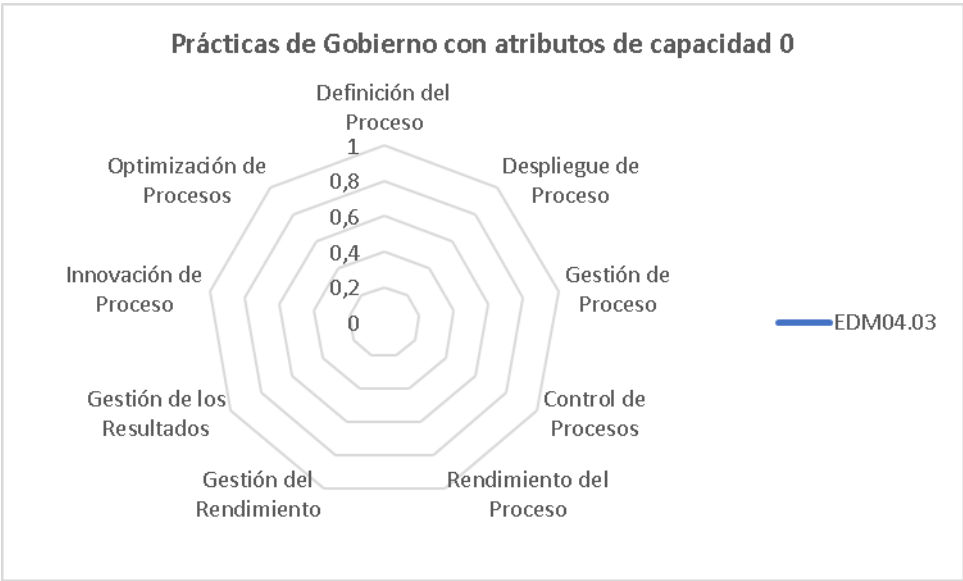


Tabla 27

Valoración de nivel de capacidad EDM04

Descripción	Valor
Valor Óptima	27
Valor Obtenido	18
% alcanzado	66.67%
Esacala	P

Tabla 28

APO01

Atributos de Capacidad del Proceso										
Proceso	Práctica de Gobierno	Modelado del Proceso	Ejecución de Proceso	Gestión de Proceso	Monitoreo de Procesos	Eficiencia del Proceso	Gestión del Rendimiento	Gestión de los Resultados	Mejora de Proceso	Optimización de Procesos
APO01	APO01.01	0	0	0	0	0	0	0	0	0
	APO01.02	1	1	1	1	1	1	1	1	1
	APO01.03	0	0	0	0	0	0	0	0	0
	APO01.04	0	0	0	0	0	0	0	0	0

Figura 8

Radar de atributos de capacidad APO01.02



Figura 9

Radar de atributos de capacidad APO01

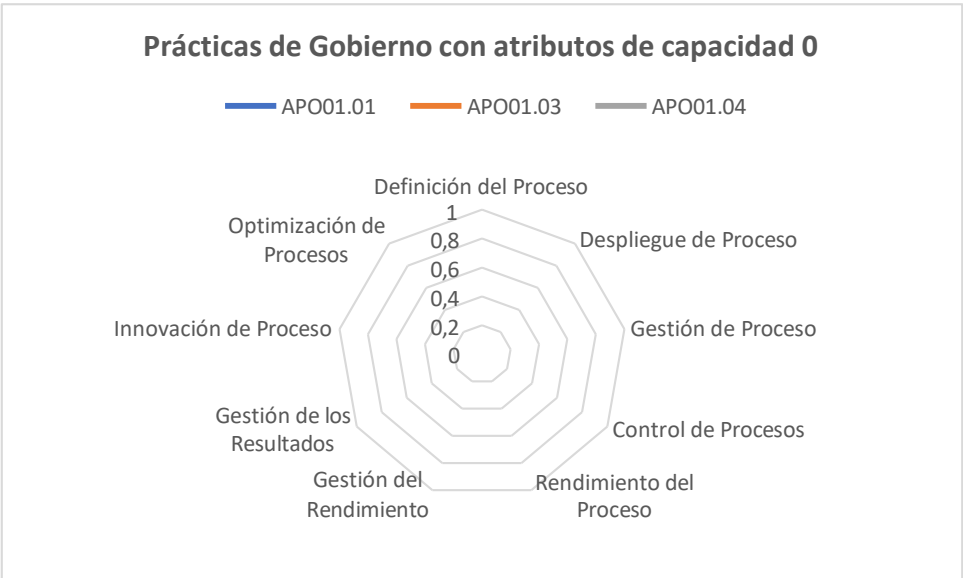


Tabla 29

Valoración de nivel de capacidad APO01

Descripción	Valor
Valor Óptima	36
Valor Obtenido	9
% alcanzado	25%
Escala	P

Tabla 30

APO12

Atributos de Capacidad del Proceso										
Proceso	Práctica de Gobierno	Modelado del Proceso	Ejecución de Proceso	Gestión de Proceso	Monitoreo de Procesos	Eficiencia del Proceso	Gestión del Rendimiento	Gestión de los Resultados	Mejora de Proceso	Optimización de Procesos
APO12	APO12.01	0	0	0	0	0	0	0	0	0
	APO12.02	0	0	0	0	0	0	0	0	0
	APO12.03	0	0	0	0	0	0	0	0	0
	APO12.04	0	0	0	0	0	0	0	0	0
	APO12.05	0	0	0	0	0	0	0	0	0

Figura 10

Radar de atributos de capacidad APO12

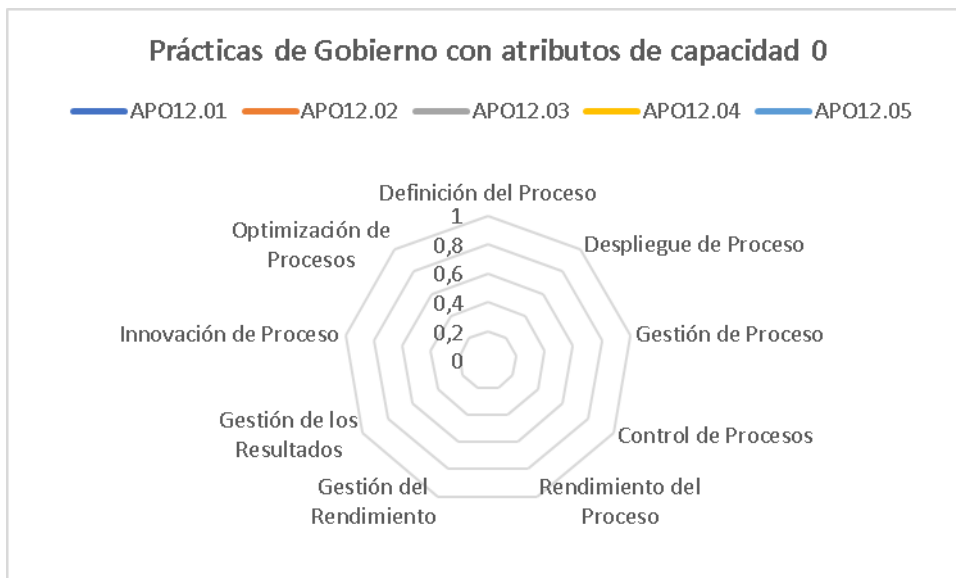


Tabla 31

Valoración de nivel de capacidad APO12

Descripción	Valor
Valor Óptima	45
Valor Obtenido	0
% alcanzado	0.00

Escala	N
--------	---

Tabla 32

APO13

Atributos de Capacidad del Proceso										
Proceso	Práctica de Gobierno	Modelado del Proceso	Ejecución de Proceso	Gestión de Proceso	Monitoreo de Procesos	Eficiencia del Proceso	Gestión del Rendimiento	Gestión de los Resultados	Mejora de Proceso	Optimización de Procesos
APO13	APO13.01	1	1	1	1	1	1	1	1	1
	APO13.02	1	1	1	1	1	1	1	1	1
	APO13.03	0	0	0	0	0	0	0	0	0

Figura 11

Radar de atributos de capacidad APO13.01

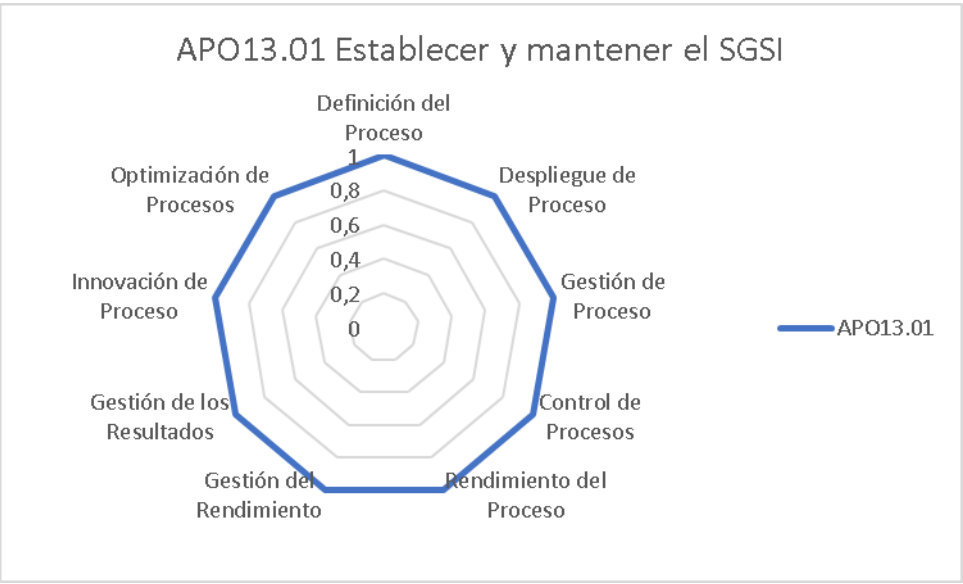


Figura 12

Radar de atributos de capacidad APO13.02

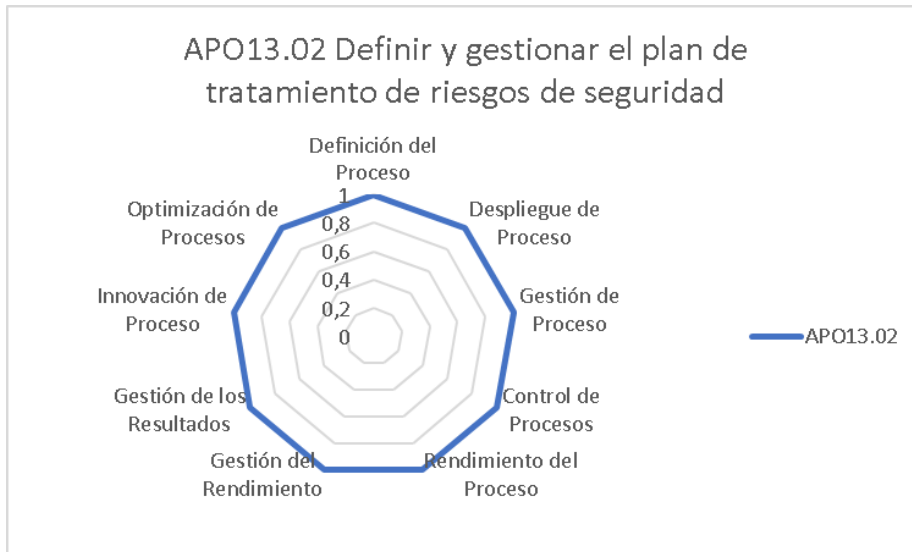


Figura 13

Radar de atributos de capacidad APO13.03

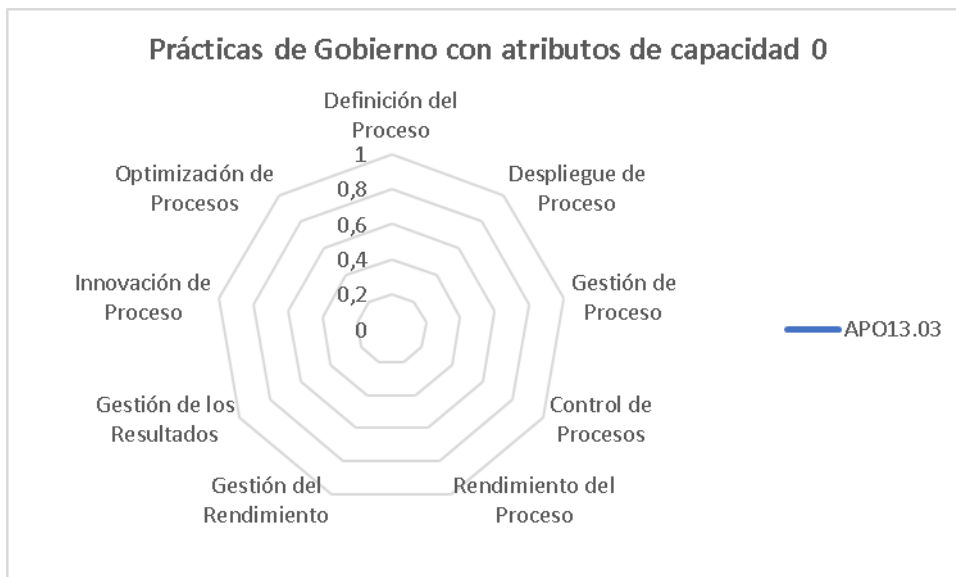


Tabla 33

Valoración de nivel de capacidad APO13

Descripción	Valor
Valor Óptima	27
Valor Obtenido	18
% alcanzado	0%
Escala	N

Tabla 34

BAI01

Atributos de Capacidad del Proceso										
Proceso	Práctica de Gobierno	Modelado del Proceso	Ejecución de Proceso	Gestión de Proceso	Monitoreo de Procesos	Eficiencia del Proceso	Gestión del Rendimiento	Gestión de los Resultados	Mejora de Proceso	Optimización de Procesos
BAI01	BAI01.01	0	0	0	0	0	0	0	0	0
	BAI01.02	1	1	1	1	1	1	1	1	1
	BAI01.03	0	0	0	0	0	0	0	0	0
	BAI01.04	0	0	0	0	0	0	0	0	0
	BAI01.05	0	0	0	0	0	0	0	0	0
	BAI01.06	0	0	0	0	0	0	0	0	0
	BAI01.07	1	1	1	1	1	1	1	1	1

Figura 14

Radar de atributos de capacidad BAI01.02

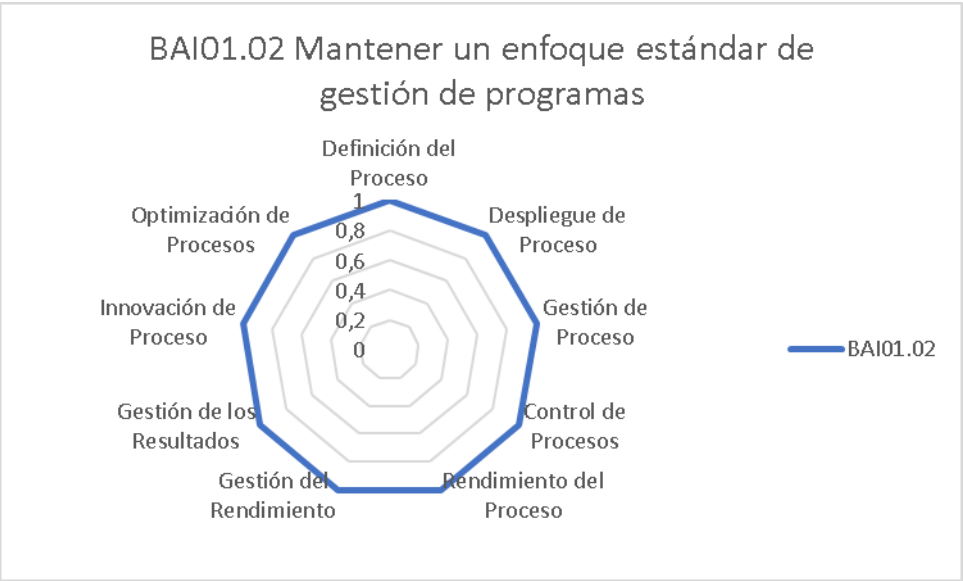


Figura 15

Radar de atributos de capacidad BAI01.07

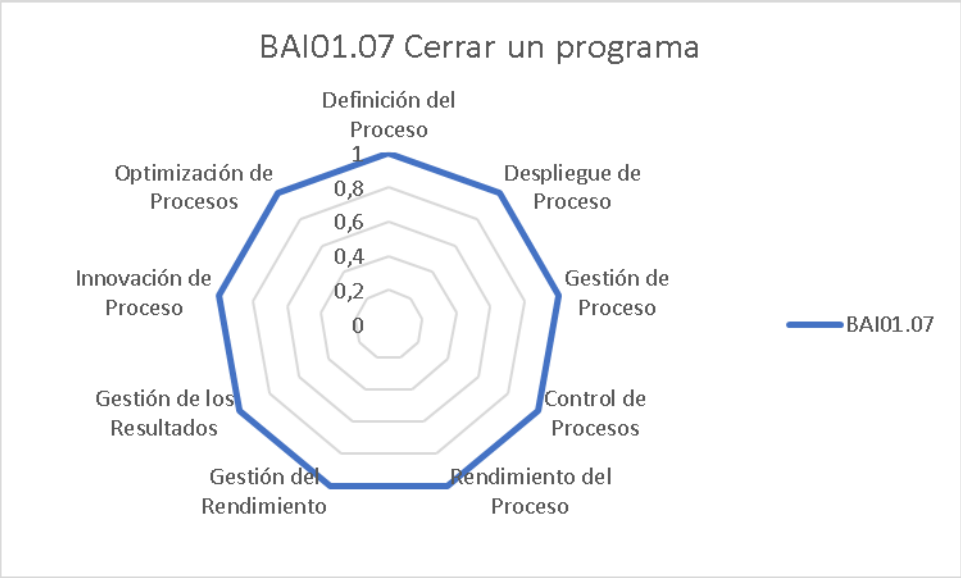


Figura 16

Radar de atributos de capacidad BAI01

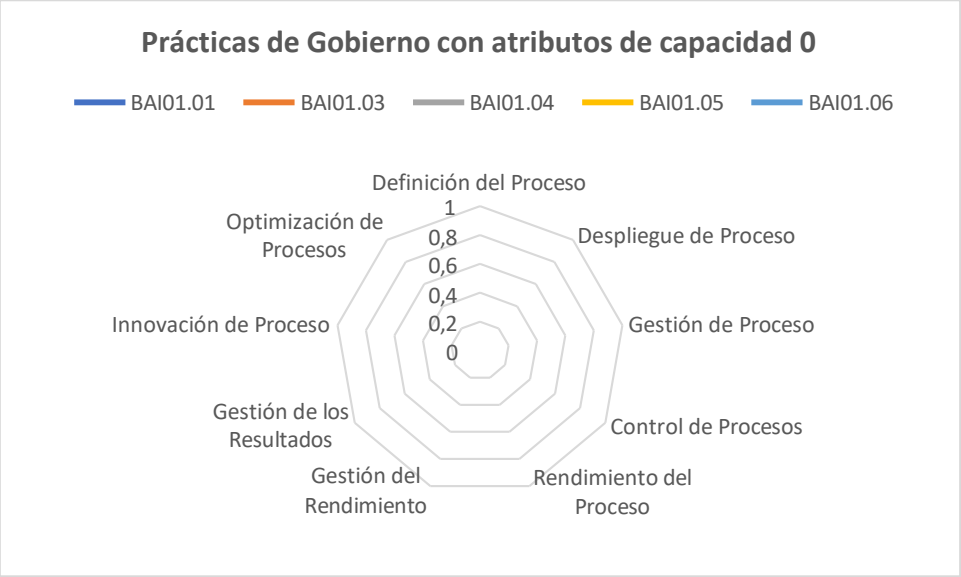


Tabla 35

Valoración de nivel de capacidad BAI01

Descripción	Valor
Valor Óptima	63

Valor Obtenido	18
% alcanzado	28.57%
Escala	P

Tabla 36

BAI09

Atributos de Capacidad del Proceso										
Proceso	Práctica de Gobierno	Modelado del Proceso	Ejecución de Proceso	Gestión de Proceso	Monitoreo de Procesos	Eficiencia del Proceso	Gestión del Rendimiento	Gestión de los Resultados	Mejora de Proceso	Optimización de Procesos
BAI09	BAI09.01	1	1	1	1	1	1	0	0	0
	BAI09.02	1	1	1	1	1	1	0	0	0
	BAI09.03	0	0	0	0	0	0	0	0	0

Figura 17

Radar de atributos de capacidad BAI09.01

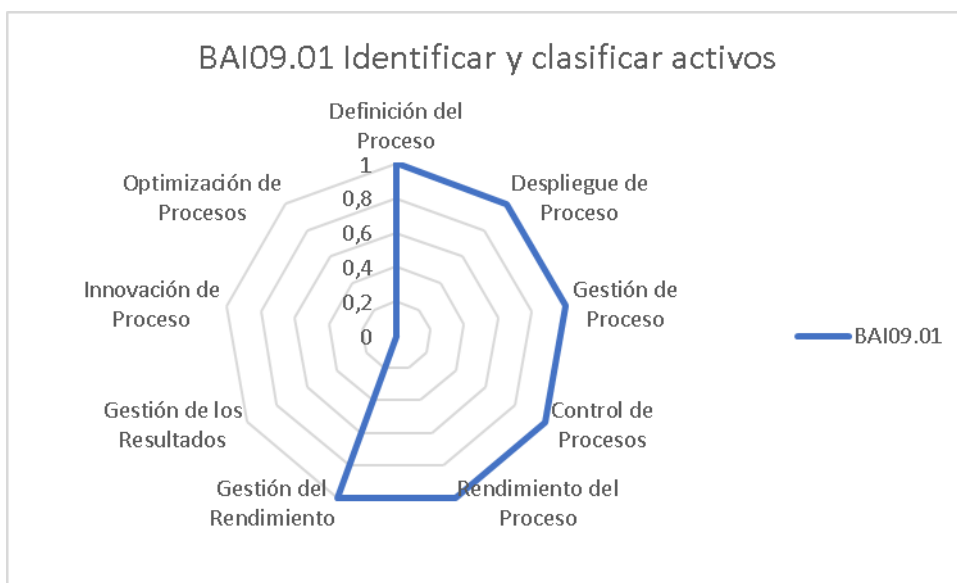


Figura 18

Radar de atributos de capacidad BAI09.02

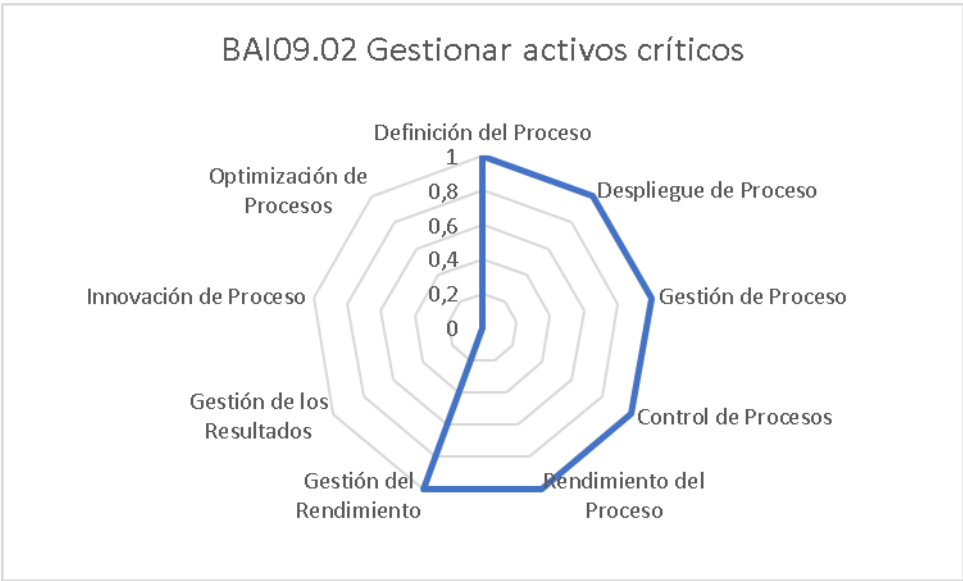


Figura 19

Radar de atributos de capacidad BAI09

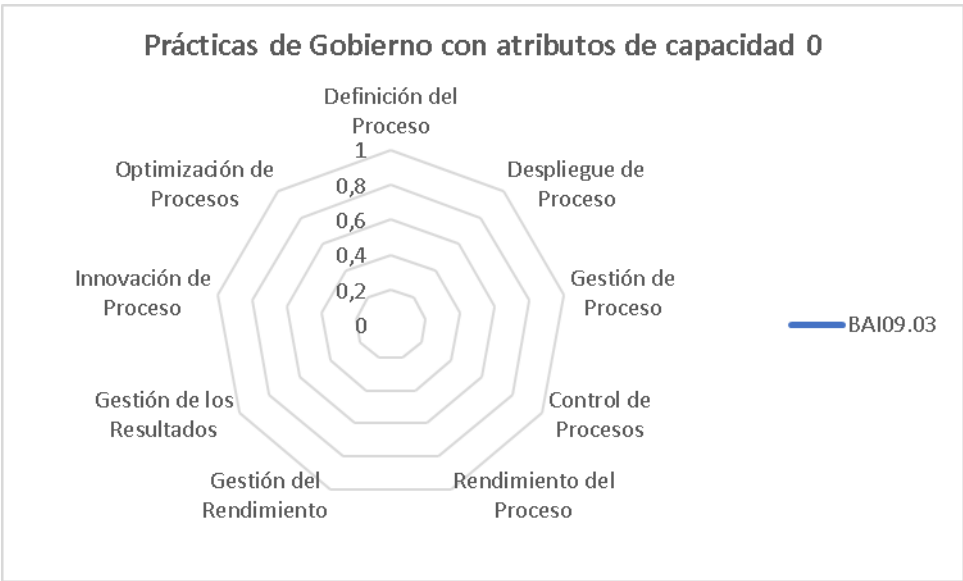


Tabla 37

Valoración de nivel de capacidad BAI09

Descripción	Valor
Valor Óptima	27
Valor Obtenido	12
% alcanzado	44.44%
Escala	P

Tabla 38

BAI10

Atributos de Capacidad del Proceso										
Proceso	Práctica de Gobierno	Modelado del Proceso	Ejecución de Proceso	Gestión de Proceso	Monitoreo de Procesos	Eficiencia del Proceso	Gestión del Rendimiento	Gestión de los Resultados	Mejora de Proceso	Optimización de Procesos
BAI10	BAI10.01	1	1	1	1	1	1	1	0	0
	BAI10.02	0	0	0	0	0	0	0	0	0
	BAI10.03	0	0	0	0	0	0	0	0	0

Figura 20

Radar de atributos de capacidad BAI10.1

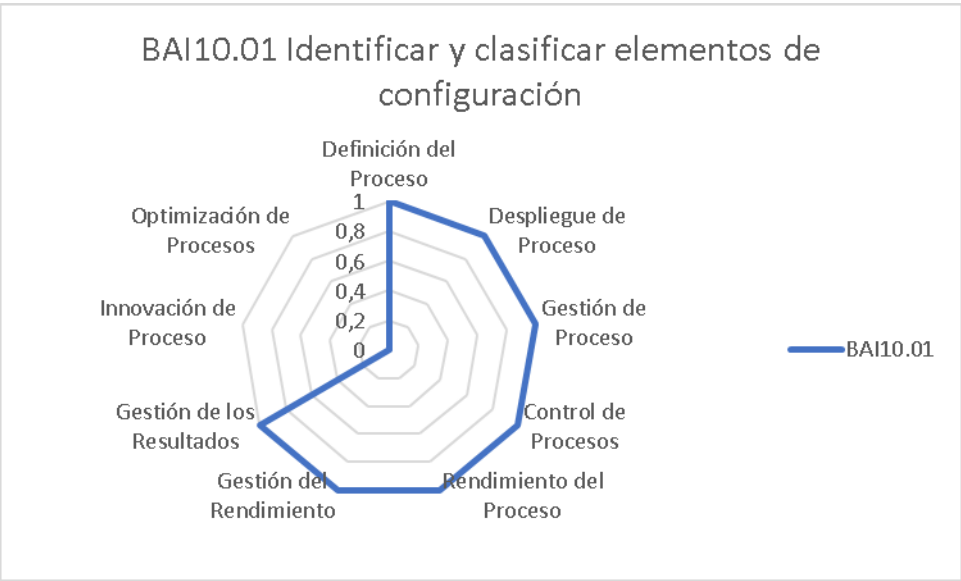


Figura 21

Radar de atributos de capacidad BAI10

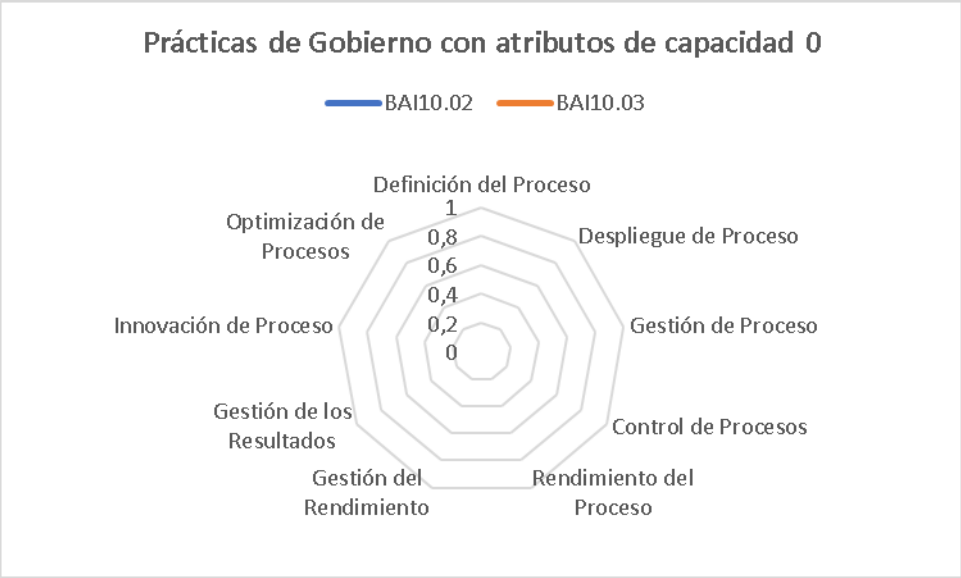


Tabla 39

Valoración de nivel de capacidad BAI10

Descripción	Valor
Valor Óptima	27
Valor Obtenido	7
% alcanzado	25.93%
Escala	P

Tabla 40

DSS02

Atributos de Capacidad del Proceso										
Proceso	Práctica de Gobierno	Modelado del Proceso	Ejecución de Proceso	Gestión de Proceso	Monitoreo de Procesos	Eficiencia del Proceso	Gestión del Rendimiento	Gestión de los Resultados	Mejora de Proceso	Optimización de Procesos
DSS02	DSS02.01	0	0	0	0	0	0	0	0	0
	DSS02.02	0	0	0	0	0	0	0	0	0
	DSS02.03	0	0	0	0	0	0	0	0	0
	DSS02.04	0	0	0	0	0	0	0	0	0

Figura 22

Radar de atributos de capacidad DSS02

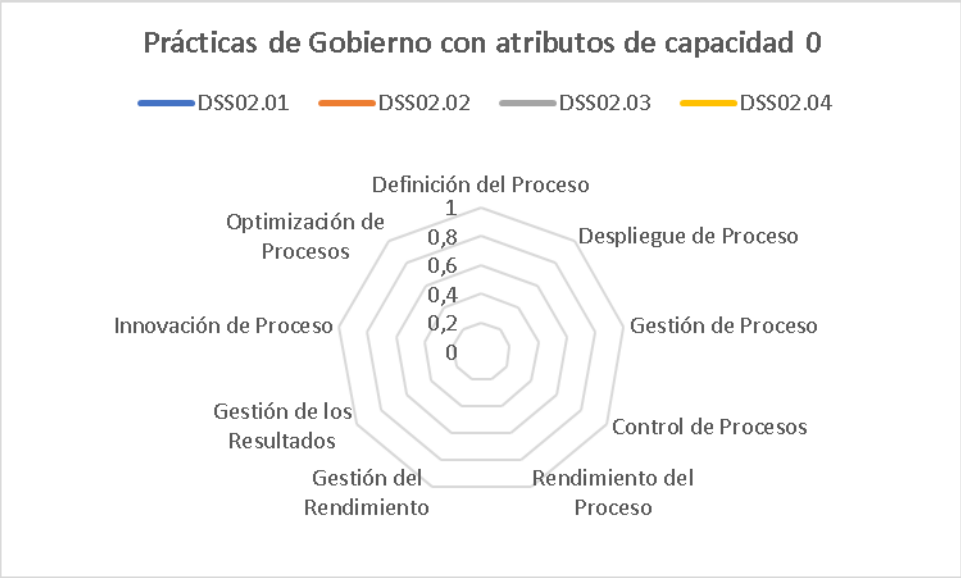


Tabla 41

Valoración de nivel de capacidad DSS02

Descripción	Valor
Valor Óptima	36
Valor Obtenido	0
% alcanzado	0%
Escala	N

Tabla 42

DSS03

Atributos de Capacidad del Proceso										
Proceso	Práctica de Gobierno	Modelado del Proceso	Ejecución de Proceso	Gestión de Proceso	Monitoreo de Procesos	Eficiencia del Proceso	Gestión del Rendimiento	Gestión de los Resultados	Mejora de Proceso	Optimización de Procesos
DSS03	DSS03.01	0	0	0	0	0	0	0	0	0
	DSS03.02	0	0	0	0	0	0	0	0	0
	DSS03.03	0	0	0	0	0	0	0	0	0
	DSS03.04	0	0	0	0	0	0	0	0	0

Figura 23

Radar de atributos de capacidad DSS03

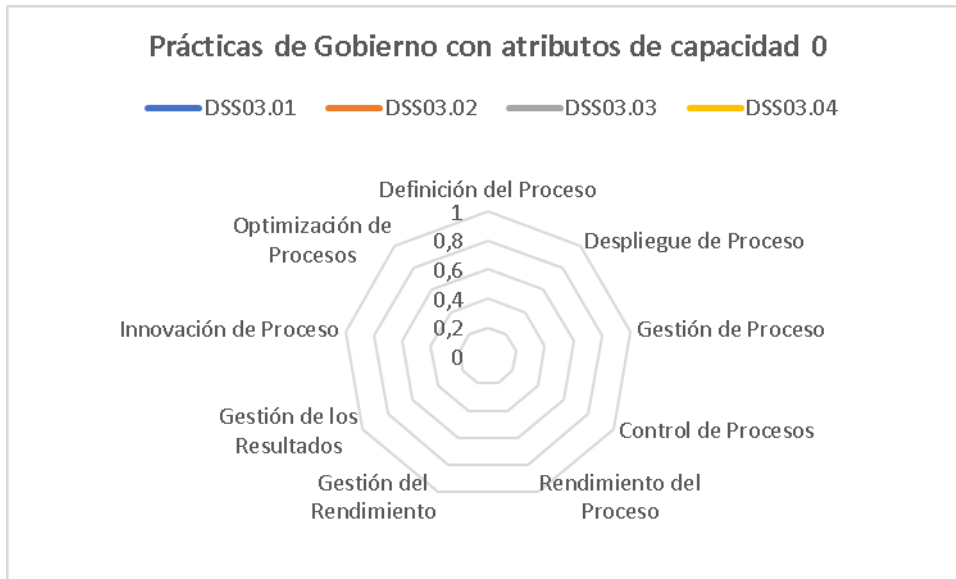


Tabla 43

Valoración de nivel de capacidad DSS03

Descripción	Valor
Valor Óptima	36
Valor Obtenido	0
% alcanzado	0%
Escala	N

Tabla 44

DSS04

Atributos de Capacidad del Proceso										
Proceso	Práctica de Gobierno	Modelado del Proceso	Ejecución de Proceso	Gestión de Proceso	Monitoreo de Procesos	Eficiencia del Proceso	Gestión del Rendimiento	Gestión de los Resultados	Mejora de Proceso	Optimización de Procesos
DSS04	DSS04.01	0	0	0	0	0	0	0	0	0
	DSS04.02	0	0	0	0	0	0	0	0	0
	DSS04.03	0	0	0	0	0	0	0	0	0
	DSS04.04	0	0	0	0	0	0	0	0	0

Figura 24

Radar de atributos de capacidad DSS04

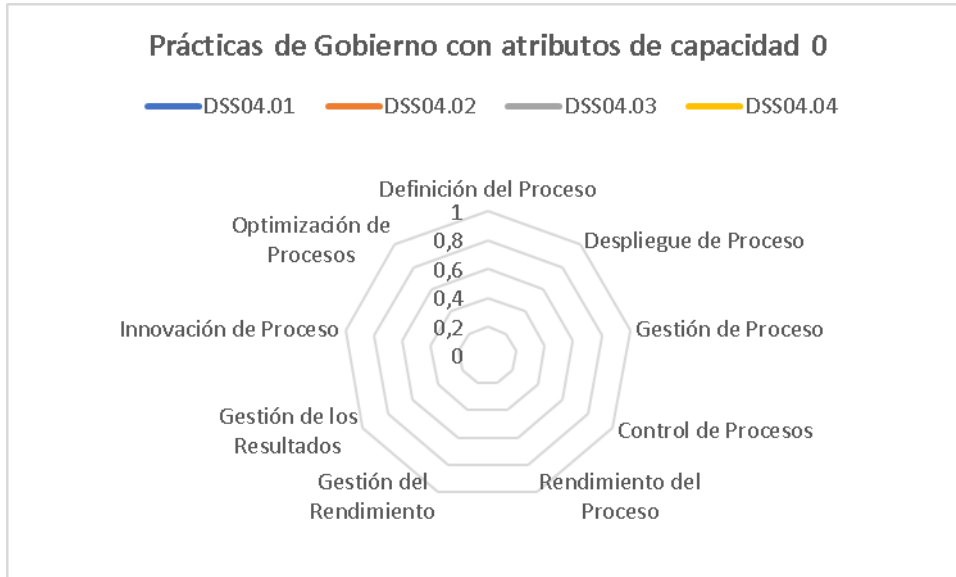


Tabla 45

Valoración de nivel de capacidad DSS04

Descripción	Valor
Valor Óptima	36
Valor Obtenido	0
% alcanzado	0%
Escala	N

Tabla 46

DSS05

Atributos de Capacidad del Proceso										
Proceso	Práctica de Gobierno	Modelado del Proceso	Ejecución de Proceso	Gestión de Proceso	Monitoreo de Procesos	Eficiencia del Proceso	Gestión del Rendimiento	Gestión de los Resultados	Mejora de Proceso	Optimización de Procesos
DSS05	DSS05.01	0	0	0	0	0	0	0	0	0
	DSS05.02	0	0	0	0	0	0	0	0	0
	DSS05.03	0	0	0	0	0	0	0	0	0

	DSS05.04	1	1	1	1	1	1	1	1	1
	DSS05.05	0	0	0	0	0	0	0	0	0
	DSS05.06	0	0	0	0	0	0	0	0	0

Figura 25

Radar de atributos de capacidad DSS05.04

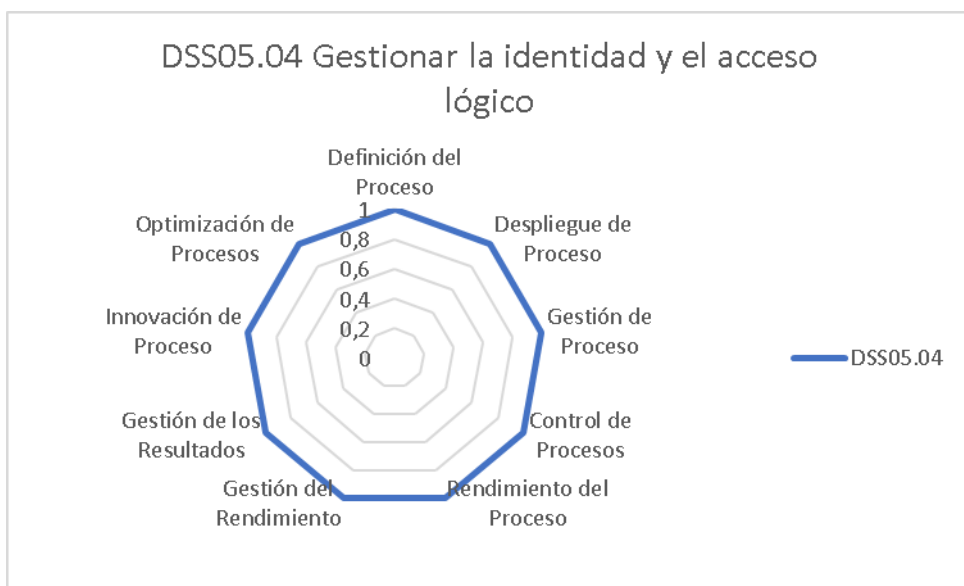


Figura 26

Radar de atributos de capacidad DSS05

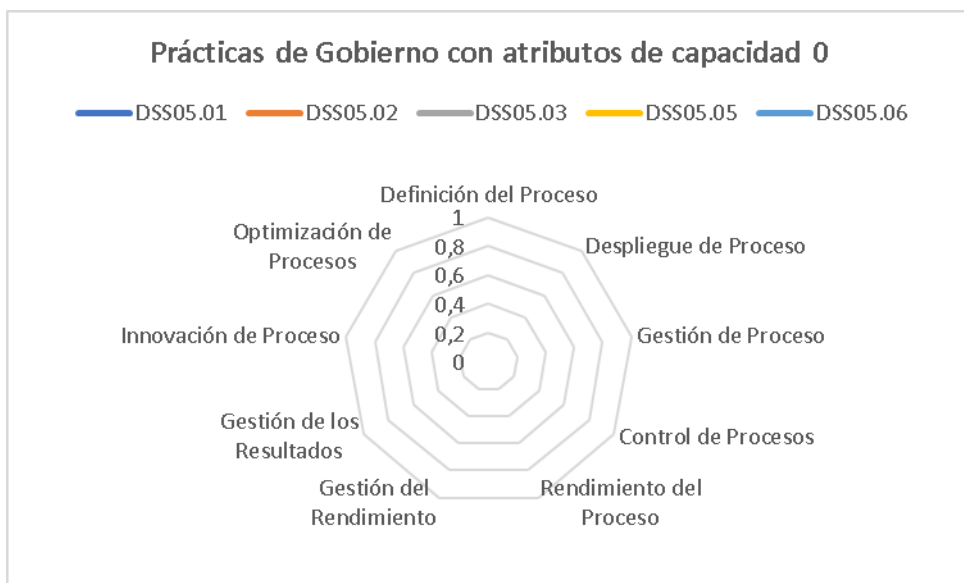


Tabla 47

Valoración de nivel de capacidad DSS05

Descripción	Valor
Valor Óptima	54
Valor Obtenido	9
% alcanzado	16.67%
Escala	P

Tabla 48

MEA02

Atributos de Capacidad del Proceso										
Proceso	Práctica de Gobierno	Modelado del Proceso	Ejecución de Proceso	Gestión de Proceso	Monitoreo de Procesos	Eficiencia del Proceso	Gestión del Rendimiento	Gestión de los Resultados	Mejora de Proceso	Optimización de Procesos
MEA02	MEA02.01	0	0	0	0	0	0	0	0	0
	MEA02.02	0	0	0	0	0	0	0	0	0
	MEA02.03	0	0	0	0	0	0	0	0	0

Figura 27

Radar de atributos de capacidad MEA02

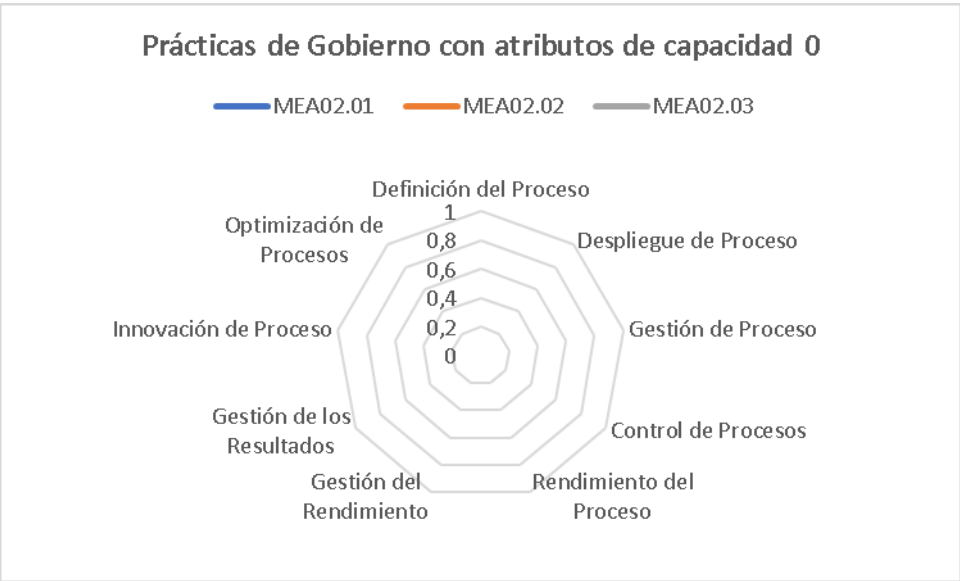


Tabla 49*Valoración de nivel de capacidad MEA02*

Descripción	Valor
Valor Óptima	27
Valor Obtenido	0
% alcanzado	0%
Escala	N

En términos consolidados, los procesos EDM03, APO12, DSS02, DSS03, DSS04 y MEA02 presentan un nivel no alcanzado, lo cual evidencia ausencia o debilidad significativa en la optimización del riesgo, la gestión formal de riesgos, la atención de incidentes, la gestión de problemas, la continuidad del servicio y el monitoreo de controles internos. Por otro lado, EDM04, APO01, APO13, BAI01, BAI09, BAI10 y DSS05 muestran avances parciales, aunque aún requieren formalización, seguimiento, indicadores y mejora continua.

Tabla 50*Evaluación consolidada de capacidad y brechas COBIT*

Proceso	% alcanzado	Escala	Brecha principal	Impacto sobre la gestión de riesgos
EDM03	0%	No alcanzado	No existe perfil, apetito, tolerancia ni reporte consolidado de riesgos.	Debilita la toma de decisiones sobre exposición al riesgo.
EDM04	66.67%	Parcialmente alcanzado	Existen controles parciales sobre recursos, pero falta monitoreo integral.	Afecta la optimización y disponibilidad de recursos tecnológicos.
APO01	25%	Parcialmente alcanzado	Roles y marco de gestión parcialmente definidos.	Limita la asignación clara de responsabilidades.

APO12	0%	No alcanzado	No existe proceso formal de recopilación, análisis y respuesta al riesgo.	Impide gestionar riesgos de manera estructurada.
APO13	66.67%	Parcialmente alcanzado	Existen controles básicos de seguridad, pero falta monitoreo.	Reduce la capacidad de prevenir incidentes de seguridad.
DSS02	0%	No alcanzado	No hay registro formal de solicitudes e incidentes.	Dificulta la atención y trazabilidad de fallas.
DSS03	0%	No alcanzado	No se identifican causas raíz ni acciones correctivas formales.	Incrementa la recurrencia de problemas.
DSS04	0%	No alcanzado	No existe política ni plan formal de continuidad.	Compromete la continuidad del servicio educativo.
DSS05	16.67%	Parcialmente alcanzado	Controles de seguridad incompletos.	Aumenta la exposición a accesos no autorizados e incidentes.
MEA02	0%	No alcanzado	No existe monitoreo formal del control interno.	Limita la mejora continua y seguimiento de controles.

4.1.4. GESTIÓN DE RIESGOS SEGÚN ISO 31000

La gestión de riesgos se estructura tomando como referencia ISO 31000, con el propósito de desarrollar un proceso formal y trazable. Por ello, la investigación integra las etapas de establecimiento del contexto, identificación de riesgos, análisis, evaluación, tratamiento, monitoreo, revisión y comunicación.

4.1.4.1. Establecimiento del contexto

Alcance del proceso de gestión de riesgos

El análisis se limita a las aulas multimedia de la UNS, además, incluye los recursos tecnológicos que soportan las actividades académicas: equipos, infraestructura física, conectividad, software, seguridad física, controles de acceso, soporte técnico y continuidad del servicio.

No abarca todos los servicios tecnológicos institucionales, sino solo los vinculados al funcionamiento de las aulas multimedia de OTIC, por ello, la delimitación enfoca la evaluación en recursos cuya falla, pérdida o deterioro puede afectar el servicio educativo.

Objetivos de la gestión de riesgos en el contexto evaluado

- Identificar los riesgos que pueden afectar los recursos tecnológicos de las aulas multimedia.
- Analizar la probabilidad e impacto de los eventos que comprometan la continuidad de las clases.
- Evaluar si los riesgos se encuentran dentro de niveles aceptables para la institución.
- Proponer acciones de tratamiento, control o mitigación frente a riesgos relevantes o inadmisibles.

Este objetivo permite que la gestión de riesgos no se limite a registrar deficiencias técnicas, sino que contribuya a priorizar decisiones de TI según su efecto sobre la continuidad del servicio académico, la seguridad de docentes y estudiantes, la integridad de la información y la disponibilidad de los ambientes multimedia.

Contexto interno

- Estado físico y operativo de computadoras, proyectores y dispositivos de conectividad.
- Disponibilidad de personal técnico para soporte, mantenimiento y atención de incidentes.
- Existencia de inventarios tecnológicos y registros de activos.
- Frecuencia de mantenimiento preventivo y correctivo.
- Formalización de políticas de uso, seguridad y control de accesos.
- Mantenimiento predominantemente correctivo, sin programación preventiva suficiente.
- Controles físicos limitados sobre puertas, ventanas, accesos y custodia de equipos.

- Falta de registros formales de incidentes y problemas recurrentes.
- Seguimiento limitado sobre software, licencias y antivirus.
- Alta dependencia de la capacidad operativa del área de OTIC para responder a fallas.

Contexto externo

- Interrupciones del suministro eléctrico.
- Dependencia de proveedores para renovación, reparación o mantenimiento de equipos.
- Limitaciones de presupuesto para reemplazo tecnológico y mejora de infraestructura.
- Cambios tecnológicos que pueden volver obsoletos ciertos equipos o aplicaciones.
- Exigencias de licenciamiento, actualización y cumplimiento normativo del software.
- Amenazas de seguridad física en ambientes de uso compartido.

Estos factores externos pueden aumentar la probabilidad o el impacto de los riesgos, es así como, cuando ocurre una interrupción eléctrica sin respaldo puede suspender clases o la falta de presupuesto puede retrasar la renovación de equipos y por otro lado la dependencia de licencias o actualizaciones externas puede generar vulnerabilidades si no existe planificación previa.

Partes interesadas

- **Personal de OTIC:** administra, mantiene y brinda soporte a los recursos tecnológicos.
- **Apoyo de OTIC:** atienden fallas, revisan infraestructura y ejecutan acciones correctivas.
- **Docentes:** utilizan los recursos multimedia para desarrollar clases y prácticas académicas.
- **Alumnado:** dependen de la disponibilidad y funcionamiento de los equipos para su aprendizaje.

- **Autoridades académicas:** requieren que el servicio educativo se mantenga operativo, seguro y alineado a los objetivos institucionales.

Activos críticos considerados

- Computadoras de aula y equipos de apoyo académico.
- Proyector, equipos de sonido y multimedia.
- Puntos de red, cableado de datos y conectividad.
- Tomacorrientes, cableado eléctrico y condiciones de energía.
- Software académico, sistemas operativos, licencias y antivirus.
- Puertas, ventanas, cerraduras y mecanismos de acceso físico.
- Mobiliario tecnológico e información académica almacenada o utilizada durante las clases.

Criterios de valoración del riesgo

- **Probabilidad:** mide la posibilidad de ocurrencia del evento de riesgo, considerando frecuencia observada, estado del activo, controles existentes y experiencia del personal técnico.
- **Impacto:** mide la severidad de las consecuencias sobre la continuidad académica, la seguridad de los usuarios, la disponibilidad tecnológica, la integridad de la información y el cumplimiento institucional.
- **Escala de probabilidad:** 1 rara vez, 2 improbable, 3 ocasional, 4 probable y 5 frecuente.
- **Escala de impacto:** 1 leve, 2 moderado, 3 significativo, 4 alto y 5 extremo.
- **Resultado esperado:** obtener una valoración comparable que permita calcular el nivel de exposición de cada riesgo.

Tolerancia y aceptabilidad del riesgo

- **Riesgos permitidos:** pueden aceptarse con monitoreo básico.
- **Riesgos admisibles:** pueden aceptarse temporalmente, siempre que exista seguimiento preventivo.

- **Riesgos limitados:** requieren acciones preventivas para evitar que aumenten su exposición.
- **Riesgos relevantes:** no deben mantenerse sin control y requieren mitigación planificada.
- **Riesgos inadmisibles:** no son aceptables y requieren tratamiento obligatorio o acción inmediata.

La tolerancia al riesgo permite establecer reglas de decisión antes de valorar los riesgos, es así como, la institución puede distinguir qué riesgos pueden aceptarse temporalmente, cuáles requieren seguimiento y cuáles deben ser tratados de forma prioritaria.

Relación del contexto con COBIT

- **EDM03:** optimización del riesgo y toma de decisiones sobre exposición.
- **APO12:** gestión formal del riesgo de TI.
- **APO13:** gestión de seguridad de la información.
- **DSS04:** continuidad del servicio educativo soportado por TI.
- **DSS05:** servicios de seguridad, protección de activos y control de accesos.
- **BAI09 y BAI10:** gestión de activos tecnológicos y configuración.
- **MEA02:** monitoreo del control interno y seguimiento de controles.

Esta relación permite integrar ISO 31000 y COBIT de manera coherente: ISO 31000 ordena el proceso de gestión de riesgos, mientras que COBIT aporta los procesos de gobierno y gestión necesarios para asignar responsabilidades, evaluar brechas, definir controles y monitorear la mejora.

4.1.4.2. Identificación de Riesgos

La identificación de riesgos se realiza a partir de la observación directa, el inventario, el análisis de controles existentes y la información proporcionada por los responsables de OTIC. Entre los riesgos identificados se encuentran equipos obsoletos, puntos eléctricos y de red deteriorados, puertas y ventanas en mal estado, software desactualizado, cables dañados, robos o pérdidas de equipos, falta de mantenimiento, uso de dispositivos USB infectados, falta de políticas de

seguridad, cortes de flujo eléctrico sin respaldo, falta de licencias de software, antivirus desactualizado e ingreso de personas no autorizadas.

Los riesgos identificados se clasifican por tipo, considerando riesgos de hardware, infraestructura, software, factor humano, operación, seguridad de la información, continuidad del servicio y cumplimiento legal. Esta clasificación permite relacionar cada riesgo con los activos afectados, sus causas, consecuencias y procesos COBIT asociados.

Tabla 51

Identificación de los riesgos

ID	Riesgo identificado	Tipo de riesgo	Activo o servicio afectado
R01	Equipos obsoletos	Hardware	PC, proyectores y equipos de sonido
R02	Tomacorrientes y puntos de red deteriorados	Infraestructura	Conectividad y energía eléctrica
R03	Ventanas y puertas rotas	Infraestructura	Seguridad física del aula
R04	Software desactualizado	Software	Sistemas y aplicaciones académicas
R05	Cables dañados por mal uso	Humano / infraestructura	Cableado eléctrico y de datos
R06	Robos y pérdidas de equipos tecnológicos	Humano / seguridad	Equipos tecnológicos e información
R07	Falta de mantenimiento	Operativo	Equipos e infraestructura tecnológica
R08	Uso de USB con virus	Seguridad de información	Computadoras e información académica
R09	Falta de políticas de seguridad	Operativo	Uso y control de aulas multimedia
R10	Cortes eléctricos sin respaldo	Continuidad	Servicio educativo y equipos
R11	Licencias de software inexistentes	Legal / cumplimiento	Software institucional

R12	Antivirus desactualizado	Seguridad de información	Computadoras y datos
R13	Ingreso de personas no autorizadas	Seguridad física	Aulas, equipos e información

Fuente. Elaboración propia

4.1.4.3. Análisis de Riesgos

El análisis de riesgos considera la probabilidad de ocurrencia y el impacto sobre el servicio educativo, la seguridad de los usuarios, la disponibilidad de los recursos tecnológicos, la integridad de la información y el cumplimiento institucional. Para ello, se utilizan niveles de probabilidad e impacto que permiten calcular el nivel de exposición de cada riesgo.

La valoración utiliza una escala de probabilidad de 1 a 5, que va desde rara vez hasta frecuente, y una escala de impacto de 1 a 5, que va desde leve hasta extremo. La combinación de ambos criterios permite calcular la exposición al riesgo y determinar si el riesgo se ubica en un nivel permitido, admisible, limitado, relevante o inadmisible.

4.1.4.3.1. Análisis cualitativo

Para identificar y priorizar se establecieron probabilidades en diferentes niveles, así como el impacto.

Tabla 52

Niveles de probabilidad de riesgo

PROBABILIDAD		
1	RARA VEZ	- Es un riesgo que casi nunca ha sucedido, aproximadamente en un rango de 2 años.
2	IMPROBABLE	- Es un riesgo que se da en el periodo de uno a 2 años

3	OCASIONAL	- El riesgo se puede presentar en un periodo de 6 meses
4	PROBABLE	- El riesgo se observa en un periodo de 3 meses
5	FRECUENTE	- El riesgo se observa constantemente en un periodo de 3 meses

Tabla 53

Niveles de impacto de riesgo

IMPACTO		
1	LEVE	- Es un riesgo que a pesar de ocurrir no es el factor principal por el cual se detengan los procesos y/o servicios
2	MODERADO	- Es un riesgo que afecta levemente a los procesos de la institución, afectando algunos usuarios por un corto tiempo
3	MEDIO	- El riesgo que afecta e interrumpe los procesos de la institución, pero no los que son críticos
4	ALTO	- El riesgo que afecta a todos los procesos tanto secundarios como críticos
5	EXTREMO	- El riesgo que afecta de manera indefinida los procesos críticos de la institución

Es así que llegamos a construir la siguiente matriz, en la que se establece una representación de cómo puede afectar a la institución.

Tabla 54

Esquema de Probabilidad e Impacto

Posibilidad de Ocurrencia	FRECUENTE	Limitado	Relevante	Inadmisible	Inadmisible	Inadmisible
	PROBABLE	Admisible	Limitado	Relevante	Inadmisible	Inadmisible
	OCASIONAL	Admisible	Limitado	Relevante	Relevante	Inadmisible
	IMPROBABLE	Permitido	Admisible	Limitado	Limitado	Relevante

	RARA VEZ	Permitido	Permitido	Admisible	Admisible	Limitado
		LEVE	MODERAD O	SIGNIFICATIV O	ALTO	EXTREM O
IMPACTO						

Además, definimos los niveles de riesgo en el siguiente cuadro

Tabla 55

Niveles de riesgo cualitativo

EXPOSICION	
0	PERMITIDO
1	PERMITIDO
5	PERMITIDO
10	ADMISIBLE
15	LIMITADO
20	RELEVANTE
25	INADMISIBLE

4.1.4.3.2. Análisis cuantitativo

Se establecen niveles cuantitativos de exposición al riesgo.

Tabla 56

Niveles de riesgo cuantitativos

EXPOSICION	
0 - 2	PERMITIDO
3 - 4	ADMISIBLE
5 - 8	LIMITADO

9 - 12	RELEVANTE
15 - 25	INADMISIBLE

Además, para este análisis se hizo uso de la siguiente matriz:

Tabla 57

Matriz de análisis de probabilidad por impacto

Posibilidad de Ocurrencia	5	FRECUENTE	5	10	15	20	25
	4	PROBABLE	4	8	12	16	20
	3	OCASIONAL	3	6	9	12	15
	2	IMPROBABLE	2	4	6	8	10
	1	RARA VEZ	1	2	3	4	5
			LEVE	MODERADO	SIGNIFICATIVO	ALTO	EXTREMO
			1	2	3	4	5
			IMPACTO				

Luego de establecer esta clasificación, se determinó las consecuencias

Tabla 58

Impacto Cuantitativo del Riesgo

Objetivo del Proyecto	Leve (0.05)	Moderado (0.1)	Significativo (0.2)	Alto (0.4)	Extremo (0.8)
Costo	Aumento poco significativo del costo	< 5% de aumento del costo	5–10% de Aumento en el costo	10–20% de Aumento en el costo	> 20% de Aumento en el costo
Tiempo	Atraso poco significativo	Atraso < 5%	Atraso 5–10%	Atraso 10–20%	Atraso > 20%
Alcance	Disminución sin notarse	Afectación secundaria	Afectación principal	Reducción Inadmisible	Producto sin utilidad

Calidad	Disminución sin notarse	Afectación exigente	Reducción con <u>aprobación</u>	Reducción Inadmisible	No utilizable
----------------	----------------------------	------------------------	---------------------------------------	--------------------------	------------------

4.1.4.4. Evaluación de Riesgos

Comparamos los niveles de exposición obtenidos con los criterios de aceptabilidad definidos. Los riesgos se clasifican como permitidos, admisibles, limitados, relevantes o inadmisibles. Esta clasificación permite priorizar los riesgos que requieren tratamiento inmediato y aquellos que pueden ser aceptados temporalmente bajo monitoreo.

De acuerdo con los resultados obtenidos, los riesgos con mayor exposición corresponden a ventanas y puertas rotas, software desactualizado, robos o pérdidas de equipos tecnológicos, licencias inexistentes e ingreso de personas no autorizadas, todos ellos clasificados como inadmisibles. También se identifican riesgos inadmisibles asociados con tomacorrientes y puntos de red deteriorados, cables dañados, falta de mantenimiento, uso de USB con virus, ausencia de políticas de seguridad y antivirus desactualizado.

Los riesgos clasificados como inadmisibles o relevantes superan la tolerancia definida para el estudio, por lo que requieren tratamiento obligatorio. En cambio, los riesgos limitados, admisibles o permitidos pueden ser gestionados mediante acciones preventivas, seguimiento o aceptación controlada.

Tabla 59

Evaluación de riesgos

ID	Nombre del riesgo	Causante	Consecuencias	Impacto		Ocurrencia		Exposición al Riesgo	
R1	Equipos obsoletos (PC, Proyector, Equipo de sonido)	Falta de recursos financieros o mal manejo	Docentes dictan clases con dificultad y tiempos de demora.	Significativo	3	Frecuente	5	Inadmisible	15
R2	Tomacorrientes y puntos de red deteriorados	Falta de mantenimiento y mal uso	Descarga eléctrica a estudiantes o docentes.	Extremo	5	Probable	4	Inadmisible	20
R3	Ventanas y Puertas rotas	Falta de mantenimiento	Pérdida o robo de equipos	Extremo	5	Frecuente	5	Inadmisible	25
R4	Software desactualizado	Falta de licencias	Problemas legales, riesgo de malware con pérdida de información.	Extremo	5	Frecuente	5	Inadmisible	25
R5	Cables dañados	Mal uso de los usuarios	Descarga eléctrica a estudiantes o docentes.	Extremo	5	Probable	4	Inadmisible	20
R6	Robos y pérdidas de equipos tecnológicos	No existen políticas de seguridad. Cámaras no funcionan	Pérdida de información, clases sin apoyo tecnológico.	Extremo	5	Frecuente	5	Inadmisible	25
R7	Falta de mantenimiento	No hay gestiones	Deterioro de equipos y licencias vencidas.	Significativo	3	Frecuente	5	Inadmisible	15

R8	Uso de USB con virus en las PC	Falta de controles de seguridad	Contaminación en los demás pc de las aulas. Pérdida de información.	Significativo	3	Frecuente	5	Inadmisible	15
R9	Falta de políticas de seguridad en las aulas	Mala gestión de seguridad	Mal uso de los equipos, pérdida o filtración de información.	Significativo	3	Frecuente	5	Inadmisible	15
R10	Cortes de fluido eléctrico sin respaldo	Falta de plan de acción	Interrupción de actividades educativas, pérdida de seguridad en puertas de aulas.	Alto	4	Medio	3	Relevante	12
R11	Licencias de software inexistentes	Falta de presupuesto	Problemas legales, riesgo de malware con pérdida de información.	Extremo	5	Frecuente	5	Inadmisible	25
R12	Falta de antivirus actualizado	Falta de mantenimiento y presupuesto	Pérdida de información y contaminación de virus masiva.	Alto	4	Frecuente	5	Inadmisible	20
R13	Ingreso de personas no autorizadas	Falta de controles de seguridad	Pérdida de equipos, robos, daños.	Extremo	5	Frecuente	5	Inadmisible	25

4.1.4.5. Tratamiento de Riesgos

Consideramos cuatro alternativas: evitar, reducir, transferir o aceptar el riesgo. El tratamiento se prioriza según el nivel de exposición y la capacidad institucional de respuesta. En los riesgos inadmisibles se recomienda reducir o evitar la exposición mediante acciones inmediatas, en los riesgos relevantes recomendamos reducir o transferir parcialmente el impacto y en los riesgos de menor nivel se permite aceptar el riesgo bajo monitoreo, siempre que exista responsable y evidencia de seguimiento.

Están orientadas a fortalecer controles preventivos, correctivos y de detección. Entre ellas se consideran mantenimiento preventivo, actualización tecnológica, regularización de licencias, políticas de seguridad, control de accesos, respaldo eléctrico, antivirus corporativo y monitoreo de incidentes.

Tabla 60

Tratamiento de riesgos

ID	Descripción del riesgo	Controles existentes	Tratamiento al riesgo	Propuesta de mejora	Riesgo residual	Riesgo secundario	Responsable
R1	Equipos obsoletos (PC, Proyector, Equipo de sonido)	Reparación y cambio de piezas.	Reducir el riesgo	Implementar inventario con fechas de vida útil de cada equipo.	Falta de administración	Interrupción por falla en los equipos	Equipo de TI
R2	Tomacorrientes y puntos de red deteriorados	No hay controles	Mitigar el riesgo	Cambio de tomacorrientes con inspecciones por ciclo	Falta de puntos de conexión ocasionando sobrecargas	Interrupción de actividades de manera temporal	Equipo de TI
R3	Ventanas y Puertas rotas	Reparación al inicio de ciclo	Reducir el riesgo	Reparar y reforzar con rejillas y/o protectores	Robo	Aulas fuera de uso de manera temporal	Equipo de TI
R4	Software desactualizado	No hay controles	Reducir el riesgo	Programación de actualizaciones automáticas cada ciclo	Fallas en las nuevas versiones	Falta de compatibilidad de las nuevas versiones	Equipo de TI

R5	Cables dañados	Cambio de cables frente a incidencias	Mitigar riesgo	el	Cableado nuevo y mejor organizado	Daño por constante manipulación	Riesgo de descarga eléctrica	Equipo de TI
R6	Robos y pérdidas de equipos tecnológicos	Ingreso de estudiantes con carnet	Mitigar riesgo	el	Cámaras de seguridad e inventario actualizado	Falta de control de cámaras de seguridad	Vulneración de la privacidad	Equipo de TI
R7	Falta de mantenimiento	Revisión cada inicio de ciclo	Reducir riesgo	el	Programa de mantenimiento por ciclo con responsables asignados	Fallas imprevistas	Recursos financieros extras	Equipo de TI
R8	Uso de USB con virus en las PC	Recomendación uso de USB solo de docentes	Reducir riesgo	el	Bloqueo de puertos USB	Virus avanzados	Impedimento y retrasos en el servicio de enseñanza por necesidad de uso de puerto USB	Equipo de TI
R9	Falta de políticas de seguridad en las aulas	Accesos autorizados con tarjeta	Mitigar riesgo	el	Reglamento de seguridad en cada aula	Falta de capacitación	Falta de compromiso	Equipo de TI
R10	Cortes de fluido eléctrico sin respaldo	UPS	Mitigar riesgo	el	Implementación de UPS	Mantenimiento de UPS	Daños por incorrecta manipulación	Equipo de TI
R11	Licencias de software inexistentes	Formateos cada inicio de ciclo	Reducir riesgo	el	Establecer recursos financieros para su regularización	Auditorías internas	Falta de capacitación para uso de nuevo software	Equipo de TI

R12	Falta de antivirus actualizado	antivirus	Instalación cada inicio de ciclo	Mitigar riesgo	el	Adquirir antivirus corporativo	Costos extra	Programa muy pesado para equipos desactualizado	Equipo de TI
R13	Ingreso de personas no autorizadas	no	No hay controles	Reducir riesgo	el	Registro de visitas con retención de credenciales	Identificaciones falsas	Falta de personal para horarios de alta demanda.	Equipo de TI

4.1.4.6. Monitoreo, revisión y comunicación

La revisión debe realizarse de forma mensual para riesgos inadmisibles, bimestral para riesgos relevantes y trimestral para riesgos limitados, admisibles o permitidos. La comunicación del riesgo debe realizarse mediante reportes técnicos dirigidos a OTIC y a los responsables institucionales correspondientes. Dichos reportes deben incluir los riesgos críticos, controles vencidos, incidentes recurrentes, acciones correctivas pendientes, responsables asignados y fecha estimada de cierre. Cuando un riesgo inadmisibles no sea tratado dentro del plazo definido, deberá escalararse a la jefatura de OTIC para la toma de decisiones y asignación de recursos.

Tabla 61

Esquema técnico de monitoreo, revisión y comunicación de riesgos

Elemento de seguimiento	Criterio técnico	Evidencia requerida	Responsable
Riesgos inadmisibles	Revisión mensual y tratamiento obligatorio.	Matriz actualizada, reporte de avance y evidencia del control aplicado.	Responsable de TI / Jefatura OTIC
Riesgos relevantes	Revisión bimestral y control planificado.	Registro de seguimiento, incidentes asociados y estado de acciones correctivas.	Responsable técnico asignado
Riesgos limitados, admisibles o permitidos	Revisión trimestral y monitoreo preventivo.	Registro de verificación y actualización del nivel de exposición.	Responsable técnico asignado
Indicadores de control	Cumplimiento de mantenimiento, actualización, incidentes, accesos y disponibilidad.	Checklist técnico, reporte de incidentes, inventario actualizado y evidencias fotográficas.	Equipo de TI
Escalamiento	Se activa cuando un riesgo inadmisibles permanece sin tratamiento o un control crítico vence.	Reporte de excepción, responsable asignado y decisión de jefatura.	Jefatura OTIC
Comunicación	Reporte periódico de riesgos críticos, acciones pendientes y estado de controles.	Informe técnico de seguimiento y acta o registro de revisión.	OTIC

4.1.4.7. CRITERIOS DE TOLERANCIA, ACEPTABILIDAD Y RESPUESTA AL RIESGO

Aquí establecimos el nivel máximo de exposición que la Universidad Nacional del Santa puede aceptar en las aulas multimedia sin comprometer la continuidad del servicio educativo, la seguridad de estudiantes y docentes, la disponibilidad de los recursos tecnológicos ni la integridad de la información.

Los riesgos permitidos y admisibles podrán ser aceptados temporalmente bajo monitoreo. Los riesgos limitados requerirán acciones preventivas para evitar su incremento. Los riesgos relevantes e inadmisibles no serán aceptados sin tratamiento y deberán contar con mecanismos de control, mitigación o reducción de exposición.

Bajo estos criterios, los riesgos con exposición inadmisibles deben ser tratados de forma prioritaria, debido a que comprometen la continuidad del servicio educativo, la seguridad de los usuarios, la disponibilidad de los recursos tecnológicos o la integridad de la información. Los riesgos relevantes requieren acciones de control planificadas y seguimiento periódico, mientras que los riesgos limitados, admisibles o permitidos pueden mantenerse bajo monitoreo según su evolución.

Tabla 62

Criterios de aceptabilidad y respuesta al riesgo

Nivel de riesgo	Aceptabilidad		Decisión requerida	Tipo de respuesta	
Permitido	Aceptable		Monitoreo básico.	Aceptar	
Admisible	Aceptable con seguimiento		Control preventivo y revisión periódica.	Aceptar / reducir	
Limitado	Parcialmente aceptable		Plan de tratamiento preventivo.	Reducir	
Relevante	No aceptable sin control		Mitigación obligatoria y responsable asignado.	Reducir / transferir	
Inadmisible	No aceptable		Acción inmediata de control o mitigación.	Evitar / reducir	

4.1.4.8. MATRIZ DE RIESGOS Y NIVELES DE EXPOSICIÓN

Consolidamos los riesgos identificados, valorando probabilidad e impacto, nivel de exposición y acciones de tratamiento, es así como la matriz representa una herramienta de análisis y soporte para la toma de decisiones.

Los riesgos identificados en el estudio muestran niveles de exposición significativos, especialmente en aquellos vinculados con infraestructura deteriorada, software desactualizado, falta de mantenimiento, ausencia de políticas de seguridad, licencias inexistentes, falta de antivirus actualizado y control insuficiente de accesos.

Tabla 63

Matriz consolidada de riesgos y niveles de exposición

ID	Riesgo	Probabilidad	Impacto	Exposición	Nivel
R01	Equipos obsoletos y Tomacorrientes	5	3	15	Inadmisible
R02	puntos de red deteriorados	4	5	20	Inadmisible
R03	Ventanas y puertas rotas	5	5	25	Inadmisible
R04	Software desactualizado	5	5	25	Inadmisible
R05	Cables dañados	4	5	20	Inadmisible
R06	Robos y pérdidas de equipos	5	5	25	Inadmisible
R07	Falta de mantenimiento	5	3	15	Inadmisible
R08	Uso de USB con virus	5	3	15	Inadmisible
R09	Falta de políticas de seguridad	5	3	15	Inadmisible
R10	Cortes eléctricos sin respaldo	3	4	12	Relevante
R11	Licencias inexistentes	5	5	25	Inadmisible
R12	Antivirus desactualizado	5	4	20	Inadmisible
R13	Ingreso de personas no autorizadas	5	5	25	Inadmisible

4.1.4.9. PLAN DE TRATAMIENTO, CONTROL Y MITIGACIÓN DE RIESGOS

El plan de tratamiento permite establecer acciones concretas frente a los riesgos priorizados. Estas acciones se relacionan con los procesos COBIT correspondientes, responsables, respuestas, prioridad y evidencia esperada. Entre las acciones prioritarias se consideran la renovación progresiva de equipos obsoletos, mantenimiento de tomacorrientes y puntos de red, reparación de puertas y ventanas, actualización y regularización de software, control de dispositivos externos, fortalecimiento de antivirus, definición de políticas de seguridad, implementación de controles de acceso, plan de continuidad ante cortes eléctricos y monitoreo periódico de incidentes.

Este tratamiento se orienta principalmente a reducir o mitigar los riesgos. Para los equipos obsoletos se plantea un inventario con vida útil y renovación progresiva, para los tomacorrientes, puntos de red, cables, puertas y ventanas, por ello se proponen inspecciones, mantenimiento y reforzamiento físico, además, para software, licencias y antivirus se recomienda regularización, actualización y control centralizado, para riesgos de acceso o robo se plantea control de ingreso, cámaras operativas, registro de visitas y políticas de seguridad en las aulas.

Tabla 64

Plan de tratamiento, control y mitigación de riesgos

Riesgo	Proceso COBIT asociado	Respuesta	Control o acción propuesta	Responsable
Equipos obsoletos	EDM04 / BAI09	Reducir	Inventario con vida útil y renovación progresiva.	Equipo de TI
Tomacorrientes, puntos de red y cables dañados	DSS04 / DSS05	Mitigar	Inspección periódica, mantenimiento y reemplazo de infraestructura deteriorada.	Equipo de TI
Puertas y ventanas rotas	DSS05	Reducir	Reparación, reforzamiento físico y control de seguridad del aula.	Equipo de TI
Software desactualizado y	BAI10 / APO13	Reducir	Actualización programada,	Equipo de TI

licencias inexistentes					regularización de licencias y control centralizado.	
Robos, pérdidas e ingreso no autorizado	DSS05 MEA02	/	Mitigar		Control de ingreso, registro de visitas, cámaras operativas y monitoreo.	Equipo de TI
Falta de mantenimiento	DSS03 BAI09	/	Reducir		Programa de mantenimiento preventivo con responsables y evidencias.	Equipo de TI
USB con virus y antivirus desactualizado	APO13 DSS05	/	Mitigar		Antivirus corporativo, bloqueo o control de puertos USB y políticas de uso.	Equipo de TI
Cortes eléctricos sin respaldo	DSS04		Mitigar		UPS, plan de continuidad y pruebas periódicas de respaldo.	Equipo de TI

4.2. ANÁLISIS DE RESULTADOS

Se realizó la Calificación de Atributos de capacidad de cada uno de los procesos seleccionados de aquellos subprocesos que cumplían con la documentación mínima, donde se observó haciendo uso del gráfico de radar que algunos procesos no han alcanzado la escala de Proceso Parcialmente Alcanzado (P), esto debido a que la UNS no se encuentra en desarrollo de las Prácticas de Gobierno mínimas para el correcto Gobierno de TI. Es así como, presentamos un resumen de Escalas de todos los procesos que fueron evaluados.

N: Proceso no alcanzado

P: Proceso parcialmente alcanzado

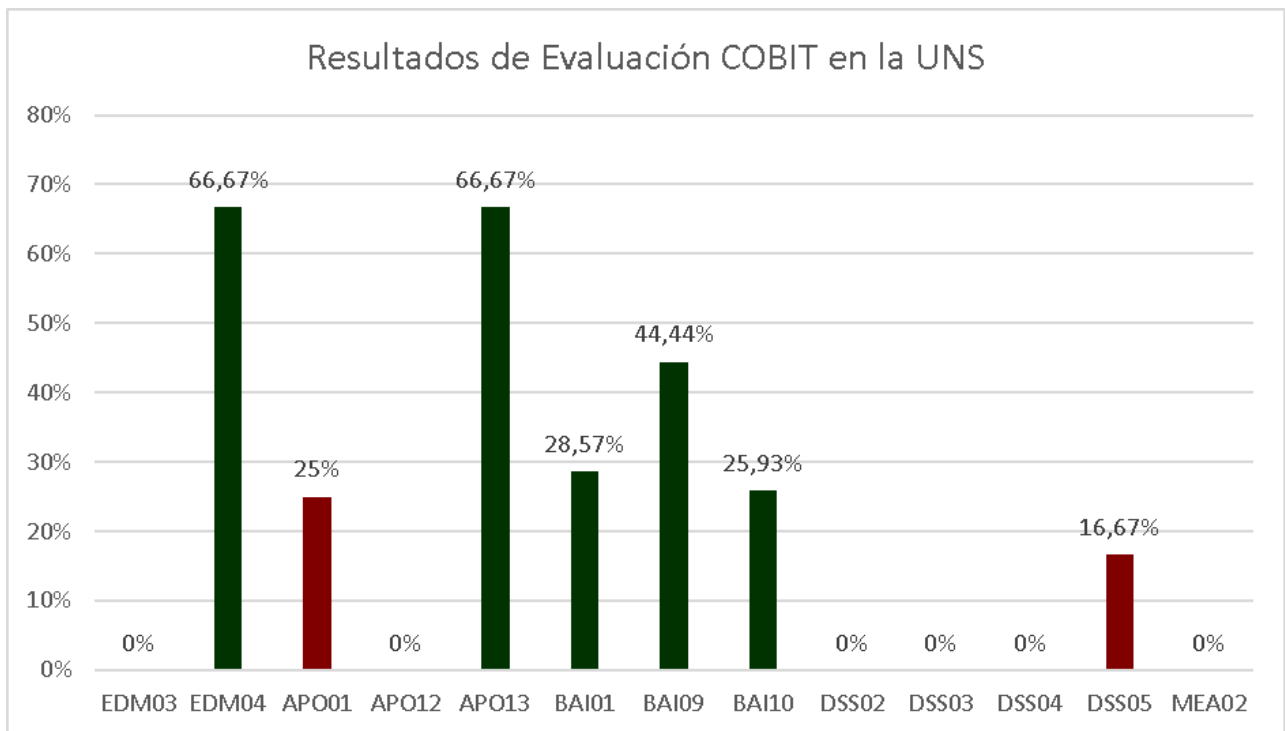
A: Proceso ampliamente alcanzado

Tabla 65*Resultados de procesos alcanzados*

Proceso	% alcanzado de la GITIC	Escala	Definición	
EDM03	0%	N	Proceso No Alcanzado	
EDM04	66.67%	P	Proceso Alcanzado	Parcialmente
APO01	25%	P	Proceso Alcanzado	Parcialmente
APO12	0%	N	Proceso No Alcanzado	
APO13	66.67%	P	Proceso Alcanzado	Parcialmente
BAI01	28.57%	P	Proceso Alcanzado	Parcialmente
BAI09	44.44%	P	Proceso Alcanzado	Parcialmente
BAI10	25.93%	P	Proceso Alcanzado	Parcialmente
DSS02	0%	N	Proceso No Alcanzado	
DSS03	0%	N	Proceso No Alcanzado	
DSS04	0%	N	Proceso No Alcanzado	
DSS05	16.67%	P	Proceso Alcanzado	Parcialmente
MEA02	0%	N	Proceso No Alcanzado	

Figura 28

Resultados de evaluación COBIT en la UNS



Se realizó la evaluación de 13 procesos de gobierno y de gestión según el Modelo COBIT, con la finalidad de gestionar los riesgos de la Oficina de Tecnología e Información. En el desarrollo se utilizó diversas herramientas de para la captura de información, dando como resultado que del 100% de los procesos evaluados, 8 procesos se encuentran en la escala de “Proceso No Alcanzado”, lo cual representa el 61.54% del total. Los procesos que obtuvieron la escala de “Proceso Parcialmente Alcanzado” fueron 5, siendo el 38.46% del total. Finalmente se observa que no existe proceso alguno que haya obtenido la escala de “Proceso Ampliamente Alcanzado”.

- En el subproceso de asegurar la optimización de recursos se alcanzó el 66,67%, obteniendo un Proceso Parcialmente Alcanzado.
- La gestión de la seguridad igualmente obtuvo un proceso parcialmente alcanzado con un 66,67%.
- La gestión de activos se encuentra en un 44,44%, evidenciando que el proceso se alcanzó parcialmente.
- En base al marco de gestión de TI, el 25% implica un proceso no alcanzado, con una limitada formalización.

4.3. DISCUSIÓN

- Con respecto a la optimización de recursos se observa con el porcentaje alcanzado que existe una buena orientación estratégica lo que aporta con la optimización de las inversiones en los recursos tecnológicos, implica que en la UNS se fortalece la sostenibilidad financiera del área de tecnología y una correcta determinación de acciones.
- Los mecanismos que protegen la información se encuentran dentro de los límites básicos para aportar con la gestión de la seguridad de la información, reduciendo las vulnerabilidades, protegiendo los datos académicos.
- Posee un nivel de inventario que implica un avance en el control y la administración de los equipos tecnológicos, además, se puede entender que en la institución se piensa en una correcta organización de los recursos tecnológicos.
- No se observa que en la universidad existe un enfoque sistemático ya que no se identifican, analizan y disminuyen los riesgos. Ello implica que aumentarán las incidencias, ciberataques y/o robos.
- El aumento de las incidencias recae en una debilidad con respecto a la gestión para resolverlos, disminuyendo el potencial de garantizar la sostenibilidad de los servicios de enseñanza.
- Con respecto al monitoreo, la UNS tiene una baja implicancia para evaluar los controles e identificar mejoras constantemente en base al desempeño de los responsables.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Se aplicó la metodología COBIT, en la que se evaluó todos los procesos obteniendo 13 relacionados con la Gestión de riesgos de TI, además, se alcanzaron 6 de ellos parcialmente.
- Aplicamos la matriz COBIT, en la que se realizó la evaluación de los procesos y subprocesos en base a la gestión de riesgos identificados como los principales que se involucran para esta metodología, mostrando los resultados haciendo uso de gráficos de radar determinando el nivel de procesos alcanzados, los procesos con mayor alcance fueron EDM04 y APO13 los cuales cuentan con un 66,67% alcanzado, y le sigue el proceso BAI09 con un 44,44% alcanzado, además, también consideramos los procesos APO01 con 25%, BAI10 con 25,93% y BAI01 con 28,57% alcanzado.
- Se identificaron trece riesgos de TI, los cuales fueron observados directamente en la institución, además, se describieron uno a uno, logrando determinar causas y consecuencias, hallando que doce de ellos son Inadmisibles, entre los cuales se encuentran los equipos obsoletos, tomacorrientes y puntos de red deteriorados, cables dañados, USB contaminados, falta de licencias de software.
- Analizamos cada riesgo para obtener la probabilidad de que cada uno suceda, obteniendo riesgos con una probabilidad muy alta de ocurrencia, lo que evidencia una clara necesidad de implementar un plan de gestión de riesgos en la institución.
- Se obtuvo el impacto de cada riesgo, de los cuales siete se encuentran en catastrófico y dos en grave, demostrando la importancia de su mitigación evitando consecuencias graves para la universidad.
- Se construyó la matriz de tratamiento al riesgo, proponiendo para cada riesgo una acción a tomar, dentro de los cuales se establecen cambios en la infraestructura dañada, reparaciones, inventarios, y la que consideramos como primordial es la implementación de cámaras de seguridad, así como, un responsable de dicha decisión.
- Se proponen acciones de mejora para una optimización de los equipos, de la infraestructura, y de la seguridad de TI en la universidad nacional del santa. Las cuales se detallaron para cada riesgo identificado, asumiendo los riesgos secundarios.

5.2. RECOMENDACIONES

- Se recomienda a la OTIC, fortalecer los procesos como la optimización del riesgo, lo que implica la implementación de la matriz de tratamiento al riesgo, asegurando la integridad de los recursos tecnológicos de la UNS.
- Los servicios de enseñanza no deben verse afectados por interrupciones de fluido eléctrico o equipos en mal estado, es por ello, que se recomienda la implementación de un plan de continuidad, lo que implica contar con respaldos frente a estas interrupciones, asegurando la calidad de la enseñanza y la información.
- Se recomienda contar con una bitácora de incidencias, así se podrán identificar a mayor detalle los puntos débiles en los recursos de TI de cada una de las aulas multimedia, además, de un correcto seguimiento y asignación de agente para la resolución de dichas fallas.
- Recomendamos realizar la asignación de roles y responsabilidades, lo que ayudará con la correcta ejecución de las actividades que implican la gestión de riesgos, tales como, el aseguramiento de los recursos tecnológicos.
- La importancia de contar con un inventario actualizado radica en una correcta gestión de activos, es así, que se recomienda esta implementación, que va de la mano con la asignación de un equipo responsable para dicha actividad, además, contar con tiempos establecidos para esta actualización.
- Se recomienda establecer las políticas de seguridad a manera de proyecto, el cual sea correctamente difundido y se observe en cada una de las aulas multimedia, asegurando que llegue a cada uno de la plana docente y población estudiantil de la universidad.
- Una de las recomendaciones más importantes es involucrar a la alta gerencia en estos procesos de mejora en la gestión de riesgos, los cuales cumplen un rol muy importante en la supervisión de estas estrategias.

Referencias Bibliográficas

- AENOR. (s.f.). *Seguridad y Privacidad de la Información: ISO 27001 e ISO 27701*.
Obtenido de Aenor: <https://www.aenor.com/certificacion/tecnologias-de-la-informacion/seguridad-informacion>
- BMC Software. (s/f). What is COBIT? COBIT explained. BMC Blogs. Recuperado el 4 de julio de 2026, de <https://www.bmc.com/blogs/COBIT/>
- Conexión Esan. (27 de Mayo de 2021). *COBIT 2019: ¿cómo beneficia a una organización?* Obtenido de Esan: <https://www.esan.edu.pe/conexion-esan/COBIT-2019-como-beneficia-a-una-organizacion>
- Esginnova Group. (15 de Junio de 2017). *ISO 27005: ¿Cómo realizar la gestión del riesgo tecnológico?* Obtenido de Esginnova Group: <https://www.pmg-ssi.com/2017/06/iso-27005-gestion-del-riesgo-tecnologico/>
- Fombona, J., & Pascual, A. (2020). *Aula Multimedia y TIC*. Obtenido de Organizaciones transparentes: <https://www.orgtransparente.uniovi.es/aula-multimedia-tic/>
- GlobalSuite Solutions. (22 de Septiembre de 2023). *¿Qué es la norma ISO 27001 y para qué sirve?* Obtenido de GlobalSuite Solutions: <https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/>
- Horvath, I. (2021, febrero 11). COBIT 5 Framework Tutorial: A principles and framework guide. Invensis Learning Blog; Invensis Learning. <https://www.invensislearning.com/blog/COBIT-5-framework-tutorial/>
- IBM. (s.f.). *¿Qué es gestión de riesgos?* Obtenido de IBM: <https://www.ibm.com/mx-es/topics/risk-management>
- Joseph, L. (2024, marzo 11). COBIT: el marco de referencia para una mejor gobernanza de los SI. Lemonlearning.com. <https://lemonlearning.com/es/blog/COBIT-gobernanza-de-ti>
- Martínez, A. (8 de Marzo de 2024). *Definición de Gestión*. Obtenido de ConceptoDefinición: <https://conceptodefinicion.de/gestion/>
- Osteicoechea, A. (14 de Junio de 2023). *Definición de Universidad*. Obtenido de ConceptoDefinicion: <https://conceptodefinicion.de/universidad/>

- Pachón, C. (6 de Febrero de 2024). *Departamento de TI: protagonismo evidente que ha tomado en empresas*. Obtenido de nsit: <https://www.nsit.com.co/departamento-de-ti-el-protagonismo-evidente-que-ha-tomado-en-las-empresas/>
- Perfil, V. T. mi. (s/f). COBIT. Blogspot.com. Recuperado el 4 de julio de 2026, de <https://COBITmmatiasc.blogspot.com/2017/03/dominios-y-procesos-de-COBIT.html>
- Por qué la gestión de riesgos es importante para las organizaciones*. (15 de Enero de 2024). Obtenido de Safety Culture: <https://safetyculture.com/es/temas/gestion-de-riesgos/>
- Rama Judicial. (2018). *Norma Internacional ISO 31000*. Obtenido de ramajudicial: <https://www.ramajudicial.gov.co/documents/5454330/14491339/Norma.ISO.31000.2018.Espanol.pdf/cb482b2c-afd9-4699-b409-0732a5261486>
- Real Academia Española. (2023). *Aplicación*. Obtenido de Real Academia Española : <https://dle.rae.es/aplicaci%C3%B3n>
- Riveros, A. (25 de Junio de 2020). *Qué es la norma ISO 31000 y para qué sirve*. Obtenido de Ealde: <https://www.ealde.es/iso-31000-para-que-sirve/>
- Universidad Nacional del Santa. (3 de Junio de 2022). *Plan Estrategico Institucional*. Obtenido de https://www.uns.edu.pe/archivos/276_modelo_educativo_uns_2017.pdf
- ¿Qué es el marco COBIT?* (s/f). Fortinet. Recuperado el 4 de julio de 2026, de <https://www.fortinet.com/lat/resources/cyberglossary/what-is-COBIT>