ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Evaluación Tecnológica de Gobierno y Gestión de TI en banco BanCodesarrollo mediante los dominios Evaluar/Orientar/Supervisar, Alinear/Planear/Organizar y Supervisar/Evaluar/Valorar de Cobit5.

Maestrantes:

Ing. Gerardo Cajamarca Méndez.

Ing. Daniel Guerrón Benalcázar.

Tutor:

Ing. Giovanni Ron Gavi Mgs.

banCODESARROLLO
Invertimos en Humanidad

CONTENIDO:

- Resumen.
- Objetivo General.
- Objetivos Específicos.
- Resumen de Cobit 5.
- Metodología.
- Evaluación y Hallazgos.
- Conclusiones.
- Recomendaciones.

RESUMEN:

- BanCodesarrollo tras contar con una importante trayectoria en el Sistema Cooperativo Nacional se constituyó como banco en febrero 2014, tornando indispensable que la institución considere y adopte todos los lineamientos de carácter normativo, orientados a cumplir con las regulaciones y administrar de manera integral sus riesgos tecnológicos.

- Este proyecto evaluará técnicamente a BanCodesarrollo empleando principalmente el Marco de Referencia de Gobierno y Gestión de TI Cobit5® (Dominios: EDM, APO, MEA).

- La evaluación técnica busca conocer el gobierno y gestión de TI, observar el impacto de los riesgos tecnológicos, valorando controles y midiendo su efectividad, en procura de minimizar la afectación sobre los activos de tecnología.

OBJETIVO GENERAL

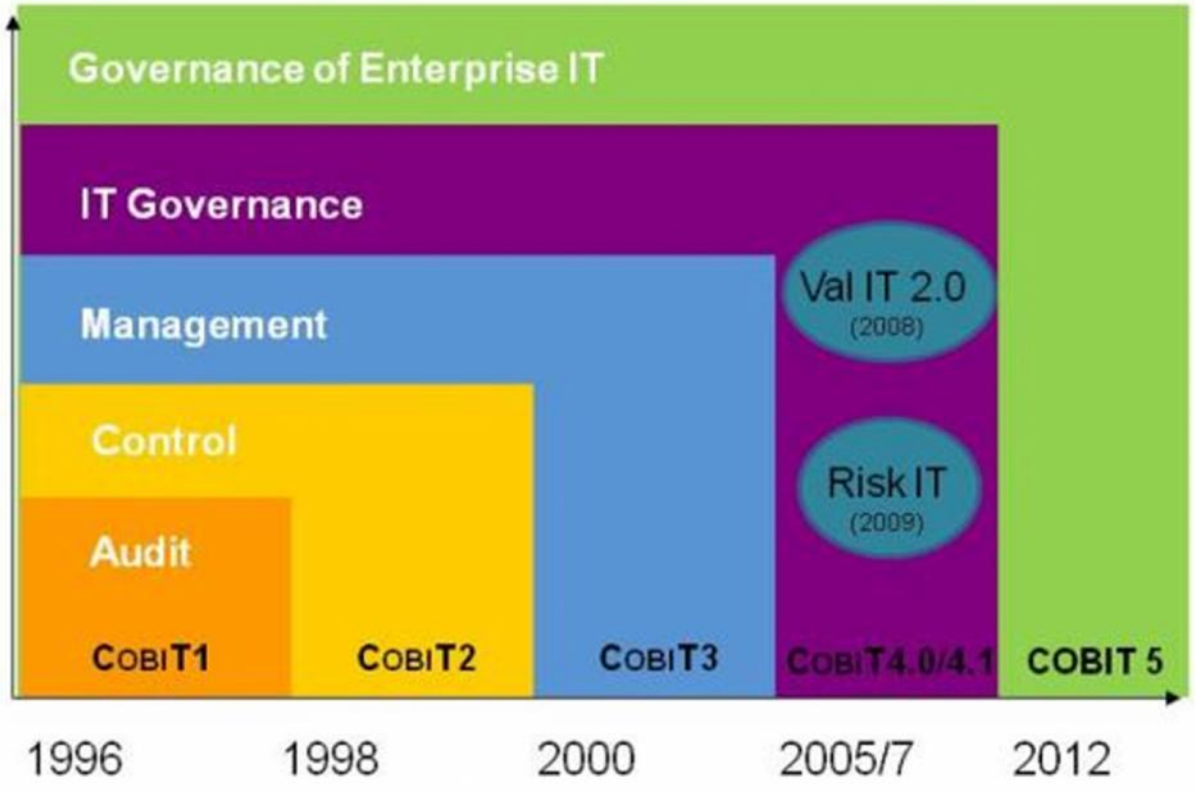
- Evaluar tecnológicamente a banco BanCodesarrollo, empleando principalmente el Marco de referencia para los Objetivos de Control y Tecnología Relacionada Cobit5® en el ámbito de los dominios Evaluar/Orientar/Supervisar, Alinear/Planear/Organizar y Supervisar/Evaluar/Valorar para tener un entendimiento detallado del gobierno y gestión de TI.

OBJETIVOS ESPECÍFICOS:

- Determinar el nivel de implementación de gobierno y gestión de TI de banco BanCodesarrollo.
- Valorar los controles que se han implementado y determinar en base al análisis de riesgos su afectación al banco.
- Emitir recomendaciones orientadas a fortalecer el gobierno y gestión de TI.
- Ayudar al banco BanCodesarrollo a robustecer el gobierno y gestión de TI, mediante la optimización de los niveles de riesgo y el uso de recursos tecnológicos.

COBIT 5.0

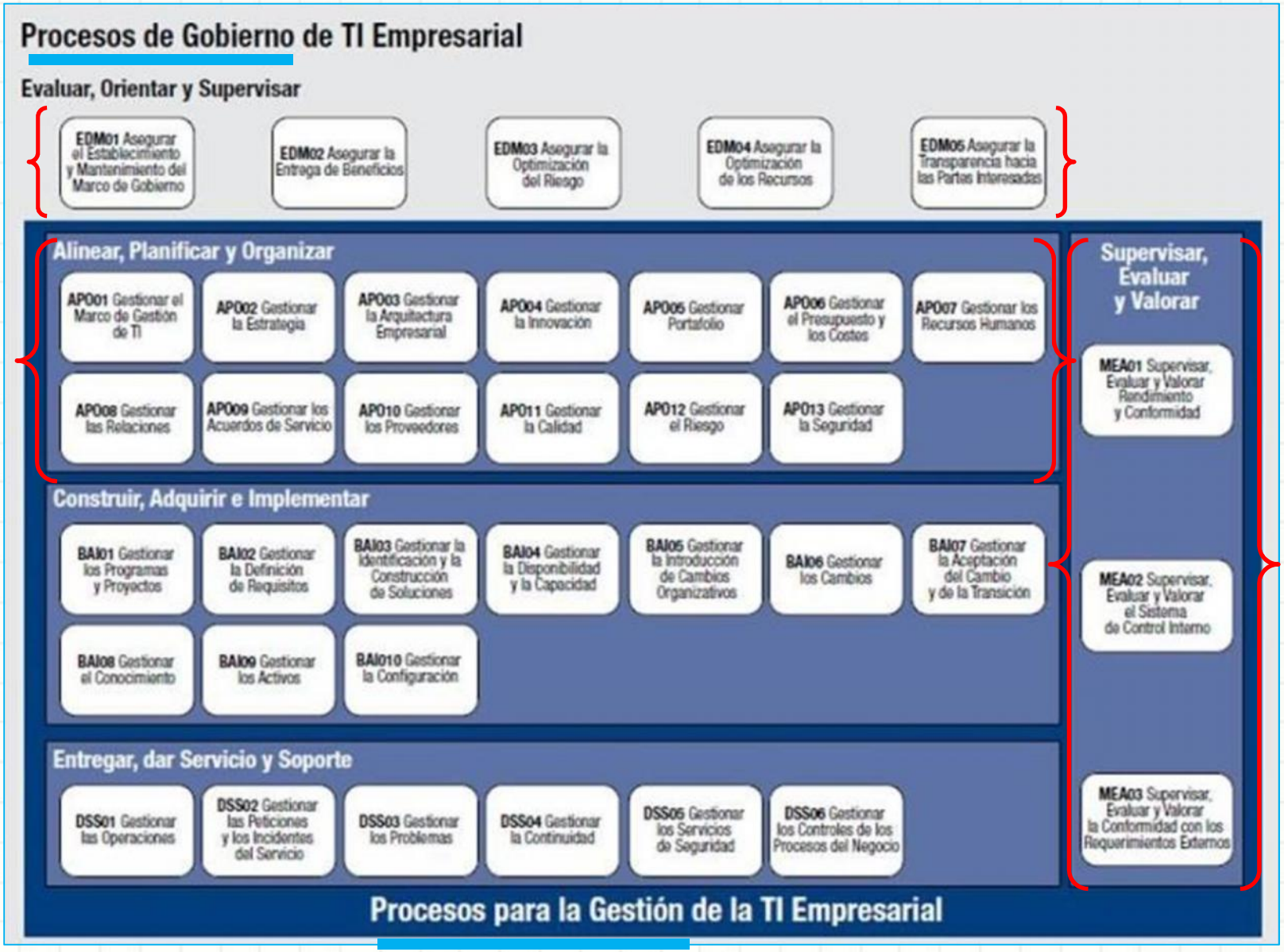
Cobit 5® es un marco de trabajo integral creado por ISACA con el objeto de ayudar a las empresas a alcanzar sus objetivos para el gobierno y gestión de tecnologías corporativas, este marco busca mantener el equilibrio entre la generación de beneficios, optimización de los niveles de riesgo y el uso de recursos.



(ISACA, 2014)

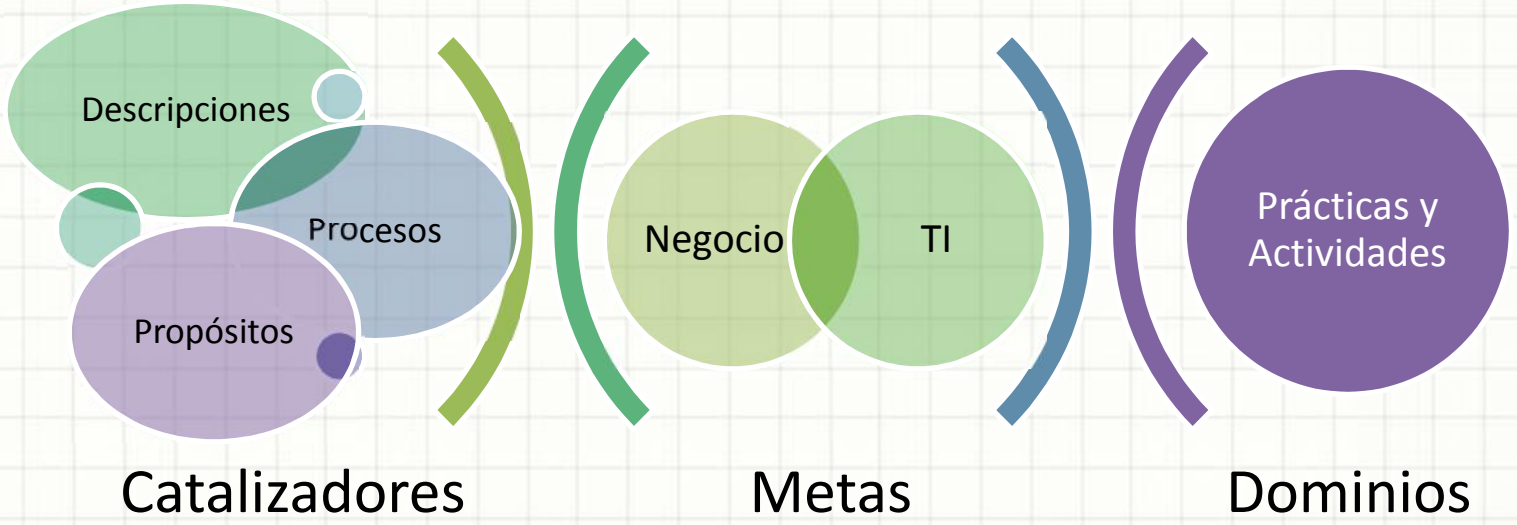
PRINCIPIOS DE COBIT 5®

PROCESOS DE COBIT 5®:



MARCO METODOLÓGICO:

Se ha empleado el marco de referencia COBIT 5, la metodología de evaluación considera el documento Procesos Catalizadores de Cobit 5.



MARCO METODOLÓGICO:

Evaluación.- hace referencia a la situación de aplicabilidad de COBIT 5 dentro de BanCodesarrollo. Por lo que se le ha asignado el peso de dos (2) puntos cuando se aplica y cero (0) cuando no se lo hace.

Cobertura.- se refiere al nivel de profundidad en la ejecución de las actividades sugeridas por COBIT 5. Para lo que se han establecido tres niveles de cobertura: Completa a la que le corresponde un peso de dos y medio (2.5) puntos, Parcial a la que se califica con uno punto setenta y cinco (1,75) y Nula a la que se le concede cero (0) puntos.

Evaluación	Valor
Aplica	2
No Aplica	0

Cobertura	Valor
Completa	2,5
Parcial	1,75
Nula	0

El producto de los dos criterios (Evaluación*Cobertura) daría lugar a un puntaje mínimo de cero (0) y el máximo de cinco (5).

MARCO METODOLÓGICO:

El límite mínimo aceptable de esta evaluación es de tres (3) puntos, cualquier resultado inferior a este será analizado con profundidad, a consecuencia de su baja aplicación y cobertura.

La evaluación se complementa con el análisis de riesgo basado en dos aspectos:

Procesos COBIT de Riesgo:

- APO13 Gestionar el Riesgo.
- EDM03 Asegurar la Optimización del Riesgo.

Controles Implementados: La naturaleza del negocio de BanCodesarrollo conlleva a mantener reserva respecto de la información que pueda ser divulgada, sin embargo es indispensable conocer los controles implementados para gestionar los riesgos.

PLANTILLA COBIT:

Tabla 3
Plantilla para el proceso EDM02

Código:	EDM02	**Area:**	Gobierno
Proceso:	Asegurar la Entrega de Beneficios	**Dominio:**	Evaluar, Orientar y Supervisar
Descripción del Proceso:			
Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costes aceptables.			
Declaración del Propósito del Proceso:			
Asegurar un valor óptimo de las iniciativas de TI, servicios y activos disponibles; una entrega coste eficiente de los servicios y soluciones y una visión confiable y precisa de los costes y de los beneficios probables de manera que las necesidades del negocio sean soportadas efectiva y eficientemente.			
El proceso apoya la consecución de un conjunto de principales metas TI:			
Meta TI	Métricas relacionadas		
01 Alineamiento de TI y estrategia de negocio.	• Porcentaje de metas estratégicas y requerimientos corporativos apoyados por metas TI estratégicas. • Nivel de satisfacción de los interesados con el alcance del portfolio de programas y servicios planificado. • Porcentaje de factores de valor TI mapeados a factores de valor del negocio.		
05 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI.	• Porcentaje de inversiones TI donde la obtención del beneficio se supervisa a lo largo de todo el ciclo de vida económico. • Porcentaje de servicios TI donde se obtienen los beneficios esperados. • Porcentaje de inversiones TI donde se cumplen o exceden los beneficios esperados.		
06 Transparencia de los costes, beneficios y riesgos de las TI.	• Porcentaje de casos de negocio de inversiones TI con costes TI y beneficios esperados claramente definidos y aprobados. • Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados • Encuesta de satisfacción de interesados clave en relación con el nivel de transparencia, comprensión y precisión de información financiera TI		

PLANTILLA COBIT:

07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	• Número de interrupciones de negocio debidas a incidentes de servicios TI • Porcentaje de partes interesadas en el negocio satisfechas de que la entrega de servicios TI cumpla los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de la entrega de servicios TI
17 Conocimiento, experiencia e iniciativas para la innovación de negocio.	• Nivel de concienciación y comprensión de la alta dirección del negocio sobre las posibilidades de innovación TI. • Nivel de satisfacción de los interesados con los niveles de experiencia e ideas de innovación de TI. • Número de iniciativas aprobadas resultantes de ideas TI innovadoras.

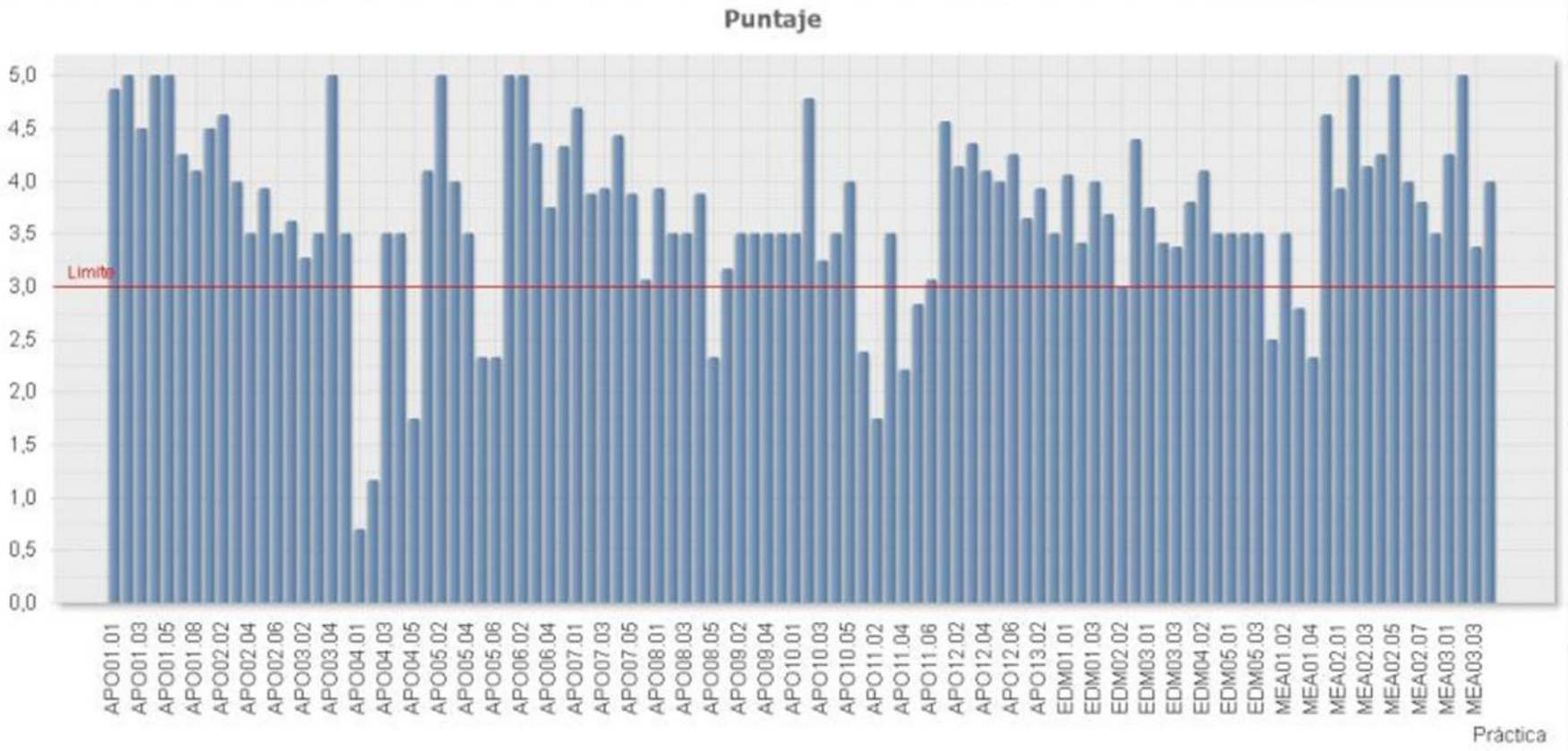
Prácticas y Actividades

EDM02.01	Evaluar la optimización de valor.	Evaluar continuamente las inversiones, servicios y activos del portafolio de TI para determinar la probabilidad de alcanzar los objetivos de la empresa y aportar valor a un coste razonable. Identificar y juzgar cualquier cambio en la dirección que necesita ser dada a la gestión para optimizar la creación de valor.	3.69

Actividad	Evaluación	Cobertura	Calificación
1. Comprender los requerimientos de las partes interesadas; temas estratégicos de TI, tales como la dependencia de las TI; y comprender la tecnología y sus capacidades considerando la importancia actual y potencial de TI para la estrategia de la empresa.	Aplica	Parcial	3.5
2. Comprender los elementos clave de gobierno necesarios para la entrega fiable, segura y coste efectiva de un valor óptimo por el uso de los servicios, activos y recursos de TI existentes y potenciales.	Aplica	Completa	5
3. Comprender y discutir regularmente las oportunidades que podrían surgir de los cambios habilitados en la empresa por las tecnologías actuales, nuevas o emergentes y optimizar el valor creado por estas oportunidades.	Aplica	Parcial	3.5
4. Comprender lo que se entiende por valor en la empresa y considerar cómo de bien se ha comunicado, comprendido y aplicado a través de los procesos de la empresa.	Aplica	Parcial	3.5

EVALUACIÓN Y HALLAZGOS:

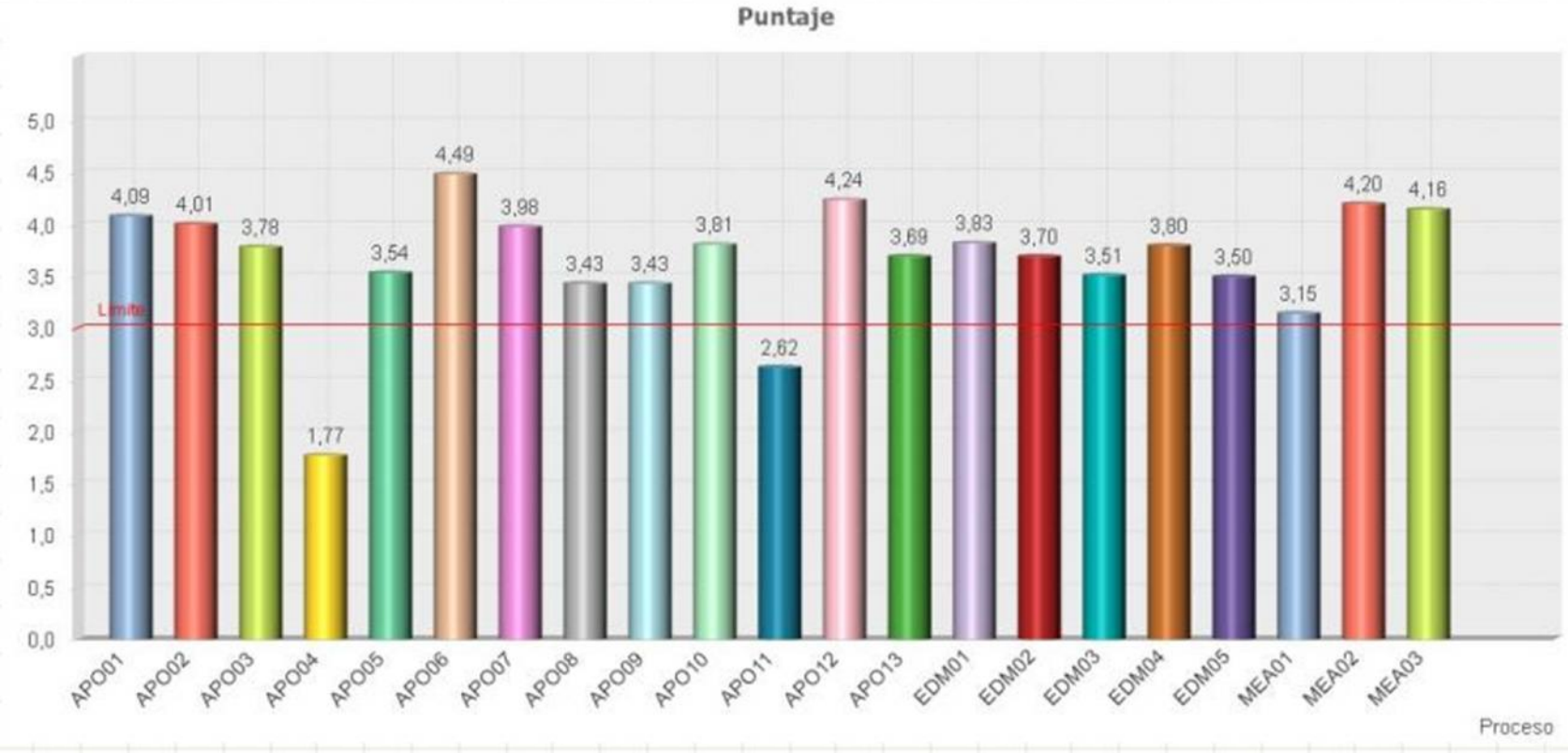
Luego de haber consolidado las matrices se obtiene el resultado de la evaluación en BanCodesarrollo para cada una de las prácticas de los procesos catalizadores, tanto en el ámbito de gobierno como en el ámbito de gestión de TI.



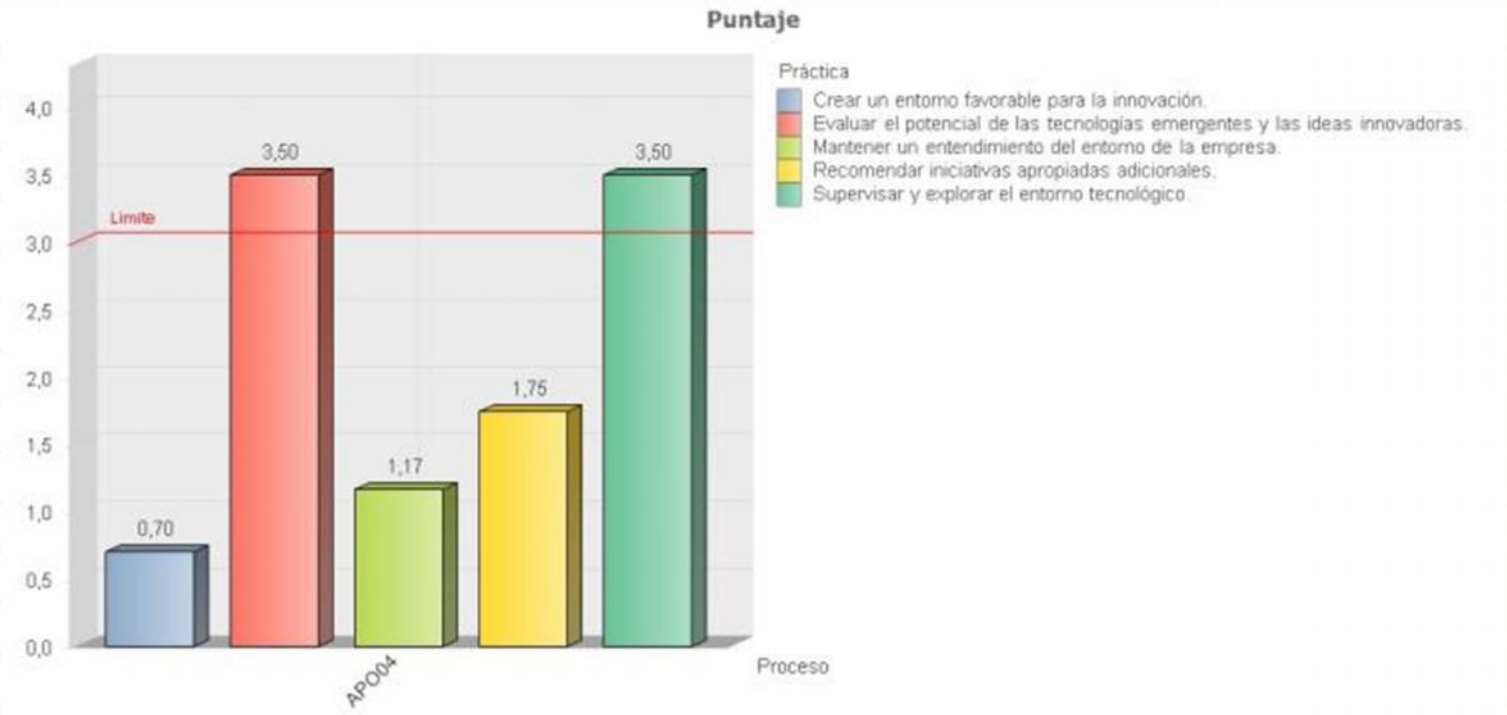
EVALUACIÓN Y HALLAZGOS:

BanCodesarrollo alcanza un promedio general de 73,17% de aplicación de COBIT 5.

Resultados de la evaluación a nivel de procesos:

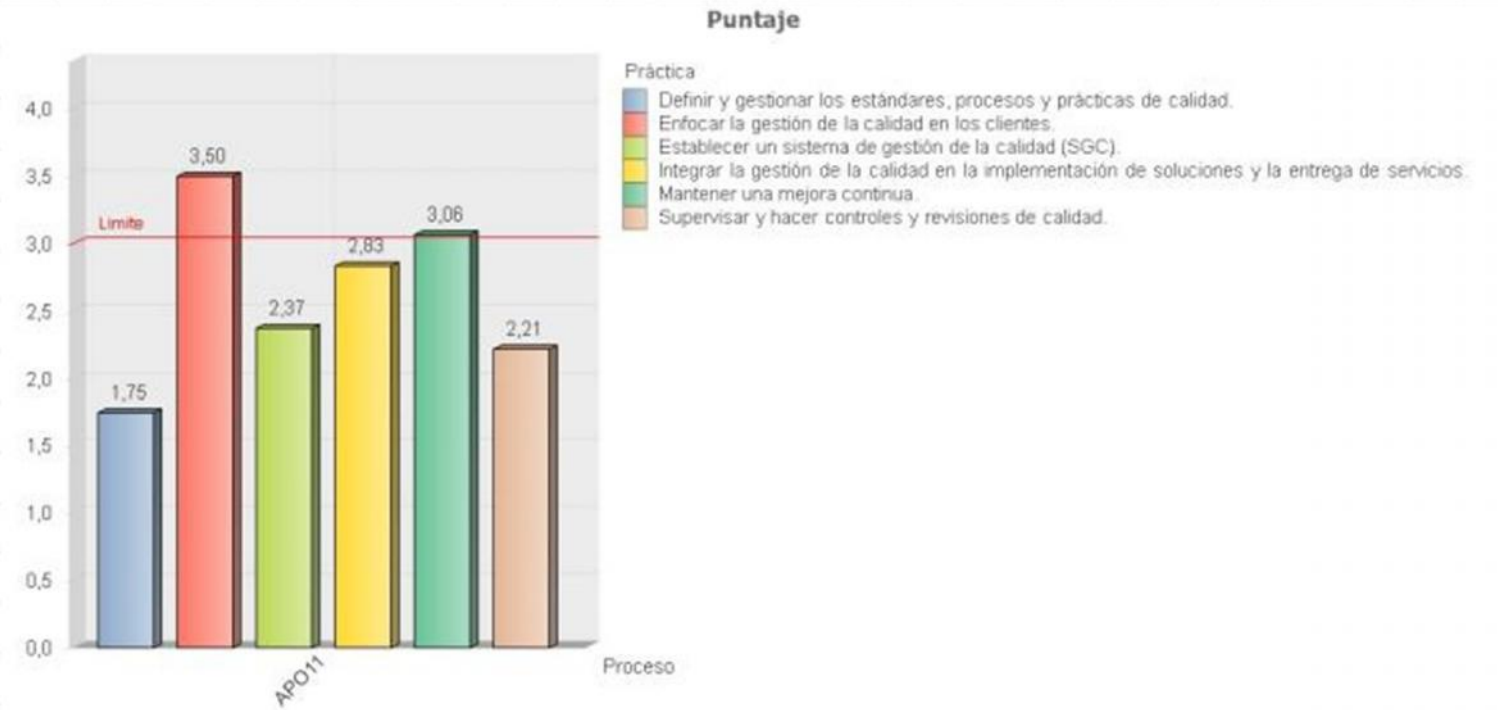


EVALUACIÓN Y HALLAZGOS:



APO04 Gestionar la Innovación: Tiene que ver con prácticas en las cuales la empresa identifique sus necesidades, genere estrategias que promuevan la investigación e innovación, sugiriendo emprender en iniciativas que propicien la implementación, uso y supervisión de la innovación, de manera que genere desarrollo y competitividad en el negocio.

EVALUACIÓN Y HALLAZGOS:



APO11 Gestionar la Calidad: Obedece a prácticas que requieran fortalecer el Sistema de Gestión de Calidad, lo que se podría alcanzar con el diseño, implementación y mejora continua de procesos donde se cuide la calidad en la implementación de soluciones y la entrega de servicios.

CONCLUSIONES:

1._ Tras tener un entendimiento global del negocio en BanCodesarrollo, entrevistar a personal clave, revisar la información proporcionada, validar la existencia y consistencia de la evidencia y finalmente evaluar a profundidad las actividades y prácticas relacionadas con TI se concluye que BanCodesarrollo lleva a cabo sus prácticas de gobierno y gestión de TI alineadas a COBIT 5 para los dominios Evaluar, Orientar y Supervisar (EDM); Alinear, Planear y Organizar (APO) y Supervisar, Evaluar y Valorar (MEA).

2._ La aplicación de la herramienta de trabajo denominada "Plantilla Cobit" junto con el marco metodológico empleado para esta evaluación tecnológica han revelado que BanCodesarrollo tiene un nivel de alineamiento de 73.17% a COBIT 5.

CONCLUSIONES:

3._ Se pudo determinar que el gobierno y gestión de tecnología de información en esta institución se alinea a marcos de referencia y buenas prácticas, puntualmente COBIT 5, no obstante que la institución aún no haya manifestado formalmente su decisión de adoptarlo.

4._ La focalización en procesos de incidencia directa a riesgos, reflejó que se consideran adecuadamente los lineamientos para administración y gestión de riesgo en BanCodesarrollo, como lo refleja el puntaje de 3.51/5 para el proceso EDM03 Asegurar la Optimización del Riesgo y 4.24/5 para el proceso APO12 Gestionar el Riesgo. Pese a que la institución no permitió se revelen a detalle los controles, se ha identificado la implementación de estos en varias áreas de BanCodesarrollo que aportan sustancialmente a la gestión de riesgo, sin que eso signifique que no puedan ser reevaluados y validados periódicamente para perfeccionarlos.

CONCLUSIONES:

5._ Del análisis de resultados obtenidos para actividades, prácticas, procesos y dominios se establece que BanCodesarrollo podría fortalecer su gobierno y gestión de TI, en todos los procesos, con mayor intensidad en dos de ellos que presentan puntuación baja, estos es: APO04 Gestionar la Innovación con 1.77/5 y APO11 Gestionar la Calidad con 2.62/5, debido a que no se llevan a cabo las actividades y prácticas relacionadas con la profundidad que el marco de referencia sugiere.

RECOMENDACIONES:

1._ Partiendo del nivel alineamiento identificado se sugiere la adopción del marco de trabajo COBIT 5® en BanCodesarrollo puesto que así no solo formalizaría sus prácticas sino también fortalecería su gobierno y gestión de TI, lo que en consecuencia le permitiría alcanzar adaptabilidad a buenas prácticas de la industria, el entendimiento y cumplimiento de resoluciones, disposiciones y recomendaciones emanadas por el ente de control. Encaminando firmemente los esfuerzos para que el negocio afiance sus resultados y asegure su permanencia en el mercado, muy de la mano del uso adecuado de las tecnologías de información.

RECOMENDACIONES:

2._ Con base en los hallazgos se recomienda a BanCodesarrollo analizar su estructura organizacional con la finalidad de que se adapte de mejor manera a las prácticas de COBIT 5 en lo referente a:

- Levantamiento e implementación de procesos, definición y seguimiento de métricas que facilite el cumplimiento tanto de metas del negocio y metas relacionadas con TI. (Área de procesos y planificación, SGC).

- Diseño de procesos y roles para llevar a cabo actividades de innovación, gestión de proyectos y análisis de la capacidad.

RECOMENDACIONES:

3._ Se recomienda emprender en un proyecto integral para implementación de COBIT 5® en la medida que le sea factible, prestando especial atención a actividades importantes como:

- Análisis, gestión y aprobación de un presupuesto para capacitación al personal en materia de COBIT 5.
- Determinación de una hoja de ruta para implementación progresiva que sea incorporada a la Planificación Estratégica Institucional.

4._ Toda vez que se cuente con experiencia en la aplicación de COBIT 5® sería ideal realizar la medición del nivel madurez y capacidad de los procesos, lo que consecuentemente elevaría los niveles de gestión integral de riesgo en BanCodesarrollo.

RECOMENDACIONES:

5._ Por último es importante realizar un estudio de la carga de trabajo, estructura y procesos en TI, con la finalidad de determinar si el personal es suficiente para cumplir con los objetivos de la institución y planificación estratégica de tecnología considerando que BanCodesarrollo recientemente está participando como banco en el sistema financiero nacional.

RESULTADOS POR PRÁCTICA:

Proceso	Práctica	Nombre	Evaluación
EDM01	EDM01.01	Evaluar el sistema de gobierno.	4,06
EDM01	EDM01.02	Orientar el sistema de gobierno.	3,42
EDM01	EDM01.03	Supervisar el sistema de gobierno.	4,00
EDM02	EDM02.01	Evaluar la optimización de valor.	3,69
EDM02	EDM02.02	Orientar la optimización del valor.	3,00
EDM02	EDM02.03	Supervisar la optimización de valor.	4,40
EDM03	EDM03.01	Evaluar la gestión de riesgos.	3,75
EDM03	EDM03.02	Orientar la gestión de riesgos.	3,42
EDM03	EDM03.03	Supervisar la gestión de riesgos.	3,38
EDM04	EDM04.01	Evaluar la gestión de recursos.	3,80
EDM04	EDM04.02	Orientar la gestión de recursos.	4,10
EDM04	EDM04.03	Supervisar la gestión de recursos.	3,50
EDM05	EDM05.01	Evaluar los requisitos de elaboración de informes de las partes interesadas.	3,50
EDM05	EDM05.02	Orientar la comunicación con las partes interesadas y la elaboración de informes.	3,50
EDM05	EDM05.03	Supervisar la comunicación con las partes interesadas.	3,50

Proceso	Práctica	Nombre	Evaluación
MEA01	MEA01.01	Establecer un enfoque de la supervisión.	2,50
MEA01	MEA01.02	Establecer los objetivos de cumplimiento y rendimiento.	3,50
MEA01	MEA01.03	Recopilar y procesar los datos de cumplimiento y rendimiento.	2,80
MEA01	MEA01.04	Analizar e informar sobre el rendimiento.	2,33
MEA01	MEA01.05	Asegurar la implantación de medidas correctivas.	4,63
MEA02	MEA02.01	Supervisar el control interno.	3,93
MEA02	MEA02.02	Revisar la efectividad de los controles sobre los procesos de negocio.	5,00
MEA02	MEA02.03	Realizar autoevaluaciones de control.	4,14
MEA02	MEA02.04	Identificar y comunicar las deficiencias de control.	4,25
MEA02	MEA02.05	Garantizar que los proveedores de aseguramiento son independientes y están cualificados.	5,00
MEA02	MEA02.06	Planificar iniciativas de aseguramiento.	4,00
MEA02	MEA02.07	Estudiar las iniciativas de aseguramiento.	3,80
MEA02	MEA02.08	Ejecutar las iniciativas de aseguramiento.	3,50
MEA03	MEA03.01	Identificar requisitos externos de cumplimiento.	4,25
MEA03	MEA03.02	Optimizar la respuesta a requisitos externos.	5,00
MEA03	MEA03.03	Confirmar el cumplimiento de requisitos externos.	3,38
MEA03	MEA03.04	Obtener garantía del cumplimiento de requisitos externos.	4,00

RESULTADOS POR PRÁCTICA:

Proceso	Práctica	Nombre	Evaluación
APO01	APO01.01	Definir la estructura organizativa	4,88
APO01	APO01.02	Establecer roles y responsabilidades	5,00
APO01	APO01.03	Mantener los elementos catalizadores del sistema de gestión	4,50
APO01	APO01.04	Comunicar los objetivos y la dirección de gestión	5,00
APO01	APO01.05	Optimizar la ubicación de la función de TI	5,00
APO01	APO01.06	Definir la propiedad de la información (datos) y del sistema	4,25
APO01	APO01.07	Gestionar la mejora continua de los procesos	0,00
APO01	APO01.08	Mantener el cumplimiento con las políticas y procedimientos	4,10
APO02	APO02.01	Comprender la dirección de la empresa.	4,50
APO02	APO02.02	Evaluar el entorno, capacidades y rendimiento actuales.	4,63
APO02	APO02.03	Definir el objetivo de las capacidades de TI	4,00
APO02	APO02.04	Realizar un análisis de diferencias.	3,50
APO02	APO02.05	Definir el plan estratégico y la hoja de ruta.	3,93
APO02	APO02.06	Comunicar la estrategia y la dirección de TI.	3,50
APO03	APO03.01	Desarrollar la visión de la arquitectura de empresa.	3,63
APO03	APO03.02	Definir la arquitectura de referencia.	3,28
APO03	APO03.03	Seleccionar las oportunidades y las soluciones.	3,50
APO03	APO03.04	Definir la implantación de la arquitectura.	5,00
APO03	APO03.05	Proveer los servicios de arquitectura empresarial.	3,50
APO04	APO04.01	Crear un entorno favorable para la innovación.	0,70
APO04	APO04.02	Mantener un entendimiento del entorno de la empresa.	1,17
APO04	APO04.03	Supervisar y explorar el entorno tecnológico.	3,50
APO04	APO04.04	Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras.	3,50
APO04	APO04.05	Recomendar iniciativas apropiadas adicionales.	1,75
APO04	APO04.06	Supervisar la implementación y el uso de la innovación.	0,00
APO05	APO05.01	Establecer la mezcla del objetivo de inversión.	4,10
APO05	APO05.02	Determinar la disponibilidad y las fuentes de fondos.	5,00
APO05	APO05.03	Evaluar y seleccionar los programas a financiar.	4,00
APO05	APO05.04	Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones.	3,50
APO05	APO05.05	Mantener los portafolios.	2,33
APO05	APO05.06	Gestionar la consecución de beneficios.	2,33
APO06	APO06.01	Gestionar las finanzas y la contabilidad.	5,00
APO06	APO06.02	Priorizar la asignación de recursos.	5,00
APO06	APO06.03	Crear y mantener presupuestos.	4,36
APO06	APO06.04	Modelar y asignar costes.	3,75
APO06	APO06.05	Gestionar costes.	4,33
APO07	APO07.01	Mantener la dotación de personal suficiente y adecuada.	4,70
APO07	APO07.02	Identificar personal clave de TI.	3,88
APO07	APO07.03	Mantener las habilidades y competencias del personal.	3,93
APO07	APO07.04	Evaluar el desempeño laboral de los empleados.	4,44
APO07	APO07.05	Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio.	3,88
APO07	APO07.06	Gestionar el personal contratado.	3,06

Proceso	Práctica	Nombre	Evaluación
APO08	APO08.01	Entender las expectativas del negocio.	3,93
APO08	APO08.02	Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio.	3,50
APO08	APO08.03	Gestionar las relaciones con el negocio.	3,50
APO08	APO08.04	Coordinar y comunicar.	3,88
APO08	APO08.05	Proveer datos de entrada para la mejora continua de los servicios.	2,33
APO09	APO09.01	Identificar servicios TI.	3,17
APO09	APO09.02	Catalogar servicios basados en TI.	3,50
APO09	APO09.03	Definir y preparar acuerdos de servicio.	3,50
APO09	APO09.04	Supervisar e informar de los niveles de servicio.	3,50
APO09	APO09.05	Revisar acuerdos de servicio y contratos.	3,50
APO10	APO10.01	Identificar y evaluar las relaciones y contratos con proveedores.	3,50
APO10	APO10.02	Seleccionar proveedores.	4,79
APO10	APO10.03	Gestionar contratos y relaciones con proveedores.	3,25
APO10	APO10.04	Gestionar el riesgo en el suministro.	3,50
APO10	APO10.05	Supervisar el cumplimiento y el rendimiento del proveedor.	4,00
APO11	APO11.01	Establecer un sistema de gestión de la calidad (SGC).	2,38
APO11	APO11.02	Definir y gestionar los estándares, procesos y prácticas de calidad.	1,75
APO11	APO11.03	Enfocar la gestión de la calidad en los clientes.	3,50
APO11	APO11.04	Supervisar y hacer controles y revisiones de calidad.	2,21
APO11	APO11.05	Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.	2,83
APO11	APO11.06	Mantener una mejora continua.	3,06
APO12	APO12.01	Recopilar datos.	4,57
APO12	APO12.02	Analizar el riesgo.	4,14
APO12	APO12.03	Mantener un perfil de riesgo.	4,36
APO12	APO12.04	Expresar el riesgo.	4,10
APO12	APO12.05	Definir un portafolio de acciones para la gestión de riesgos.	4,00
APO12	APO12.06	Responder al riesgo.	4,25
APO13	APO13.01	Establecer y mantener un SGSI.	3,64
APO13	APO13.02	Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	3,93
APO13	APO13.03	Supervisar y revisar el SGSI.	3,50

VALORACIÓN DE CRITERIOS:

Proceso	Práctica	Nombre	Documentación analizada.
EDM01	EDM01.01	Evaluar el sistema de gobierno.	Prácticas de Gobierno Corporativo (Análisis del Entorno). Planificación Estratégica de TI. Planificación Estratégica Institucional. Políticas de Institución. Estructura Organizacional. Código de Ética. Políticas de Cumplimiento.
	EDM01.02	Orientar el sistema de gobierno.	
	EDM01.03	Supervisar el sistema de gobierno.	
EDM02	EDM02.01	Evaluar la optimización de valor.	Planificación Estratégica de TI. Planificación Estratégica Institucional. Presupuestos. Entrevista. Evaluación de desempeño, cumplimiento de planes operativos y estratégicos.
	EDM02.02	Orientar la optimización del valor.	
	EDM02.03	Supervisar la optimización de valor.	
EDM03	EDM03.01	Evaluar la gestión de riesgos.	Cumplimento de resoluciones. Entrevista. Manual de Administración Integral de Riesgos. Análisis BIA. Políticas y procedimientos de Riesgos. Plan de Contingencias de TI. Evaluación de riesgos. Actas de Comité de Riesgos.
	EDM03.02	Orientar la gestión de riesgos.	
	EDM03.03	Supervisar la gestión de riesgos.	
EDM04	EDM04.01	Evaluar la gestión de recursos.	Políticas y procedimientos de TI. Planificación Estratégica de TI. Manual de Funciones. Nómina de TI. Entrevista. Bitácoras de operación. Informes de desempeño.
	EDM04.02	Orientar la gestión de recursos.	
	EDM04.03	Supervisar la gestión de recursos.	
EDM05	EDM05.01	Evaluar los requisitos de elaboración de informes de las partes interesadas.	Políticas y procedimientos de TI. Políticas y procedimientos institucionales. Entrevista. Manual de Funciones.
	EDM05.02	Orientar la comunicación con las partes interesadas y la elaboración de informes.	
	EDM05.03	Supervisar la comunicación con las partes interesadas.	

VALORACIÓN DE CRITERIOS:

APO01	APO01.01	Definir la estructura organizativa	Estructura Organizacional. Manual de Funciones. Políticas y procedimientos administrativas. Políticas y procedimientos de TI. Entrevista. Funciones del Comité de TI. Evaluación de desempeño. Cumplimiento de resoluciones. Plan de continuidad del negocio. Planificación Estratégica y de TI. Plataforma de TI. Inventario de hardware y software.
	APO01.02	Establecer roles y responsabilidades	
	APO01.03	Mantener los elementos catalizadores del sistema de gestión	
	APO01.04	Comunicar los objetivos y la dirección de gestión	
	APO01.05	Optimizar la ubicación de la función de TI	
	APO01.06	Definir la propiedad de la información (datos) y del sistema	
	APO01.07	Gestionar la mejora continua de los procesos	
	APO01.08	Mantener el cumplimiento con las políticas y procedimientos	
APO02	APO02.01	Comprender la dirección de la empresa.	Planificación Estratégica de TI. Planificación Estratégica Institucional. Entrevista. Evaluación de desempeño, cumplimiento de planes operativos y estratégicos. Análisis del Entorno. Políticas y procedimientos. Análisis de riesgos. Plataforma de TI. Planes operativos.
	APO02.02	Evaluar el entorno, capacidades y rendimiento actuales.	
	APO02.03	Definir el objetivo de las capacidades de TI	
	APO02.04	Realizar un análisis de diferencias.	
	APO02.05	Definir el plan estratégico y la hoja de ruta.	
	APO02.06	Comunicar la estrategia y la dirección de TI.	
APO03	APO03.01	Desarrollar la visión de la arquitectura de empresa.	Planificación Estratégica Institucional y de TI. Plataforma de TI. Análisis del Entorno. Presupuesto de TI. Plan de Contingencias de TI. Manuales de usuario. Inventario de hardware y software. Diccionario de datos. Entrevista. Requerimientos normativos. Seguimiento de proyectos de TI. Portafolio de Servicios de TI. Comité de TI.
	APO03.02	Definir la arquitectura de referencia.	
	APO03.03	Seleccionar las oportunidades y las soluciones.	
	APO03.04	Definir la implantación de la arquitectura.	
	APO03.05	Proveer los servicios de arquitectura empresarial.	

VALORACIÓN DE CRITERIOS:

APO04	APO04.01	Crear un entorno favorable para la innovación.	Planificación Estratégica Institucional y de TI. Análisis del Entorno. Plan de Capacitación de TI. Entrevista. Plataforma de TI. Comité de TI.
	APO04.02	Mantener un entendimiento del entorno de la empresa.	
	APO04.03	Supervisar y explorar el entorno tecnológico.	
	APO04.04	Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras.	
	APO04.05	Recomendar iniciativas apropiadas adicionales.	
	APO04.06	Supervisar la implementación y el uso de la innovación.	
APO05	APO05.01	Establecer la mezcla del objetivo de inversión.	Planificación Estratégica de TI. Presupuesto de TI. Inventario de hardware y software. Presupuesto Institucional. Seguimiento del plan operativo. Proyectos de TI. Evaluación de desempeño. Políticas y procedimientos de TI.
	APO05.02	Determinar la disponibilidad y las fuentes de fondos.	
	APO05.03	Evaluar y seleccionar los programas a financiar.	
	APO05.04	Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones.	
	APO05.05	Mantener los portafolios.	
	APO05.06	Gestionar la consecución de beneficios.	
APO06	APO06.01	Gestionar las finanzas y la contabilidad.	Planificación Estratégica de TI. Presupuesto de TI. Cumplimiento de plan operativo. Evaluación de desempeño. Portafolio de Servicios de TI. Seguimiento a proveedores. SLAs. Políticas y procedimientos administrativos.
	APO06.02	Priorizar la asignación de recursos.	
	APO06.03	Crear y mantener presupuestos.	
	APO06.04	Modelar y asignar costes.	
	APO06.05	Gestionar costes.	
APO07	APO07.01	Mantener la dotación de personal suficiente y adecuada.	Planificación Estratégica de TI. Políticas y procedimientos de Talento Humano. Seguimiento a proveedores. Políticas y procedimientos de TI. Entrevista. Plan de capacitación de TI. Evaluación de desempeño. Políticas y procedimientos administrativos.
	APO07.02	Identificar personal clave de TI.	
	APO07.03	Mantener las habilidades y competencias del personal.	
	APO07.04	Evaluar el desempeño laboral de los empleados.	
	APO07.05	Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio.	
	APO07.06	Gestionar el personal contratado.	

VALORACIÓN DE CRITERIOS:

APO08	APO08.01	Entender las expectativas del negocio.	Estructura Organizacional. Manual de Funciones. Políticas y procedimientos administrativas. Políticas y procedimientos de TI. Entrevista. Funciones del Comité de TI. Análisis del Entorno. Soporte a usuarios. Herramienta de Help Desk.
	APO08.02	Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio.	
	APO08.03	Gestionar las relaciones con el negocio.	
	APO08.04	Coordinar y comunicar.	
	APO08.05	Proveer datos de entrada para la mejora continua de los servicios.	
APO09	APO09.01	Identificar servicios TI.	Políticas y procedimientos de TI. Portafolio de Servicios. SLAs. BIA. Soporte a usuarios. Herramienta de Help Desk.
	APO09.02	Catalogar servicios basados en TI.	
	APO09.03	Definir y preparar acuerdos de servicio.	
	APO09.04	Supervisar e informar de los niveles de servicio.	
	APO09.05	Revisar acuerdos de servicio y contratos.	
APO10	APO10.01	Identificar y evaluar las relaciones y contratos con proveedores.	Políticas y procedimientos administrativos. Políticas y procedimientos de TI. Portafolio de proveedores. Seguimiento a proveedores. Estructura de TI. BIA.
	APO10.02	Seleccionar proveedores.	
	APO10.03	Gestionar contratos y relaciones con proveedores.	
	APO10.04	Gestionar el riesgo en el suministro.	
	APO10.05	Supervisar el cumplimiento y el rendimiento del proveedor.	
APO11	APO11.01	Establecer un sistema de gestión de la calidad (SGC).	Estructura Organizacional. Manual de Funciones. Políticas y procedimientos administrativos. Entrevista. Políticas y procedimientos de TI. SLAs. Cumplimiento del plan operativo. Planes de prueba. Plataforma de TI.
	APO11.02	Definir y gestionar los estándares, procesos y prácticas de calidad.	
	APO11.03	Enfocar la gestión de la calidad en los clientes.	
	APO11.04	Supervisar y hacer controles y revisiones de calidad.	
	APO11.05	Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.	
	APO11.06	Mantener una mejora continua.	
APO12	APO12.01	Recopilar datos.	Políticas y procedimientos de riesgos. Entrevista. Políticas y procedimientos de TI. BIA. Seguimiento a riesgos. Informes mensuales. Portafolio de Servicios. Plan de contingencias de TI.
	APO12.02	Analizar el riesgo.	
	APO12.03	Mantener un perfil de riesgo.	
	APO12.04	Expresar el riesgo.	
	APO12.05	Definir un portafolio de acciones para la gestión de riesgos.	
	APO12.06	Responder al riesgo.	

VALORACIÓN DE CRITERIOS:

APO13	APO13.01	Establecer y mantener un SGSI.	Políticas y procedimientos de TI. Entrevista. Seguimiento a resoluciones de ente de control. Procedimientos de Seguridad.
	APO13.02	Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	
	APO13.03	Supervisar y revisar el SGSI.	
MEA01	MEA01.01	Establecer un enfoque de la supervisión.	Estructura Organizacional. Entrevista. Evaluación del desempeño. Planificación Estratégica Institucional y de TI. Análisis del Entorno. Manual de funciones.
	MEA01.02	Establecer los objetivos de cumplimiento y rendimiento.	
	MEA01.03	Recopilar y procesar los datos de cumplimiento y rendimiento.	
	MEA01.04	Analizar e informar sobre el rendimiento.	
	MEA01.05	Asegurar la implantación de medidas correctivas.	
MEA02	MEA02.01	Supervisar el control interno.	Estructura Organizacional. Políticas y procedimientos administrativos. Portafolio de Proveedores. Seguimiento a proveedores. Evaluación de desempeño. Entrevista. Ejecución de Auditorías Internas y Externas. Evaluación del control interno. Seguimiento del plan estratégico y operativo. Bitácoras. Código de Ética.
	MEA02.02	Revisar la efectividad de los controles sobre los procesos de negocio.	
	MEA02.03	Realizar autoevaluaciones de control.	
	MEA02.04	Identificar y comunicar las deficiencias de control.	
	MEA02.05	Garantizar que los proveedores de aseguramiento son independientes y están cualificados.	
	MEA02.06	Planificar iniciativas de aseguramiento.	
	MEA02.07	Estudiar las iniciativas de aseguramiento.	
	MEA02.08	Ejecutar las iniciativas de aseguramiento.	
MEA03	MEA03.01	Identificar requisitos externos de cumplimiento.	Seguimiento a recomendaciones del ente de control. Entrevista. Políticas y procedimientos administrativos. Seguimiento al cumplimiento. Auditorías internas y externas. Planificación Estratégica institucional.
	MEA03.02	Optimizar la respuesta a requisitos externos.	
	MEA03.03	Confirmar el cumplimiento de requisitos externos.	
	MEA03.04	Obtener garantía del cumplimiento de requisitos externos.	

CONTROLES:

LISTADO DE CONTROLES POR AREA DE NEGOCIO	
Área	**Control**
Desarrollo	Acceso a datos y programas
Desarrollo	Aprobación de Requerimiento de Desarrollo
Desarrollo	Autenticación e integridad en transacciones
Desarrollo	Chequeos de Integridad, Exactitud y Autenticidad
Desarrollo	Control de cambios
Desarrollo	Control de versionamiento
Desarrollo	Integridad y Validez en procesamiento
Desarrollo	Manejo de documentación
Desarrollo	Metodología desarrollo de sistemas
Desarrollo	Revisión de salidas y manejo de errores
Desarrollo	Validación de Requerimiento de Desarrollo
Operaciones	Bitácoras de operación
Operaciones	Control a contabilidad y cálculos
Operaciones	Cuadres
Operaciones	Eficiencia Operativa
Operaciones	Gestión de Calidad
Operaciones	Monitoreo de operaciones
Operaciones	Piloto
Operaciones	Planificación de salida a producción
Operaciones	Pruebas en ambientes controlados
Operaciones	Revisión de conformidad
Operaciones	Seguimiento a contratos
Operaciones	Seguimiento Postimplementación
Producción	Acceso a recursos de TI
Producción	Antivirus
Producción	Bitácoras de procesamiento
Producción	Contingencias
Producción	Cumplimiento SLAs
Producción	Firewall
Producción	Generación de respaldos
Producción	Inventario y Mantenimiento de Equipos
Producción	Monitoreo de condiciones ambientales
Producción	Monitoreo de enlaces
Producción	Procedimientos de Operación
Producción	Prueba de respaldos
Producción	Registro de respaldos
Producción	Seguridad física en centros de datos

LISTADO DE CONTROLES POR AREA DE NEGOCIO	
Área	**Control**
Riesgos	Capacitación
Riesgos	Definición de tiempos de operación y recuperación
Riesgos	Planeación de continuidad de negocios
Riesgos	Pruebas de contingencias
Riesgos	Pruebas de cumplimiento
Riesgos	Revisiones independientes de TI
Riesgos	Simulacros
Riesgos	Tratamiento de Riesgos
Seguridad Física	Autorización de Acceso
Seguridad Física	Políticas y Procedimientos de Seguridad física y lógica
Seguridad Física	Registro de Visitantes
Seguridad Física	Solicitud de identificación
Seguridad Física	Video vigilancia
Seguridad Informática	Control de privilegios
Seguridad Informática	Incompatibilidad de funciones
Seguridad Informática	Registro de incidentes de seguridad
Seguridad Informática	Registro de pistas de auditoría
Seguridad Informática	Registro de violaciones de acceso
Seguridad Informática	Seguridad perimetral
Subgerencia de Operaciones	Control presupuestario
Subgerencia de Operaciones	Continuidad del Negocio
Subgerencia de Operaciones	Gestión de adquisiciones
Subgerencia de Operaciones	Planificación Estratégica
Subgerencia de Operaciones	Revisión de políticas y procedimientos
Subgerencia de Operaciones	Segregación de funciones
Talento Humano	Políticas de Capacitación
Talento Humano	Políticas de Selección
Talento Humano	Políticas de Vinculación y Desvinculación