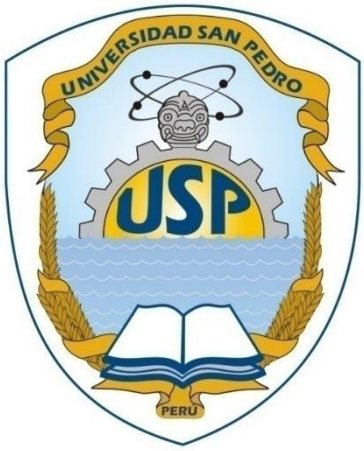
UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA

INFORMÁTICA Y DE SISTEMAS



Evaluación de la seguridad del centro de datos del Poder Judicial del Santa, Chimbote

"TESIS PARA OBTENER EL TITULO PROFESIONAL DE INGENIERA EN INFORMATICA Y DE SISTEMAS"

AUTOR

Bach. Rodriguez Vera Raquel Gianina

ASESOR:

Ing. Miguel Arturo Valle Peláez

CHIMBOTE

2018

ÍNDICE

PALABRAS CLAVE

Tema	Evaluación de la Seguridad
Especialidad	Gestión

KEYWORDS

Topic	Safety Assessment
Specialty	Management

LINEA DE INVESTIGACION

Área	Ingeniería y Tecnología
Sub Área	Ingeniería Eléctrica, Electrónica e Informática
Disciplina	Ingeniería de Sistemas y Comunicaciones

Evaluación de la seguridad del centro de datos del Poder Judicial del Santa, Chimbote

RESUMEN

La presente investigación tuvo como objetivo la Evaluación de la Seguridad del Centro de Datos del Poder Judicial del Santa – Chimbote que permitió la recopilación de las políticas de seguridad, la evaluación técnica de la gestión de las tecnologías de la información con las que actualmente cuentan para garantizar la confidencialidad, integridad y disponibilidad de la información alojada en los servidores y sistemas de almacenamientos ubicados en el data center para determinar el cumplimiento de las normas y estándares internacionales que establecen el marco de la seguridad informática.

El presente proyecto, se desarrolló mediante una investigación documental – descriptiva; para la recolección de la información se empleó técnicas de investigación de campo de fuentes primarias, como observación, análisis documental, entrevista; y secundarias como son documentos y libros. Dicha información fue analizada y evaluada, mediante lo cual, se empleó el marco de referencia COBIT determinando si existe integridad, confidencialidad y disponibilidad de la información, dando como resultado la identificación de vulnerabilidades de seguridad en todos los elementos que se encontró en el Centro de Datos ,de esta manera se planteó un control generando reportes de los incidentes y recomendando se establezcan políticas de seguridad de la información y medidas preventivas considerando el mejoramiento continuo de la seguridad.

ABSTRACT

The present investigation had as objective the Security Assessment of the Data Center of the Judiciary of Santa - Chimbote that allowed the compilation of the security policies, the technical evaluation of the management of the information technologies with which they currently count for guarantee the confidentiality, integrity and availability of the information hosted in the servers and storage systems located in the data center to determine compliance with international norms and standards that establish the framework of computer security.

The present project was developed through documentary - descriptive research; for the collection of information, field research techniques were used from primary sources, such as observation, documentary analysis, interview; and secondary ones such as documents and books. This information was analyzed and evaluated, whereby the COBIT frame of reference was used to determine if there is integrity, confidentiality and availability of the information, resulting in the identification of security vulnerabilities in all elements found in the Center Data, this way a control was generated generating reports of the incidents and recommending to establish policies of information security and preventive measures considering the continuous improvement of the security.

1. INTRODUCCIÓN

De los antecedentes encontrados se han abordado los trabajos más relevantes a esta investigación:

En la tesis Narváez Mejía, Jhon Alexis (2012) "Evaluación Técnica Informática Del Comil 10 Abdón, Utilizando El Estándar Internacional COBIT" se propuso realizar la evaluación técnica informática del colegio militar N° 10 Abdón Calderón utilizando el estándar internacional COBIT. Los procedimientos de la gestión tecnológica que aplica actualmente el Departamento de Tecnologías de Información del Comil N° 10, resultado de la evaluación son seleccionados y adaptados a un modelo de gestión de TI que dificultad la toma de decisiones en cuanto al desempeño de tecnologías en el interior de la institución, además de requiere medir y controlar el desarrollo y aplicación de los procesos tecnológicos para que permitan mejorar la trayectoria estratégica y operativa.

En la tesis Viteri Díaz, Sofía Monserrath (2013) "Evaluación Técnica de la Seguridad Informática del Data Center de la Brigada De Fuerzas Especiales No. 9 Patria" se propuso como objetivo central diseñar un programa de mejora continua con un plan de Seguridad Informática, el mismo que servirá para que los usuarios del Data Center de la Brigada "Patria", se encuentren en capacidad de aplicar medidas de seguridad para mantener la información disponible, confiable y oportuna.

En la tesis Anasi Suntasig, Karina Isabel y Paspuel Morales, Paulina Tatiana (2013) "Evaluación de la Gestión Informática de la Unidad de TI de la Cooperativa de Ahorro y Crédito TEXTIL 14 DE MARZO usando COBIT 4.1" se propuso en realizar la Evaluación de la Gestión Informática de la Unidad de TI de la Cooperativa de Ahorro y Crédito TEXTIL14 DE MARZO usando COBIT 4.1 el cual se lo ha estructurado en cuatro capítulos. Usando como marco de referencia COBIT 4.1, contiene la planificación de la evaluación, la conformación del grupo evaluador y la descripción de la herramienta para la medición del nivel de madurez de los procesos seleccionados. Se efectúo el análisis de los resultados y se proponen mejoras para la gestión informática de los procesos seleccionados. Finalmente, se exponen las conclusiones y recomendaciones obtenidas con la realización del presente proyecto.

En la tesis Gualsaquí Vivar, Juan Carlos, Quito (2013) "Desarrollo Del Marco De Referencia COBIT 5.0 Para La Gestión Del Área De Ti De La Empresa Blue Card" se propuso de realizar una correcta y aplicada gestión del área de información tecnológica permitiendo no solo el aseguramiento y aprovechamiento de los diferentes recursos que la misma posee sino también como por ejemplo controlar el acceso no apropiado y autorizado de personas que estén hábiles de manipular intencionalmente o no datos e información significativa de cualquier organización o empresa logrando sus objetivos basados en la gestión de Gobierno y de las TI corporativas, creando valores óptimos desde TI generando beneficios y optimizando el riesgo y uso de recursos.

Asimismo Cáceres Bustamante, Susan y García García, Johana (2014) en la tesis "Implementación de una Auditoria Informática para la Oficina de Servicios Informáticos de la UNJFSC Aplicando el Marco de Referencia COBIT", se propuso realizar una evaluación de la Gestión de la Información en la Oficina de Servicios Informáticos de la Universidad Nacional José Faustino Sánchez Carrión. Con dicha investigación se logra encontrar aspectos que no permiten la optimización y la buena gestión de la Información en dicha oficina la cual fueron observadas para la evaluación correspondiente, usando la metodología de trabajo COBIT se llegará a medir el grado de madurez en la que se encuentra.

Esta investigación se justifica a nivel social ya que permite garantizar la confidencialidad, integridad y disponibilidad de la información alojada en los servidores y sistemas de almacenamientos ubicados en el data center brindando un mejor control de la información del Poder Judicial del Santa, agilizando los procesos y de esta manera presentar a nuestra sociedad a una entidad capaz de garantizar la completa seguridad de la información de los diversos trámites judiciales en la entidad.

La investigación aporta en lo científico porque busca conocimientos selectivos y sistematizados para el desarrollo de la Evaluación Técnica de Seguridad Informática, el cual se usó como herramienta de apoyo el marco de trabajo COBIT que es precisamente un modelo para evaluar la gestión y control de los sistemas de información y tecnología con la finalidad de lograr que las diferentes entidades reguladas optimicen sus inversiones de TI y administren adecuadamente sus riesgos tecnológicos.

Actualmente en todas las empresas y negocios de cualquier tamaño sus operaciones y procedimientos dependen de los sistemas informáticos, ya que gracias a ellos las organizaciones pueden realizar sus operaciones de manera más eficiente para brindar mejores servicios. Actualmente en el Poder Judicial del Santa el acceso al centro de datos es restringido al personal autorizado, sin embargo, no tiene una clara visibilidad de las métricas importantes para su infraestructura e integridad física, por lo que no se puede planificar con precisión, detectar posibles problemas ni optimizar la asignación de los recursos como suministro de energía, mecanismos de detección y alarmas.

El Poder Judicial del santa - Chimbote tiene diferentes órganos institucionales en la parte administrativa entre ellas: las oficinas de planeamiento de proyectos y estadística, contabilidad, tesorería, unidad de administración y finanzas, personal, logística, Gerencia de administración, informática; todas ellas se encuentran con la necesidad de comunicarse entre ellos debido al gran flujo de información, por lo que es fundamental que los sistemas de información tienen que actualizarse permanentemente.

Teniendo conocimiento de la gran cantidad de datos que manejan los sistemas de información, imprescindible disponer de servidores que almacenen los datos, pero su descuido en no cumplir con las normas técnicas correspondientes para controlar la eficiencia de sus procesos, da origen a que nos plantemos o formulemos el problema de la siguiente manera: ¿Cómo desarrollar una Evaluación de la Seguridad del Centro de Datos del Poder Judicial del Santa, Chimbote?

Después de haber formulado la problemática es necesario tener algunos conceptos básicos con respecto a las variables de trabajo, que en la presente investigación se determinaron como “Seguridad Informática” y “Centro de Datos”.

Según Jorge Ramió (2006), define que la seguridad informática es “un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas”.
Los elementos básicos de la seguridad informática son:

- Confidencialidad: Los componentes del sistema serán accesibles sólo por aquellos usuarios autorizados.
- Integridad: Los componentes del sistema sólo pueden ser creados y modificados por los

usuarios autorizados.

- Disponibilidad: Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.

Por su lado Mario G. Piattini y Emilio del Peso (2001), Un data center sigue un modelo organizativo más o menos estándar, aunque debido a diferentes causas, como puedes ser el tipo de empresa al que pertenece, situación económica, disponibilidades de espacio, actitud de la Dirección, etc. Haces que, en realidad los centros de proceso de datos difieran bastante uno de los otros.

Mientras que la empresa IBM (2012), en un artículo publicado define que: El entorno del Data Center es una compilación de servidores, almacenamiento, sistemas de redes, sistemas mecánicos/eléctricos, aplicaciones y herramientas, procedimientos de gobernanza y personal. El único medio efectivo para medir la eficiencia de las operaciones del Data Center es incorporar un enfoque global que considere múltiples medidas en todos los elementos.

Se señalan a continuación algunas Fuentes que deben estar accesibles en todo Centro de Proceso de Datos:

- Políticas, Normas y Planes sobre Seguridad emitidos y distribuidos tanto por la Dirección de la empresa en términos generales como por el Departamento de Seguridad siguiendo un enfoque más detallado.
- Auditorías anteriores, generales y parciales, referentes a la Seguridad física o cualquier otro tipo de auditoría que, de una u otra manera, esté relacionada con la Seguridad Física.
- Contratos de seguros, de proveedores y de mantenimiento.
- Entrevistas con el personal de seguridad, personal informático y de otras actividades.
- Actas e informes de técnicos y consultores.
- Plan de contingencia y valoración de las pruebas.
- Informes sobre accesos y visitas. Existencia de una sistema de control de entradas y salidas diferenciando entre áreas Perimetral, interna y restringida.
- Informes sobre pruebas de evacuación ante diferentes tipos de amenaza: incendio, catástrofe natural, terrorismo, etc.
- Informe sobre evacuaciones reales.
- Políticas de personal.

- Inventarios de soportes.

Por su lado ISACA (2013), expone que COBIT ayuda a las Organizaciones a crear un valor óptimo a partir de la TI, al mantener un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos. Permite que las tecnologías de la información y relacionadas se gobiernen y administren de una manera holística a nivel de toda la Organización, incluyendo el alcance completo de todas las áreas de responsabilidad funcionales y de negocios, considerando los intereses relacionados con la TI de las partes interesadas internas y externas.

El marco de referencia de COBIT consta de objetivos de control de TI de alto nivel y de una estructura general para su clasificación y presentación, que han sido basadas en tres niveles de actividades de TI al considerar la administración de sus recursos, estos son:

- Actividades: Las actividades y tareas son las acciones requeridas para lograr un resultado medible. Las actividades tienen un ciclo de vida, mientras que las tareas son más discretas.
- Procesos: Son conjuntos de actividades o tareas con delimitación o cortes de control.
- Dominios: Es la agrupación natural de procesos denominados frecuentemente como dominios que corresponden a la responsabilidad organizacional.

Por lo tanto, el marco de referencia conceptual puede ser enfocado desde tres puntos estratégicos: criterios de información, recursos de TI y procesos de TI.
Estos tres puntos estratégicos son descritos en el cubo COBIT que se ilustra en la figura 01.

CUBO COBIT

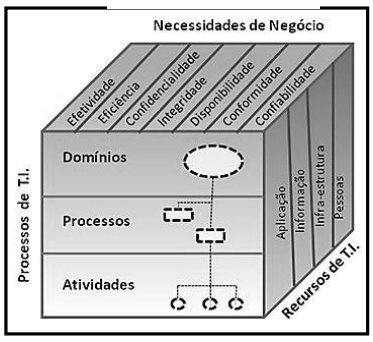


Figura 01
Fuente: Marco Referencia COBIT

Para lograr la alineación de las mejores prácticas con los requerimientos del negocio, se recomienda que COBIT se utilice al más alto nivel, brindando así un marco de control general basado en un modelo de procesos de TI que debe ser aplicable en general a toda empresa.

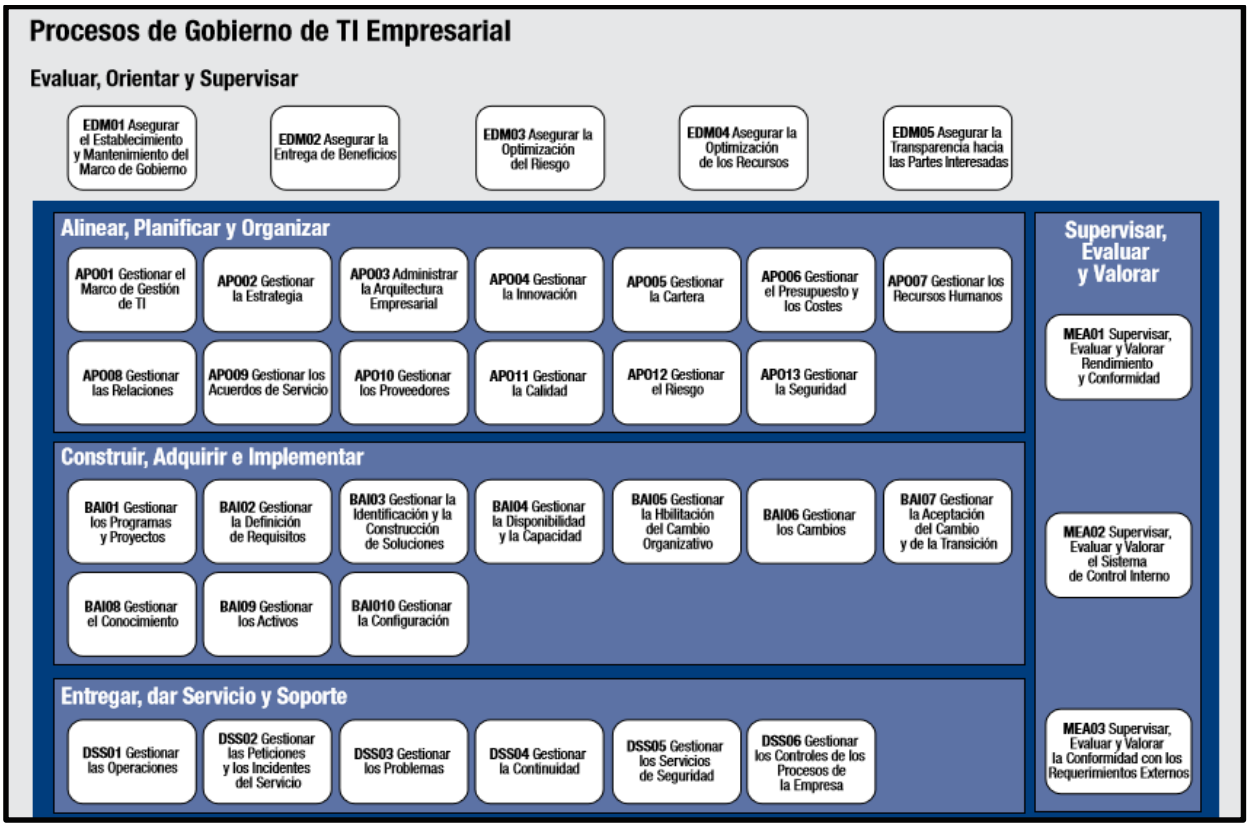


Figura 02: Modelo de Referencia de Procesos de COBIT 5
Fuente: Marco Referencia COBIT

COBIT presenta treinta y siete objetivos generales, uno para cada uno de los procesos de las TI, estos procesos están agrupados en cuatro dominios como lo muestra la figura 03.

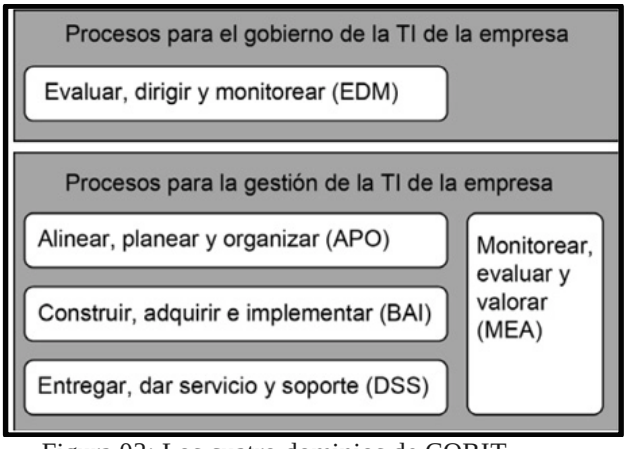


Figura 03: Los cuatro dominios de COBIT
Fuente: Marco Referencia COBIT

- EVALUAR, DIRIGIR Y MONITOREAR (EDM)

Dominio que Gobierno asegura que los objetivos de la empresa se logren mediante la evaluación de las necesidades de las partes interesadas, las condiciones y opciones, estableciendo la dirección a través de la priorización y decisión, y monitoreando el desempeño, el cumplimiento y el progreso contra acordaron dirección y objetivos.

Este dominio considera los siguientes objetivos de alto nivel o procesos:

EDM01 Asegurar El Establecimiento Y Mantenimiento Del Marco De Referencia De Gobierno

EDM02 Asegurar La Entrega De Beneficios

EDM03 Asegurar La Optimización Del Riesgo

EDM04 Asegurar La Optimización De Recursos

EDM05 Asegurar La Transparencia Hacia Las Partes Interesadas

- ALINEAR, ADQUIRIR E IMPLEMENTAR (APO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada.

Este dominio considera los siguientes objetivos de alto nivel o procesos:

APO01 Gestionar El Marco De Gestión De TI

APO02 Gestionar La Estrategia

APO03 Administrar La Arquitectura Empresarial

APO04 Gestionar La Innovación

APO05 Gestionar La Cartera

APO06 Gestionar El Presupuesto Y Los Costes.

APO07 Gestionar Los Recursos Humanos

APO08 Gestionar Las Relaciones

APO09 Gestionar Los Acuerdos De Servicio

APO10 Gestionar Los Proveedores

APO11 Gestionar La Calidad

APO12 Gestionar El Riesgo

APO13 Gestionar La Seguridad

- CONSTRUIR, ADQUIRIR E IMPLEMENTAR (BAI)

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Este dominio considera los siguientes objetivos de alto nivel o procesos:

BAI01 Gestionar Los Programas Y Proyectos

BAI02 Gestionar La Definición De Requisitos

BAI03 Gestionar La Identificación Y La Construcción De Soluciones

BAI04 Gestionar La Disponibilidad Y La Capacidad

BAI05 Gestionar La Facilitación Del Cambio Organizativo.

BAI06 Gestionar Los Cambios

BAI07 Gestionar La Aceptación Del Cambio Y La Transición

BAI08 Gestionar El Conocimiento

BAI09 Gestionar Los Activos

BAI10 Gestionar La Configuración

- ENTREGA, SERVICIO Y SOPORTE (DSS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales.

Este dominio considera los siguientes objetivos de alto nivel o procesos:

DSS01 Gestionar Operaciones

DSS02 Gestionar Peticiones E Incidentes De Servicio

DSS03 Gestionar Problemas

DSS04 Gestionar La Continuidad

DSS05 Gestionar Servicios De Seguridad

DSS06 Gestionar Controles De Proceso De Negocio

- SUPERVISAR, EVALUAR Y VALORAR (MEA)

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la

administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

Este dominio considera los siguientes objetivos de alto nivel o procesos:

MEA01 Supervisar, Evaluar Y Valorar El Rendimiento Y La Conformidad

MEA02 Supervisar, Evaluar Y Valorar El Sistema De Control Interno

MEA03 Supervisar, Evaluar Y Valorar La Conformidad De Los Requerimientos Externos

En resumen, los Recursos de TI necesitan ser administrados por un conjunto de procesos agrupados en forma natural, con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos.

COBIT es considerada una herramienta completa ya que permite administrar los sistemas de información a un nivel más alto que los estándares existentes para el mismo propósito. Se ha determinado que por las características y ambiente de aplicación de COBIT, ésta es la herramienta más útil para fundamentar el presente proyecto, ya que, independientemente dela misión de la organización a ser auditada, la plataforma en la que se basa el desarrollo de las tecnologías de la información, el servicio o producto que ofrezca, el tipo de administración que predomine; el marco de referencia COBIT no es sólo una guía para auditores o técnicos profesionales en procesos TI, sino también para gerentes y todos quienes están involucrados en el cumplimiento de los objetivos del negocio, pues en ambos aspectos, gerencial y tecnológico, su implementación será fundamental para que el gobierno de TI se desarrolle como debe ser.

OBJETIVOS DE CONTROL

Un objetivo de control de TI es una declaración del resultado o fin que se desea lograr al implantar procedimientos de control en una actividad de TI en particular. Los objetivos de control de COBIT son los requerimientos mínimos para un control efectivo de cada proceso de IT. Ya que los objetivos de control de TI de COBIT están organizados por procesos de TI, el marco de trabajo brinda vínculos claros entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI.

Cada uno de los procesos de TI de COBIT tiene un objetivo de control de alto nivel y un número de objetivos de control detallados. Los objetivos de control detallados se identifican por dos caracteres que representan el dominio (EDM, APO, BAI, DSS y MEA) más un número de proceso y un número de objetivo de control.

Además de los objetivos de control detallados, cada proceso COBIT tiene requerimientos de control genéricos que se identifican con PCN (Control de Proceso número) COBIT también ofrece un conjunto recomendado de objetivos de control de las aplicaciones identificados por ACN, número de Control de Aplicación.

MODELOS DE MADUREZ

Los modelos de madurez para el control de los procesos de TI consisten en desarrollar un método de puntaje de modo que una organización pueda calificarse a sí misma desde inexistente hasta optimizada (de 0 a 5). Este método ha sido derivado del modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad de desarrollo de software. Contra estos niveles, desarrollados para cada uno de los treinta y cuatro procesos de TI de COBIT, la administración puede mapear o cruzar:

El estado actual de la organización - dónde está la organización actualmente
El estado actual de la industria (la mejor de su clase en), la comparación
El estado actual de los estándares internacionales, comparación adicional
La estrategia de la organización para mejoramiento, dónde quiere estar la organización.

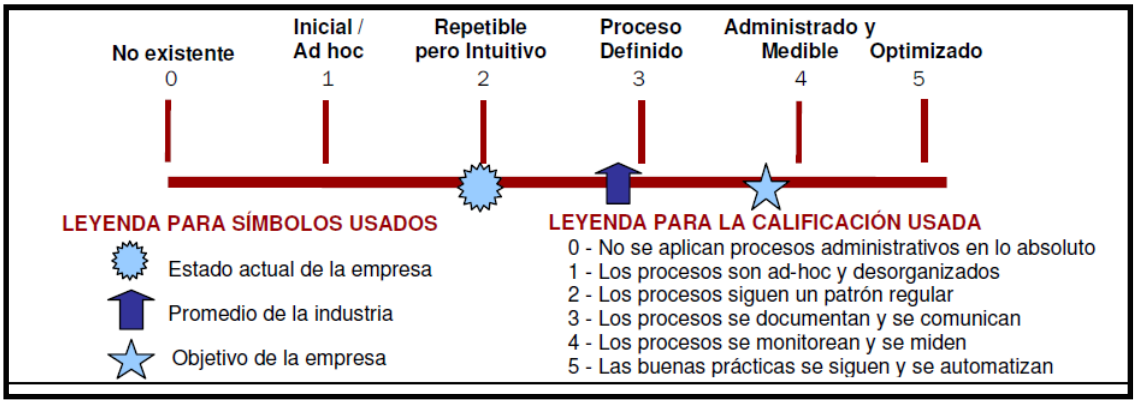


Figura 04:Representación gráfica de los modelos de madurez
Fuente: Marco Referencia COBIT

- Inexistente (0): Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.
- Inicia (1): Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

- Repetible (2): Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.
- Definido (3): Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.
- Administrado (4): Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.
- Optimizado (5): Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa deforma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

En resumen, los modelos de madurez brindan un perfil genérico de las etapas a través de las cuales evolucionan las empresas para la administración y el control de los procesos de TI:

- Un conjunto de requerimientos y los aspectos que los hacen posibles en los distintos niveles de madurez
- Una escala donde la diferencia se puede medir de forma sencilla
- Una escala que se presta a sí misma para una comparación práctica
- La base para establecer el estado actual y el estado deseado
- Soporte para un análisis de brechas para determinar qué se requiere hacer para alcanzar el nivel seleccionado
- Tomado en conjunto, una vista de cómo se administra la TI en la empresa.

Según CMMI Institute las siglas de CMMI responden a Capability Maturity Model Integration, en español Integración de Modelos de Madurez de las Capacidades. Siendo un poco más claros, CMMI es un conjunto de modelos basados en las mejores prácticas en la

gestión de los procesos, desarrollados a través de un proyecto conjunto en el que participaron el SEI (Software Engineering Institute), el gobierno estadounidense y algunos miembros de la industria. Dichos modelos establecen cinco niveles de 'madurez' de las organizaciones en función de si tienen o no una serie de características que detalla cada modelo. Las organizaciones pueden ser evaluadas y, en función de dicha evaluación, se las puede otorgar un nivel de madurez del 1 al 5. Es decir, a través de CMMI, podemos saber el grado de 'madurez' de los procesos que tiene una organización, de acuerdo a un modelo de buenas prácticas. En principio, CMMI estaba orientado exclusivamente al desarrollo de software, pero se ha ido generalizando hasta finalmente derivar en los 3 modelos que conforman el conjunto:

- Desarrollo de productos y servicios (CMMI-DEV)
- Establecimiento y gestión de servicios (CMMI-SVC)
- Adquisición de productos y servicios (CMMI-ACQ)

La investigación tiene un alcance de carácter descriptivo, tiene como alcance la Evaluación de la Seguridad del Centro de Datos del Poder Judicial del Santa, Chimbote; no se considera plantear una hipótesis debido a que no se intenta correlacionar o explicar causalidad de variables. Por tal razón se considera una hipótesis implícita.

En la investigación se planteó como objetivo general: Evaluar la Seguridad del Centro de Datos del Poder Judicial del Santa. Y como Objetivos específicos: 1) Establecer el marco de trabajo para la medición de la gestión de seguridad del centro de datos, 2) Realizar el proceso de evaluación utilizando el marco de trabajo para medición del proceso de seguridad, 3) Elaborar los Planes de Acción para la Mejora de la seguridad del centro de datos.

2. METODOLOGÍA DEL TRABAJO

El presente trabajo de investigación según su orientación es de tipo aplicado y de acuerdo a su nivel de estudio: descriptivo; considerando, que es necesario la recolección de información relacionada con la "Evaluación de la Seguridad del Centro de Datos del Poder Judicial del Santa, Chimbote"

El diseño de investigación es: no experimental, porque trata de observar las características de los hechos, en los cuales no se interviene o manipula deliberadamente los fenómenos de estudio. Y respecto a la temporalidad es de corte transversal porque se realiza la recopilación de la información en un solo tiempo para el desarrollo de la evaluación técnica.

Para la aplicación del instrumento de recopilación de datos se tomó la muestra igual a la población conformada por los colaborados de la Oficina de Informática del Poder Judicial del Santa – Chimbote involucrados directamente con el manejo de la información almacenada en los sistemas quienes respondieron al instrumento.

Las técnicas e instrumentos de recolección de datos que se emplearon para el presente proyecto de investigación fueron:

Tabla 1: Técnicas e instrumentos de Recolección de Datos

Técnicas	Instrumentos	Uso
Entrevista	Cuestionario de preguntas	Se aplicaron cuestionarios al personal involucrado
Análisis documental	Textos, tesis, revistas y estudios previos	Se analizó la documentación para fundamentar la investigación
Observación	Visitas presenciales	Para conocer directamente la situación actual de la seguridad de la

	información.

Elaborado por: RVRG

Se estructuraron preguntas abiertas y cerradas que brindaron información muy certera y directa en cuanto a los objetivos específicos planteados, para obtener mayor información y reforzar el tema del proyecto de investigación.

La metodología de diseño utilizada fue el marco de trabajo COBIT el cual tiene 5 dominios y 37 procesos.

Etapas del Marco de Trabajo COBIT

- Los objetivos de control para la información y las tecnologías relacionadas (COBIT), ayuda a satisfacer las múltiples necesidades de la administración estableciendo un puente entre los riesgos del negocio, los controles necesarios y los aspectos técnicos.

El impacto sobre los recursos de TI son resaltados en el Marco de Referencia de COBIT junto con los requerimientos del negocio que deben ser alcanzados:

Eficiencia
Efectividad
Confidencialidad
Integridad
Disponibilidad
Cumplimiento y
Confiabilidad de la información

- Dominios: Existen dos dominios principales de procesos que divide COBIT 5 detallados a continuación:

Gobierno: contiene un dominio con cinco procesos de gobierno, y dentro de cada uno de ellos se establecen prácticas de evaluación, orientación y supervisión (EDM).

Gestión: contiene cuatro dominios e igualmente dentro de cada uno de ellos se establecen prácticas de planificación, implementación, soporte y evaluación de las TI.

Evaluar, Dirigir Y Monitorear (EDM), Alinear, Planificar y Organizar (Align, Plan and Organise, APO), Construir, Adquirir e Implementar (Build, Acquire and Implement, BAI), Entregar, dar Servicio y Soporte (Deliver, Service and Support, DSS), Supervisar, Evaluar y Valorar (Monitor, Evaluate and Assess, MEA)

A continuación se detallan los 37 procesos contenidos en los cinco dominios principales de COBIT.

Evaluar, Dirigir Y Monitorear (EDM)

EDM01 Asegurar El Establecimiento Y Mantenimiento Del Marco De Referencia De Gobierno

EDM02 Asegurar La Entrega De Beneficios

EDM03 Asegurar La Optimización Del Riesgo

EDM04 Asegurar La Optimización De Recursos

EDM05 Asegurar La Transparencia Hacia Las Partes Interesadas

Alinear, Adquirir E Implementar (Apo)

APO01 Gestionar El Marco De Gestión De TI

APO02 Gestionar La Estrategia

APO03 Administrar La Arquitectura Empresarial

APO04 Gestionar La Innovación

APO05 Gestionar La Cartera

APO06 Gestionar El Presupuesto Y Los Costes.

APO07 Gestionar Los Recursos Humanos

APO08 Gestionar Las Relaciones

APO09 Gestionar Los Acuerdos De Servicio

APO10 Gestionar Los Proveedores

APO11 Gestionar La Calidad

APO12 Gestionar El Riesgo

APO13 Gestionar La Seguridad

Construir, Adquirir E Implementar (BAI)

BAI01 Gestionar Los Programas Y Proyectos

BAI02 Gestionar La Definición De Requisitos

BAI03 Gestionar La Identificación Y La Construcción De Soluciones

BAI04 Gestionar La Disponibilidad Y La Capacidad

BAI05 Gestionar La Facilitación Del Cambio Organizativo.

BAI06 Gestionar Los Cambios

BAI07 Gestionar La Aceptación Del Cambio Y La Transición

BAI08 Gestionar El Conocimiento

BAI09 Gestionar Los Activos

BAI10 Gestionar La Configuración

Entrega, Servicio Y Soporte (Dss)

DSS01 Gestionar Operaciones

DSS02 Gestionar Peticiones E Incidentes De Servicio

DSS03 Gestionar Problemas

DSS04 Gestionar La Continuidad

DSS05 Gestionar Servicios De Seguridad

DSS06 Gestionar Controles De Proceso De Negocio

Supervisar, Evaluar Y Valorar (Mea)

MEA01 Supervisar, Evaluar Y Valorar El Rendimiento Y La Conformidad

MEA02 Supervisar, Evaluar Y Valorar El Sistema De Control Interno

MEA03 Supervisar, Evaluar Y Valorar La Conformidad De Los Requerimientos Externos

- Modelos De Madurez: Los modelos de madurez para el control de los procesos de TI consisten en desarrollar un método de puntaje de modo que una organización pueda calificarse a sí misma desde inexistente hasta optimizada (de 0 a 5).

Inexistente (0): Carencia completa de cualquier proceso reconocible

Inicia (1): Existe evidencia que la empresa ha reconocido que los problemas existen y Requieren ser resueltos.

Repetible (2): Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea.

Definido (3): Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento.

Administrado (4): Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva.

Optimizado (5): Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas.

- CMMI: Según Las organizaciones pueden ser evaluadas y, en función de dicha evaluación, se las puede otorgar un nivel de madurez del 1 al 5. Es decir, a través de

CMMI, podemos saber el grado de ‘madurez’ de los procesos que tiene una organización, de acuerdo a un modelo de buenas prácticas.

3. RESULTADOS

La entrevista fue realizada al personal de la Oficina de Informática del poder judicial del Santa-Chimbote, consta de 17 preguntas el cual se encuentra en anexos.

1. ¿Los procesos que se desarrollan en el Centro de Datos son documentados?

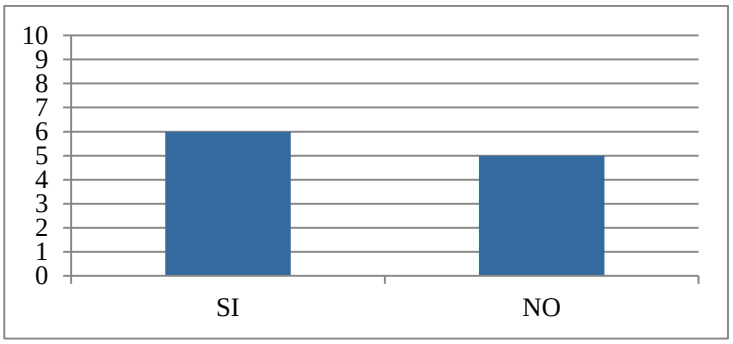


Figura 05: Gráfico documentación procesos en el Centro de Datos
Elaborado por: RVRG

Interpretación: El 45,45% de la población entrevistada respondió que sí son documentados los procesos que se desarrollan en el Centro de Datos y el 54,54 % respondió que no son documentados los procesos que se desarrollan en el Centro de Datos.

2. ¿Se realizan inventarios de los equipos en el Centro de Datos?

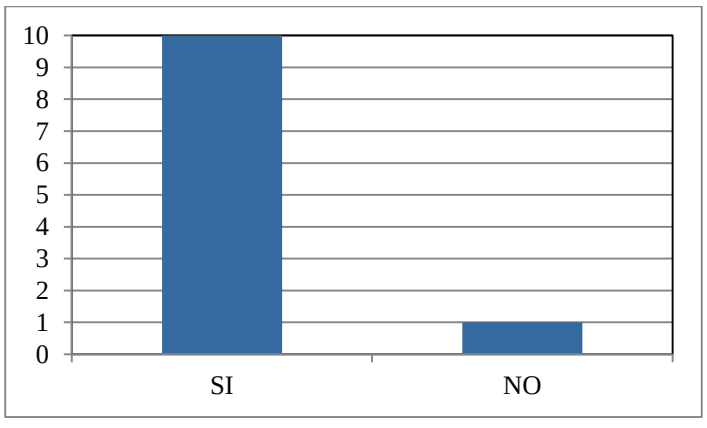


Figura 06: Gráfico inventario de equipos informáticos
Elaborado por: RVRG

Interpretación: El 9,09% de la población entrevistada respondió que sí se realizan inventarios de los equipos en el Centro de datos y el 90,90 % respondió que no se realizan inventario de los equipos en el

Centro de Datos.

3. ¿Se cuenta con manuales por cada Sistema Implantado o software que se utiliza?

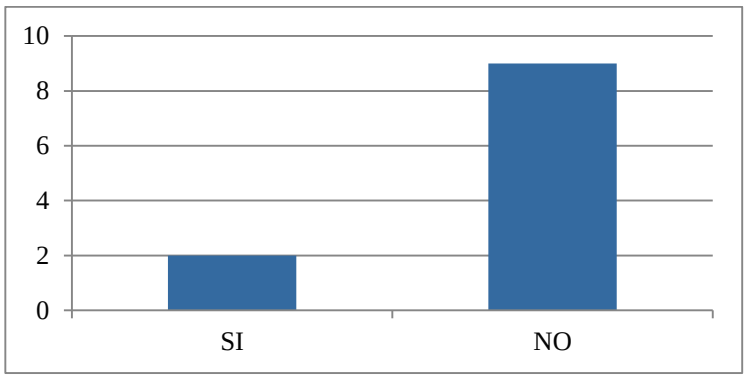


Figura 07: Gráfico manuales para Sistemas
Elaborado por: RVRG

Interpretación: El 81,81% de la población entrevistada respondió que sí se cuenta con manuales por cada sistema implantado o software que se utiliza y el 18,18 % respondió que no se cuenta con manuales por cada sistema implantado o software que se utiliza.

4. ¿Existe un reglamento para el personal de sistemas sobre el acceso al Centro de Datos?

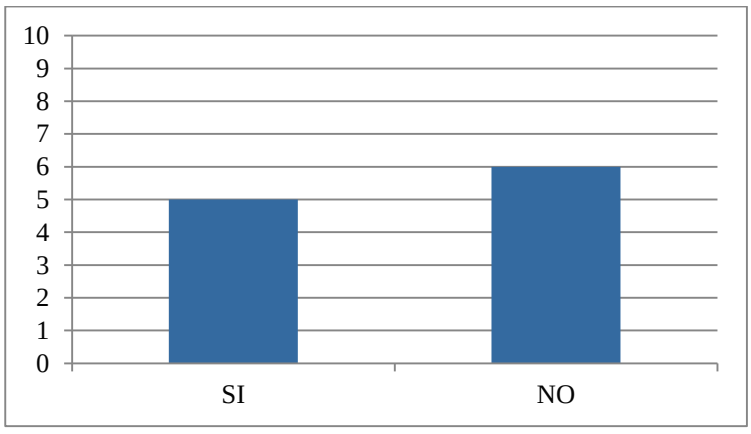


Figura 08: Gráfico existencia de reglamento para personal de sistemas
Elaborado por: RVRG

Interpretación: El 54,54% de la población entrevistada respondió que sí existe un reglamento para el personal de sistemas sobre el acceso de Datos y el 45,45 % respondió que no existe un reglamento para el personal de

sistemas sobre el acceso al Centro de Datos.

5. ¿Se cuenta con un plan operativo?

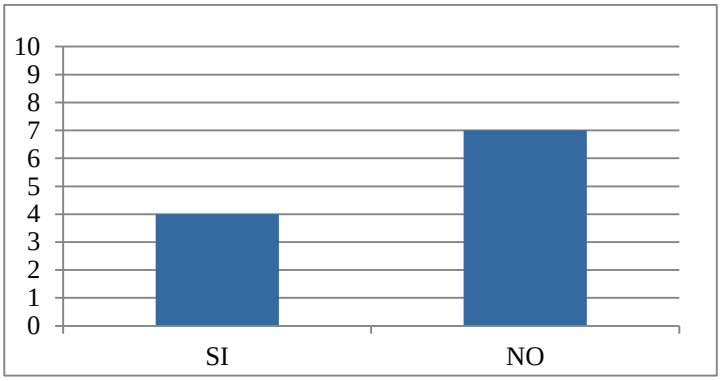


Figura 09: Gráfico plan operativo
Elaborado por: RVRG

Interpretación: El 63,63% de la población entrevistada respondió que si se cuenta con un plan operativo y el 36,36 % respondió que no se cuenta con un plan operativo.

6. La infraestructura del Centro de Datos está construido con un material confiable?

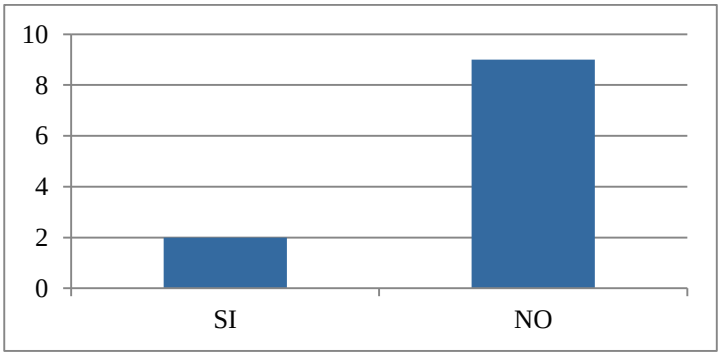


Figura 10: Gráfico infraestructura del centro de datos
Elaborado por: RVRG

Interpretación: El 81,81% de la población entrevistada respondió que si La infraestructura del Centro de Datos está construido con un material confiable y el 18,18 % respondió que La infraestructura del Centro de Datos no está construido con un material confiable

7. ¿El lugar en donde se encuentran los equipos es seguro?

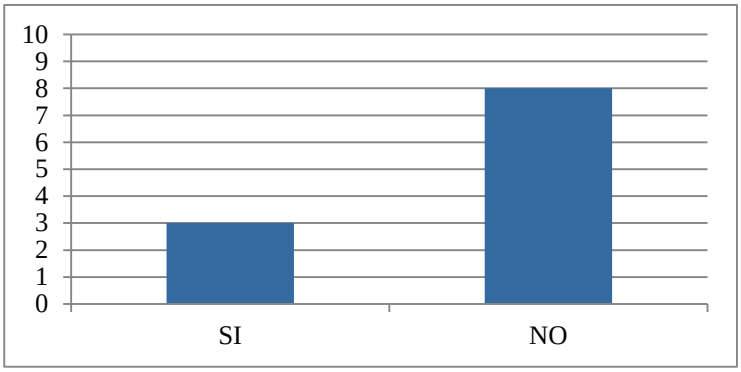


Figura 11: Gráfico ubicación de seguridad de los equipos
Elaborado por: RVRG

Interpretación: El 72,72% de la población entrevistada respondió que El lugar en donde se encuentran los equipos es seguro y el 27,27 % respondió que no es seguro El lugar en donde se encuentran los equipos.

8. ¿Existe algún tipo de material que sea inflamable o pueda resultar peligroso para los equipos?

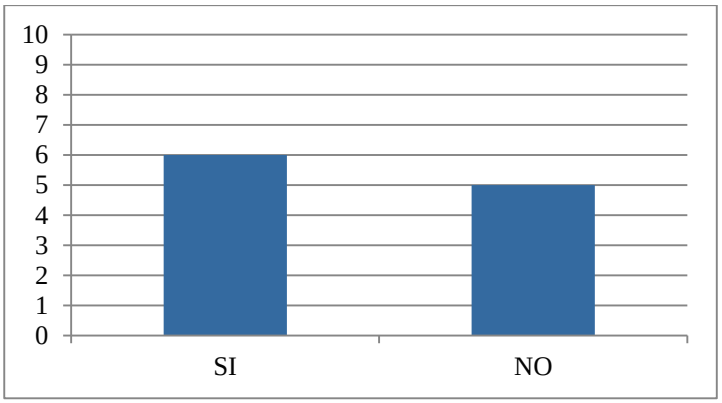


Figura 12: Gráfico peligro de material
Elaborado por: RVRG

Interpretación: El 45,45% de la población entrevistada respondió que si Existe algún tipo de material que sea inflamable o pueda resultar peligroso para los equipos y el 54,54 % respondió que no Existe algún tipo de material que sea inflamable o pueda resultar peligroso para los equipos.

9. ¿Existe algún tipo de mantenimiento preventivo para los equipos del Centro de Datos?

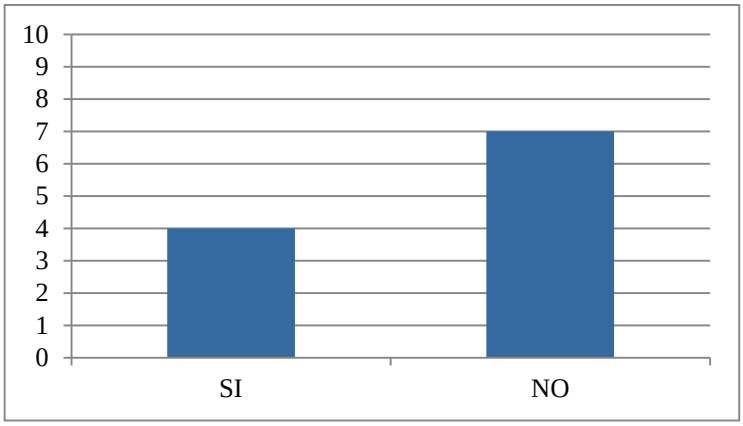


Figura 13: Gráfico mantenimiento preventivo de equipos
Elaborado por: RVRG

Interpretación: El 63,63% de la población entrevistada respondió que si Existe algún tipo de mantenimiento preventivo para los equipos del Centro de Datos y el 36,63 % respondió que no existe algún tipo de mantenimiento preventivo para los equipos del centro de datos.

10. ¿Está conforme con la infraestructura del Centro de Datos?

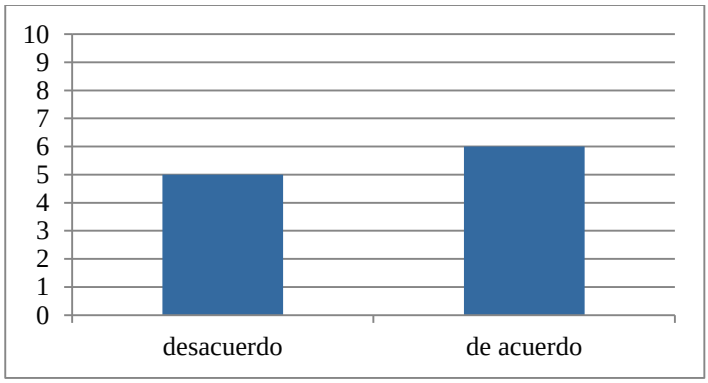


Figura 14: Gráfico conformidad centro de datos
Elaborado por: RVRG

Interpretación: El 54,54% de la población entrevistada está de acuerdo con la conformidad de la infraestructura del Centro de Datos y el 9,90 % está en desacuerdo.

11. ¿Considera importante las salidas de emergencia en el lugar en donde se encuentran los equipos?

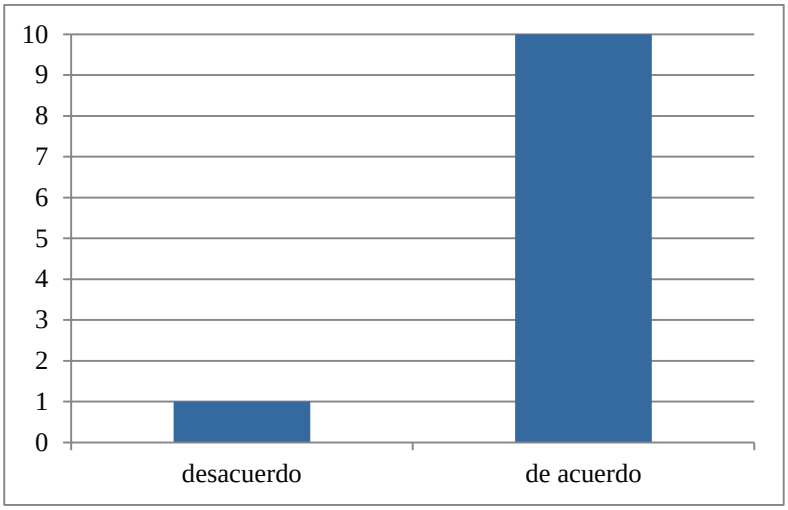


Figura 15: Gráfico importancia salidas de
Elaborado por: RVRG

Interpretación: El 90,90% de la población entrevistada está de acuerdo con que se Considera importante las salidas de emergencia en el lugar en donde se encuentran los equipos y el 9,90 % está en desacuerdo.

12. ¿Está conforme con la seguridad física y tecnológica de vigilancia dentro del Centro de Datos?

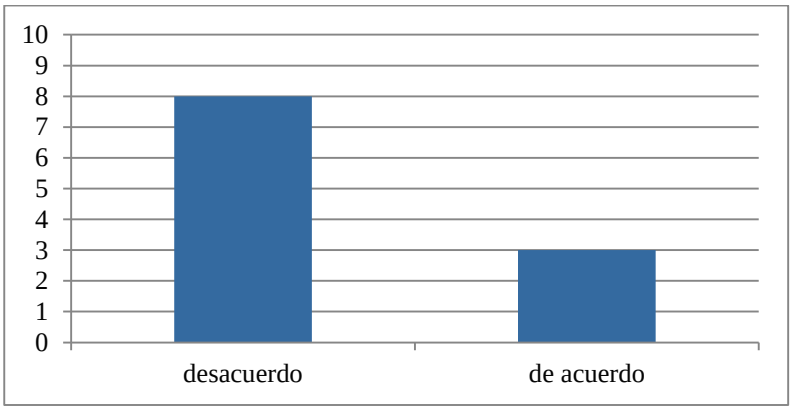


Figura 16: Gráfico seguridad física y tecnológica de vigilancia
Elaborado por: RVRG

Interpretación: El 27,27% de la población entrevistada está de acuerdo con la conformidad con la seguridad física y tecnológica de vigilancia dentro del Centro de Datos y el 72,72 % está en desacuerdo.

13. ¿Cómo considera el cableado y las vías del cuarto de equipo en relación con los estándares generales?

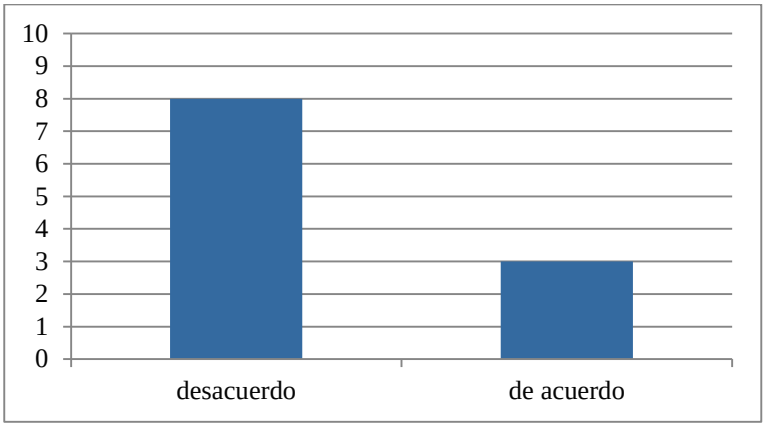


Figura 17: Gráfico cableado del cuarto de equipo
Elaborado por: RVRG

Interpretación: El 27,27% de la población entrevistada está de acuerdo con Como considera el cableado y las vías del cuarto de equipo en relación con los estándares generales y el 72,72 % está en desacuerdo.

14. ¿Está conforme con los etiquetados de cada uno de los equipos dentro del Centro de Datos?

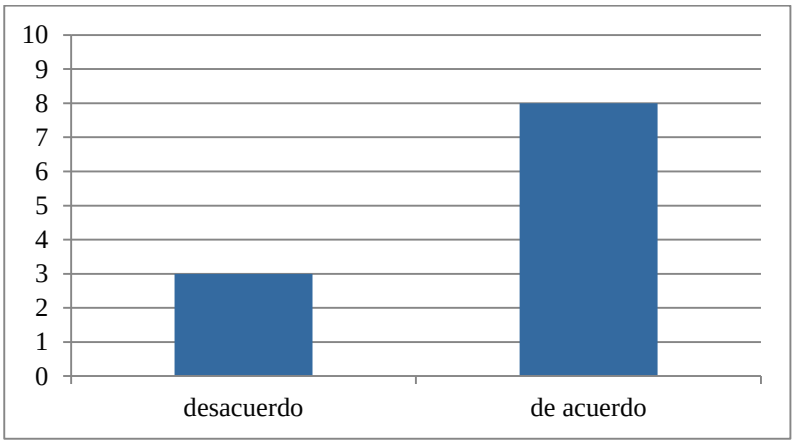


Figura 18: Gráfico etiquetado de los equipos
Elaborado por: RVRG

Interpretación: El 72,72% de la población entrevistada está de acuerdo con los etiquetados de cada uno de los equipos dentro del Centro de Datos y el 27,27 % está en desacuerdo.

15. ¿Está conforme con la distribución de las vías de distribución dentro del lugar de los equipos?

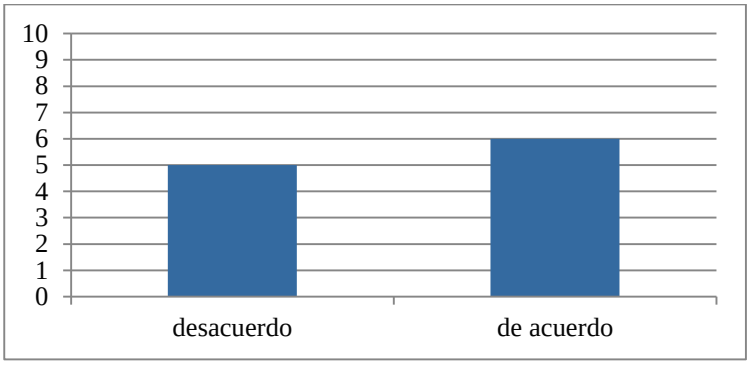


Figura 19: Gráfico conformidad de vías de distribución de equipos
Elaborado por: RVRG

Interpretación: El 54,54% de la población entrevistada está de acuerdo con Está conforme con la distribución de las vías de distribución dentro del lugar de los equipos y el 45,45 % está en desacuerdo.

16. ¿Considera que las tuberías de agua están a buena distancia del el lugar donde se encuentran los equipos?

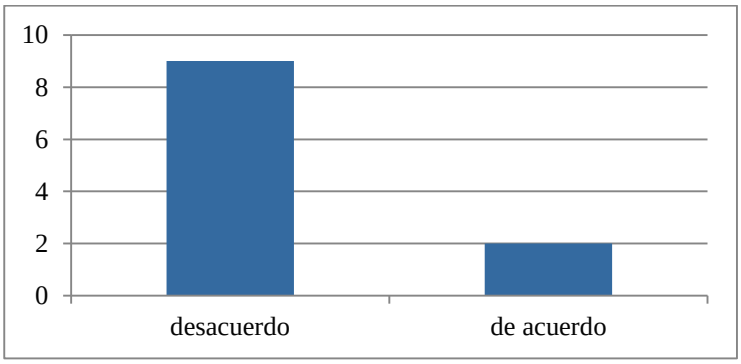
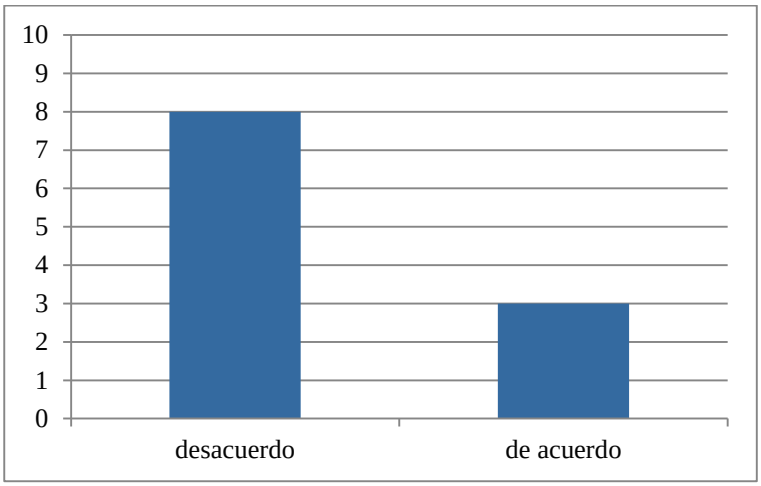


Figura 20: Gráfico seguridad de
Elaborado por: RVRG

Interpretación: El 18,18% de la población entrevistada está de acuerdo con que se Considera que las tuberías de agua están a buena distancia del el lugar donde se encuentran los equipos y el 81,81 % está en desacuerdo.

17. ¿El control de humedad es efectivo dentro del lugar de los equipos?



Interpretación: El 27.27% de la población entrevistada está de acuerdo con El control de humedad es efectivo dentro del lugar de los equipos y el 27.27 % está en desacuerdo.

Figura 21: Gráfico control de humedad en el lugar de equipos
Elaborado por: RVRG

SELECCIÓN DE LOS PROCESOS COBIT A APLICAR

Resultaría demasiado extenso el aplicar la evaluación en todos los procesos y objetivos de control que abarca el marco de referencia de COBIT, por lo que se estructuro la siguiente tabla de todos los procesos COBIT, a fin de realizar la selección de procesos siendo llenada por el mismo investigador tomando como referencia resultados de nuestras observaciones, cuestionarios y entrevista.

Tabla 2: Diagnóstico de Procesos

TABLA DE DIAGNOSTICO DE PROCESOS

OBJETIVOS DE CONTROL	GRADOS DE IMPORTANCIA				
	1	2	3	4	5
	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
EVALUAR, ORIENTAR Y SUPERVISAR					
EDM01 Asegurar El Establecimiento Y Mantenimiento Del Marco De Gobierno	**X**				
EDM02 Asegurar La Entrega De Beneficios	**X**				
EDM03 Asegurar La Optimización Del Riesgo		**X**			
EDM04 Asegurar La Optimización De los Recursos		**X**			
EDM05 Asegurar La Transparencia Hacia Las Partes Interesadas	**X**				
ALINEAR, PLANIFICAR Y ORGANIZAR					
APO01 Gestionar El Marco De Gestión De TI		**X**			
APO02 Gestionar La Estrategia			**X**		
APO03 Administrar La Arquitectura Empresarial					**X**
APO04 Gestionar La Innovación			**X**		

APO05 Gestionar La Cartera	**X**			
APO06 Gestionar El Presupuesto Y Los Costes.	**X**			
APO07 Gestionar Los Recursos Humanos		**X**		
APO08 Gestionar Las Relaciones	**X**			
APO09 Gestionar Los Acuerdos De Servicio	**X**			
APO10 Gestionar Los Proveedores	**X**			
APO11 Gestionar La Calidad				**X**
APO12 Gestionar El Riesgo				**X**
APO13 Gestionar La Seguridad			**X**	
CONSTRUIR, ADQUIRIR E IMPLEMENTAR				
BAI01 Gestionar Los Programas Y Proyectos		**X**		
BAI02 Gestionar La Definición De Requisitos		**X**		
BAI03 Gestionar La Identificación Y La Construcción De Soluciones				**X**
BAI04 Gestionar La Disponibilidad Y La Capacidad		**X**		
BAI05 Gestionar La Facilitación Del Cambio Organizativo.	**X**			
BAI06 Gestionar Los Cambios				**X**
BAI07 Gestionar La Aceptación Del Cambio Y La Transición		**X**		
BAI08 Gestionar El Conocimiento	**X**			
BAI09 Gestionar Los Activos	**X**			

BAI10 Gestionar La Configuración		**X**	
ENTREGA, SERVICIO Y SOPORTE			
DSS01 Gestionar las Operaciones			**X**
DSS02 Gestionar las Peticiones y los Incidentes Del Servicio	**X**		
DSS03 Gestionar los Problemas			**X**
DSS04 Gestionar La Continuidad			**X**
DSS05 Gestionar los Servicios De Seguridad			**X**
DSS06 Gestionar los Controles De los Proceso De la Empresa		**X**	
SUPERVISAR, EVALUAR Y VALORAR			
MEA01 Supervisar, Evaluar Y Valorar El Rendimiento Y La Conformidad	**X**		
MEA02 Supervisar, Evaluar Y Valorar El Sistema De Control Interno	**X**		
MEA03 Supervisar, Evaluar Y Valorar La Conformidad De Los Requerimientos Externos	**X**		

Elaborado por: RVRG

Dominio EDM: EVALUAR, ORIENTAR Y SUPERVISAR

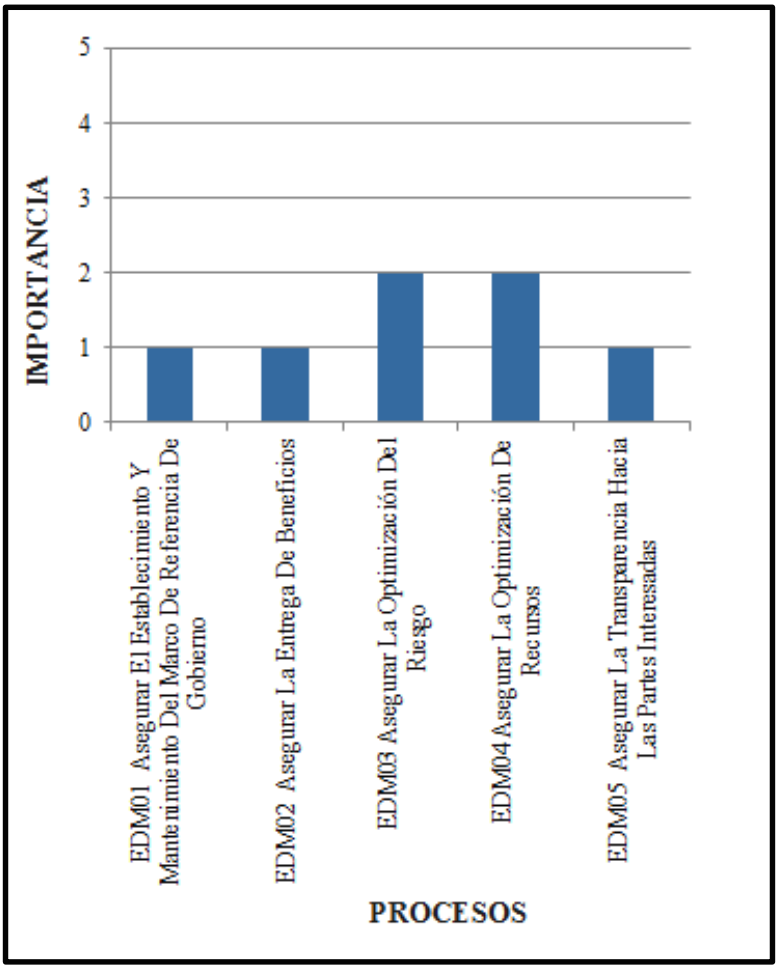


Figura 22: "Evaluar, Orientar Y Supervisar – clasificación por importancia"
Elaborado por: RVRG

Del gráfico se tomará en cuenta los procesos con grado de importancia muy alto, los cuales consideraremos:

No se encontró en el cuadro proceso alguno con grado de importancia muy alto

Dominio APO: ALINEAR, PLANIFICAR Y ORGANIZAR

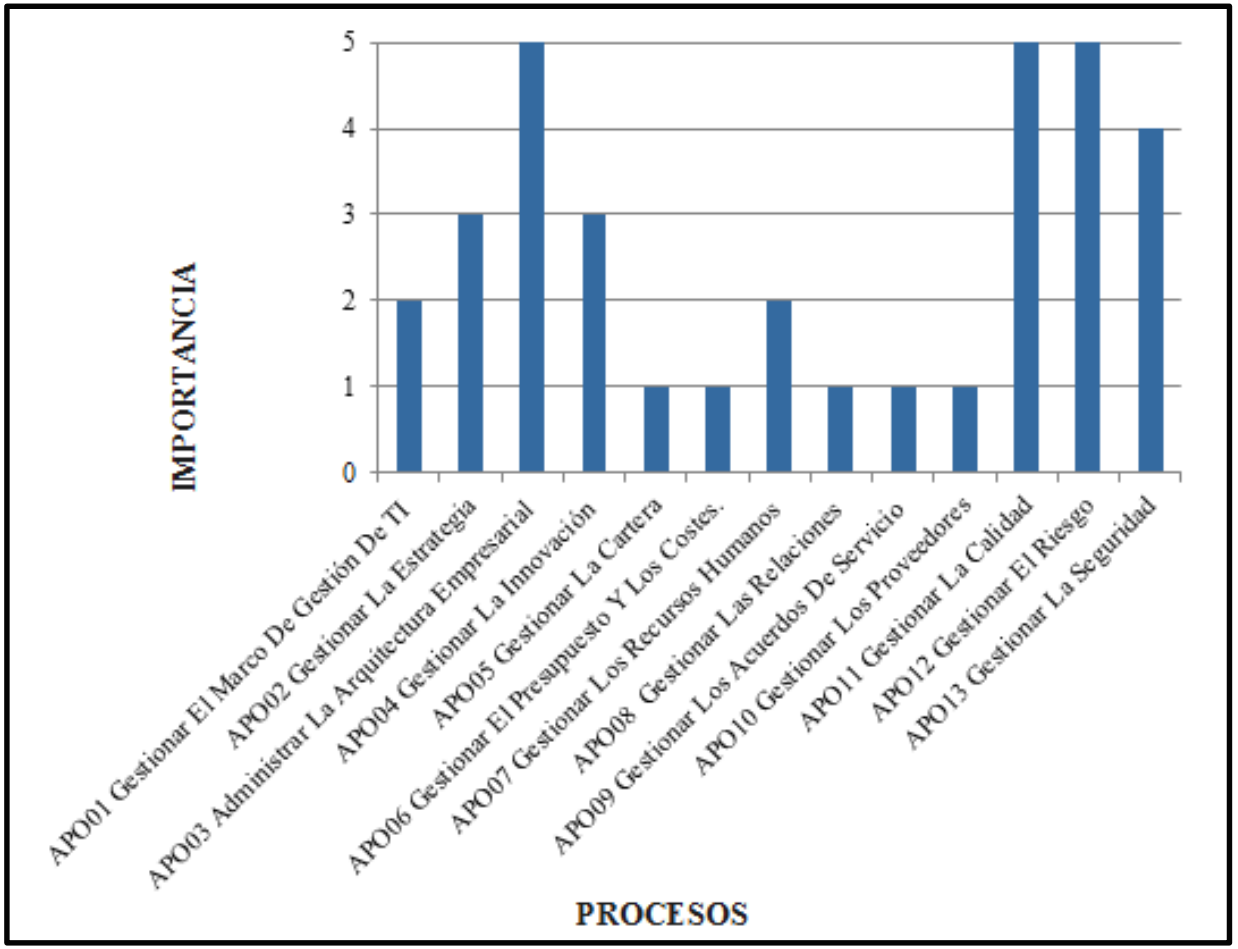


Figura 23: "Alinear, Planificar Y Organizar – clasificación por importancia"
Elaborado por: RVRG

Del gráfico se tomará en cuenta los procesos con grado de importancia muy alto, los cuales consideraremos:

APO03 Administrar La Arquitectura Empresarial

APO11 Gestionar La Calidad

APO12 Gestionar El Riesgo

Dominio BAI: CONSTRUIR, ADQUIRIR E IMPLEMENTAR

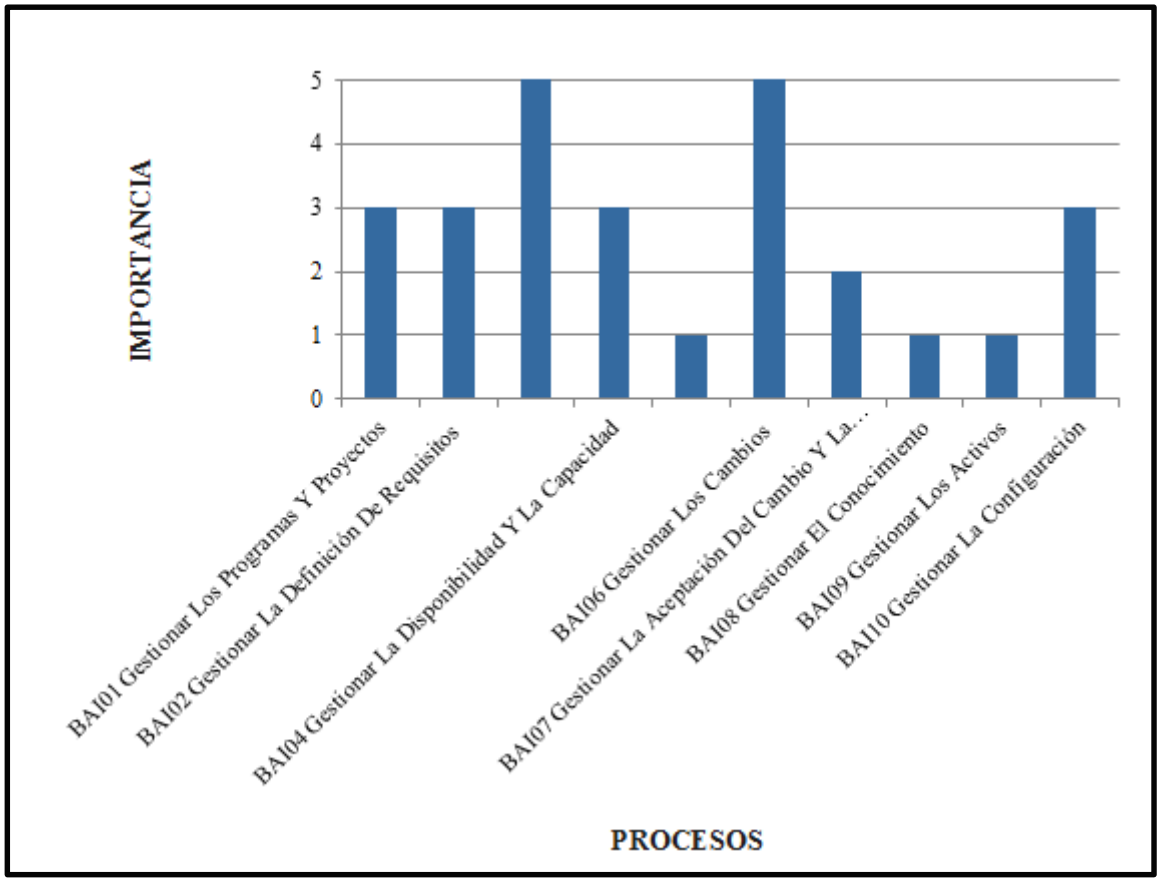


Figura 24: "Construir, Adquirir E Implementar – clasificación por importancia"
Elaborado por: RVRG

Del gráfico se tomará en cuenta los procesos con grado de importancia muy alto, los cuales consideraremos:

BAI03 Gestionar La Identificación Y La Construcción De Soluciones

BAI06 Gestionar Los Cambios

Dominio DSS: ENTREGA, SERVICIO Y SOPORTE

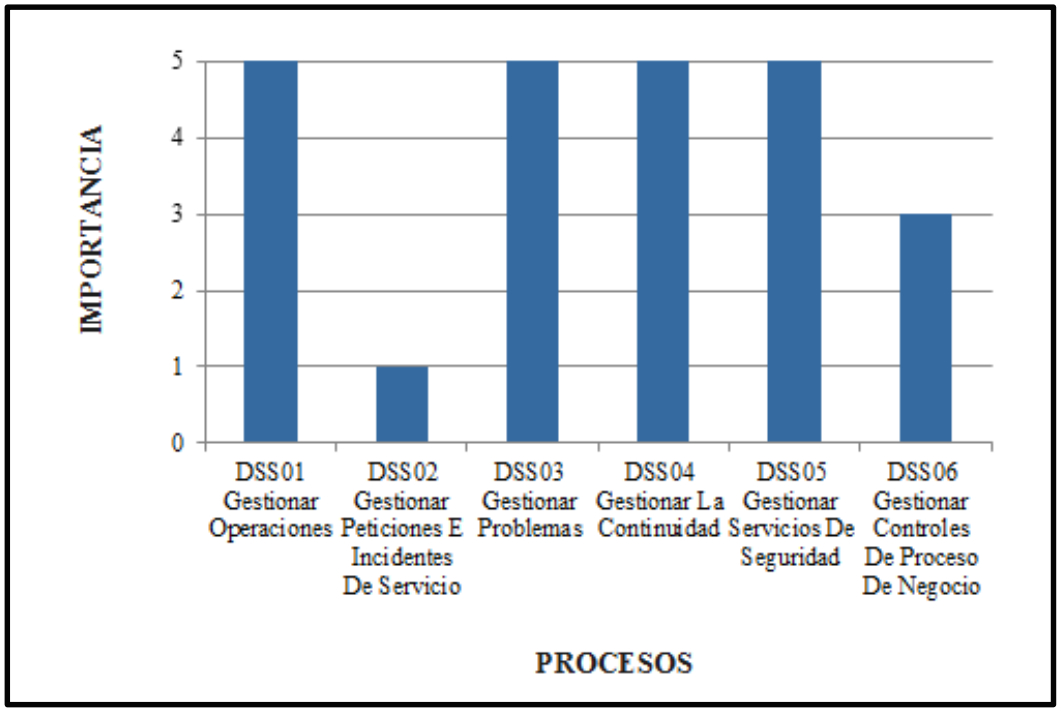


Figura 25: "Entrega, Servicio Y Soporte – clasificación por importancia"
Elaborado por: RVRG

Del gráfico se tomará en cuenta los procesos con grado de importancia muy alto, los cuales consideraremos:

DSS01 Gestionar Operaciones

DSS03 Gestionar Problemas

DSS04 Gestionar La Continuidad

DSS05 Gestionar Servicios De Seguridad

Dominio MEA: SUPERVISAR, EVALUAR Y VALORAR

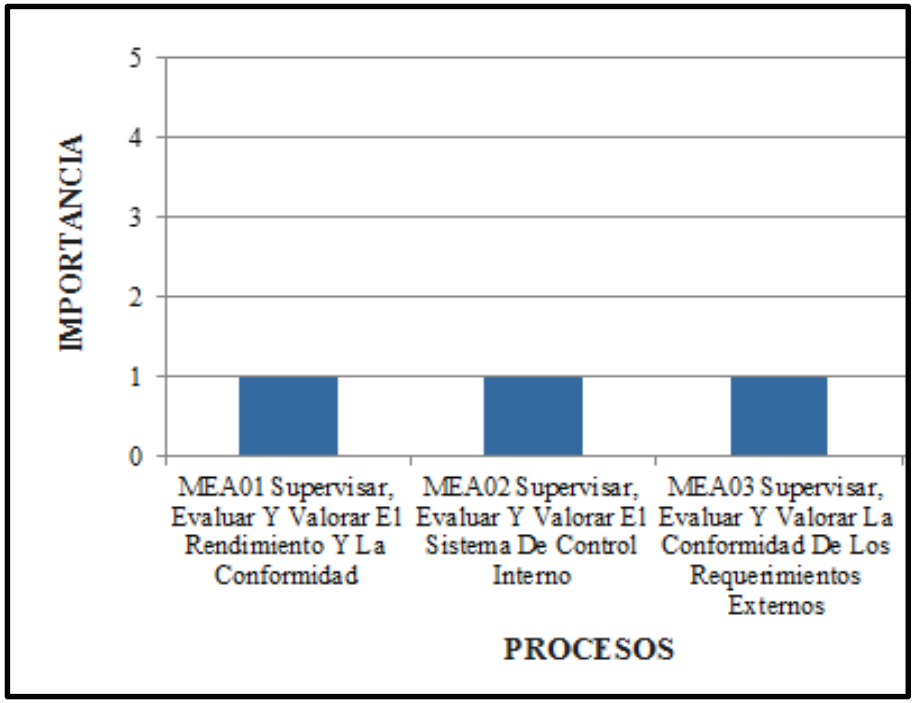


Figura 26: "Supervisar, Evaluar Y Valorar – clasificación por importancia"
Elaborado por: RVRG

Del gráfico se tomará en cuenta los procesos con grado de importancia muy alto, los cuales consideraremos:

No se encontró en el cuadro proceso alguno con grado de importancia muy alto

En base a la evaluación realizada, podemos determinar que dominios y procesos y sus objetivos de control son necesarios aplicar en la evaluación:

Dominio APO: Alinear, Planificar y Organizar

- APO03 Administrar La Arquitectura Empresarial
  - APO03.01 Desarrollar la visión de la arquitectura de referencia.
  - 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.
- APO11 Gestionar La Calidad
  - APO11.01 Establecer un sistema de gestión de la calidad (SGC).
  - 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 Gestionar El Riesgo
  - APO12.01 Recopilar datos.
  - 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 riesgo.
  - APO12.06 Responder al riesgo.

Dominio BAI: Construir, Adquirir e Implementar

- BAI03 Gestionar La Identificación Y La Construcción De Soluciones
  - BAI03.01 Diseñar soluciones de alto nivel.
  - BAI03.02 Diseñar los componentes detallados de la solución.
  - BAI03.03 Desarrollar los componentes de la solución.
  - BAI03.04 Obtener los componentes de la solución.
  - BAI03.05 Construir soluciones.
  - BAI03.06 Realizar controles de calidad.

BAI03.07 Preparar pruebas de la soluciones.

BAI03.08 Ejecutar pruebas de la solución.

BAI03.09 Gestionar cambios a los requerimientos.

BAI03.10 Mantener soluciones.

BAI03.11 Definir los servicios TI y mantener el catálogo de servicios.

- BAI06 Gestionar Los Cambios

BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio.

BAI06.02 Gestionar cambios de emergencia.

BAI06.03 Hacer seguimiento e informar de cambios de estado.

BAI06.04 Cerrar y documentar los cambios.

Dominio DSS: Entregar, Servir y Dar Soporte

- DSS01 Gestionar Operaciones

DSS01.01 Ejecutar procedimientos operativos.

DSS01.02 Gestionar servicios externalizados de TI

DSS01.03 Supervisar la infraestructura de TI.

DSS01.04 Gestionar el entorno.

DSS01.05 Gestionar las instalaciones.

- DSS03 Gestionar Problemas

DSS03.01 Identificar y clasificar problemas

DSS03.02 Investigar y diagnosticar problemas.

DSS03.03 Levantar errores conocidos.

DSS03.04 Resolver y cerrar problemas.

DSS03.05 Realizar una gestión de problemas proactiva.

- DSS04 Gestionar La Continuidad

DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance.

DSS04.02 Mantener una estrategia de continuidad.

DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.

DSS04.04 Ejercitar, probar y revisar el plan de continuidad.

DSS04.05 Revisar, mantener y mejorar el plan de continuidad.

DSS04.06 Proporcionar formación en el plan de continuidad.

DSS04.07 Gestionar acuerdos de respaldo.

DSS04.08 Ejecutar revisiones post-reanudación.

- DSS05 Gestionar los Servicios De Seguridad

  DSS05.01 Proteger contra software malicioso (malware).

  DSS05.02 Gestionar la seguridad de la red y las conexiones.

  DSS05.03 Gestionar la seguridad de los puestos de usuario final.

  DSS05.04 Gestionar la identidad del usuario y el acceso lógico.

  DSS05.05 Gestionar el acceso físico a los activos de TI.

  DSS05.06 Gestionar documentos sensibles y dispositivos de salida.

  DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.

COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprende la tecnología de información, como por ejemplo los recursos humano, instalaciones, sistemas entre otros, y finalmente se realizara una evaluación sobre los procesos involucrados en la organización.

Tabla 3: Modelo de Madurez a Nivel Cualitativo (COSO)

OBJETIVOS DE CONTROL DE COBIT		CRITERIO DE INFORMACIÓN						RECURSOS DE TI			
		Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Personas	Información	Aplicación	Infraestructura
EVALUAR, ORIENTAR Y SUPERVISAR												
EDM01	Asegurar El Establecimiento Y Mantenimiento Del Marco De Gobierno											
EDM02	Asegurar La Entrega De Beneficios											

EDM03	Asegurar La Optimización Del Riesgo											
EDM04	Asegurar La Optimización De los Recursos											
EDM05	Asegurar La Transparencia Hacia Las Partes Interesadas											
	ALINEAR, PLANIFICAR Y ORGANIZAR											
APO01	Gestionar el Marco de Gestión de TI											
APO02	Gestionar la Estrategia											
APO03	Administrar la Arquitectura Empresarial	P	S	S	S					X	X	X
APO04	Gestionar la Innovación											
APO05	Gestionar La Cartera											
APO06	Gestionar El Presupuesto Y Los Costes											
APO07	Gestionar Los Recursos Humanos											
APO08	Gestionar Las Relaciones											
APO09	Gestionar Los Acuerdos De Servicio											
APO10	Gestionar Los Proveedores											
APO11	Gestionar La Calidad	P	P			P	S		X		X	
APO12	Gestionar El Riesgo	S	S	P	P	P	S	S	X	X	X	X

APO13	Gestionar La Seguridad										
	CONSTRUIR, ADQUIRIR E IMPLEMENTAR										
BAI01	Gestionar Los Programas Y Proyectos										
BAI02	Gestionar La Definición De Requisitos										
BAI03	Gestionar La Identificación Y La Construcción De Soluciones	P	P		S		S	S			X	X
BAI04	Gestionar La Disponibilidad Y La Capacidad										
BAI05	Gestionar La Facilitación Del Cambio Organizativo										
BAI06	Gestionar Los Cambios	P	P		P	P		S	X	X	X	X
BAI07	Gestionar La Aceptación Del Cambio Y La Transición										
BAI08	Gestionar El Conocimiento										
BAI09	Gestionar Los Activos										
BAI10	Gestionar La Configuración										
	ENTREGA, SERVICIO Y SOPORTE										
DSS01	Gestionar las Operaciones				P	P						X
DSS02	Gestionar las Peticiones y los incidentes Del Servicio										
DSS03	Gestionar los Problemas	P	P		S				X	X	X	X

DSS04	Gestionar La Continuidad	P	S			P			X	X	X	X
DSS05	Gestionar los Servicios De Seguridad			P	P	S	S	S	X	X	X	X
DSS06	Gestionar los Controles De los Procesos Del Negocio											
SUPERVISAR, EVALUAR Y VALORAR												
MEA01	Supervisar, Evaluar Y Valorar El Rendimiento Y La Conformidad											
MEA02	Supervisar, Evaluar Y Valorar El Sistema De Control Interno											
MEA03	Supervisar, Evaluar Y Valorar La Conformidad De Los Requerimientos Externos											

Elaborado por: RVRG

COSO (Sponsoring Organizations of the Treadway) establece una ponderación para el grado de impacto que tienen los criterios de información dentro de un proceso, además de permitir determinar el nivel de riesgo que tendría dicho proceso, para lo cual establece rangos de calificación para los niveles bajo, medio alto; como se puede apreciar en la siguiente tabla.

IMPACTO	CALIFICACIÓN %		PROMEDIO
BAJO	15%	50%	**32%**
MEDIO	51%	75%	**63**
ALTO	76%	95%	**86**
VACÍO	-	-	-

Figura 27: Manejo de riesgos COSO
Fuente: Marco de referencia COSO

Tomando en cuenta la propuesta de COSO, podemos dar los valores promedios al impacto de los criterios de información establecidos en COBIT dentro de cada proceso, luego comenzamos a asignar estos valores en la siguiente tabla, donde el 86% significa que el grado de impacto es primario, el 63% cuando el grado de impacto es secundario y en blanco cuando no existe impacto alguno.

Tabla 4: **Promedio de Impacto**

IMPACTO	PROMEDIO
Bajo	32%
Medio	63%
Alto	86%

Fuente: COBIT

A continuación se colocaran los valores obtenidos en los criterios de información que establece COBIT:

Tabla 5: Valores promedios al impacto de los criterios de información

OBJETIVOS DE CONTROL DE COBIT		CRITERIO DE INFORMACIÓN						
		Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
EVALUAR, ORIENTAR Y SUPERVISAR								
EDM01	Asegurar El Establecimiento Y Mantenimiento Del Marco De Gobierno							
EDM02	Asegurar La Entrega De Beneficios							
EDM03	Asegurar La Optimización Del Riesgo							

EDM04	Asegurar La Optimización De los Recursos							
EDM05	Asegurar La Transparencia Hacia Las Partes Interesadas							
ALINEAR, PLANIFICAR Y ORGANIZAR								
APO01	Gestionar el Marco de Gestión de TI							
APO02	Gestionar la Estrategia							
APO03	Administrar la Arquitectura Empresarial	0.86	0.63	0.63	0.63			
APO04	Gestionar la Innovación							
APO05	Gestionar La Cartera							
APO06	Gestionar El Presupuesto Y Los Costes							
APO07	Gestionar Los Recursos Humanos							
APO08	Gestionar Las Relaciones							
APO09	Gestionar Los Acuerdos De Servicio							
APO10	Gestionar Los Proveedores							
APO11	Gestionar La Calidad	0.86	0.63			0.86	0.63	
APO12	Gestionar El Riesgo	0.63	0.63	0.86	0.86	0.86	0.63	0.63
APO13	Gestionar La Seguridad							

CONSTRUIR, ADQUIRIR E IMPLEMENTAR							
BAI01	Gestionar Los Programas Y Proyectos						
BAI02	Gestionar La Definición De Requisitos						
BAI03	Gestionar La Identificación Y La Construcción De Soluciones	0.86	0.86	0.63		0.63	0.63
BAI04	Gestionar La Disponibilidad Y La Capacidad						
BAI05	Gestionar La Facilitación Del Cambio Organizativo						
BAI06	Gestionar Los Cambios	0.86	0.86	0.86	0.86		0.63
BAI07	Gestionar La Aceptación Del Cambio Y La Transición						
BAI08	Gestionar El Conocimiento						
BAI09	Gestionar Los Activos						
BAI10	Gestionar La Configuración						
ENTREGA, SERVICIO Y SOPORTE							
DSS01	Gestionar Operaciones			0.86	0.86		
DSS02	Gestionar Peticiones y los E Incidentes De Servicio						
DSS03	Gestionar los Problemas	0.86	0.86	0.63			
DSS04	Gestionar La Continuidad	0.86	0.86		0.86		

DSS05	Gestionar los Servicios De Seguridad	0.86	0.86	0.63	0.63	0.63
DSS06	Gestionar los Controles De los Procesos De Negocios					
SUPERVISAR, EVALUAR Y VALORAR						
MEA01	Supervisar, Evaluar Y Valorar El Rendimiento Y La Conformidad					
MEA02	Supervisar, Evaluar Y Valorar El Sistema De Control Interno					
MEA03	Supervisar, Evaluar Y Valorar La Conformidad De Los Requerimientos Externos					

Elaborado por: RVRG

Una vez que se han especificados los valores a cada uno de los Criterios de información se procede a utilizarlos en un cálculo entre el nivel de madurez de cada proceso establecido por COBIT. El total ideal, es la suma de cada uno de los criterios, cuando se asigna a todos los procesos el nivel de madurez 5, siendo este el valor ideal al que la empresa debería llegar, obteniéndolo del resultado de la multiplicación entre cada criterio de información y el nivel de madurez tal como se especificó anteriormente.
Por último se obtiene el porcentaje que se lo relacionara con el valor real establecido por COBIT y el valor ideal, para posteriormente demostrar a través de gráficos estadísticos, cada uno de los criterios.

Se mostrara a continuación un análisis de los modelos de madurez de COBIT por cada proceso seleccionado anteriormente, para determinar el nivel de grado de madurez:

Tabla 6: Modelo de Madurez APO03

DOMINIO: ALINEAR, PLANIFICAR Y ORGANIZAR				
APO03 Administrar la Arquitectura Empresarial				
Descripción: Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Definir los requisitos para la taxonomía, las normas, las directrices, los procedimientos, las plantillas y las herramientas y proporcionar un vínculo para estos componentes. Mejorar la adecuación, aumentar la agilidad, mejorar la calidad de información y generar ahorros de costes potenciales mediante iniciativas tales como la reutilización de bloques de componentes para los procesos de construcción. asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado				
Propósito del Proceso: Representar a los diferentes módulos que componen la empresa y sus interrelaciones, así como los principios rectores de su diseño y evolución en el tiempo, permitiendo una entrega estándar, sensible y eficiente de los objetivos operativos y estratégicos				
APO03.01 Desarrollar la visión de la arquitectura de referencia.				
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.				
NIVEL DE LOS MODELOS DE MADUREZ / **CRITERIO**		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
Nivel 0 ***Incompleto***	Carencia de la importancia de la arquitectura de información en el Centro de Datos que este	X		**GRADO DE MADUREZ**

	alineada con algún estándar o buena práctica. El conocimiento, la experiencia y las responsabilidades necesarias para desarrollar esta arquitectura no existen en la organización.		El proceso de Administrar la Arquitectura Empresarial está en el nivel de madurez **3.**
Nivel 1 ***Ejecutado***	Existe evidencia que la entidad ha reconocido la necesidad de alinear la arquitectura de la información en el centro de datos con algún estándar relacionado. La infraestructura no se encuentra correctamente organizada y no se han tomado medidas para mejorar dicha infraestructura. El desarrollo de algunos componentes de una arquitectura de información ocurre de manera inicial. Existe una comunicación esporádica e inconsistente de la necesidad de una arquitectura de información.	X	
Nivel 2 ***Gestionado***	Surge un proceso de implementar una arquitectura de información en el centro de datos y existen procedimientos similares, aunque intuitivos e informales, que se siguen por distintos individuos dentro de la organización. Las personas	X	

	obtienen sus habilidades al construir la arquitectura de información por medio de experiencia práctica y la aplicación repetida de técnicas.		
Nivel 3 ***Establecido***	Se entiende y se acepta la importancia de la arquitectura de información en el centro de datos, y la responsabilidad de su aplicación se asigna y se comunica de forma clara. Los procedimientos, herramientas y técnicas relacionados, aunque no son sofisticados, se han estandarizado y documentado y son parte de actividades informales de entrenamiento. Se han desarrollado políticas básicas de arquitectura de información, incluyendo algunos requerimientos estratégicos, aunque el cumplimiento de políticas, estándares y herramientas no se refuerza de manera consistente.	X	
Nivel 4 ***Predecible***	Se da soporte completo al desarrollo e implantación de la arquitectura de información del centro de datos por medio de métodos y técnicas formales. Se han identificado métricas		X

	básicas y existe un sistema de medición	
Nivel 5 ***Optimizado***	La arquitectura de información en el centro de datos es reforzada de forma consistente a todos los niveles. El valor de la arquitectura de información para el negocio se enfatiza de forma continua. El personal de TI cuenta con la experiencia y las habilidades necesarias para desarrollar y dar mantenimiento a una arquitectura de información robusta y sensible que refleje todo los requerimientos del negocio. Toda la arquitectura de información en el centro de datos se encuentra correctamente alineada con los estándares y con las mejores prácticas actuales.	X

Fuente: Poder Judicial del Santa – Chimbote
Elaborado por: RVRG

HALLAZGOS

- La arquitectura de información no se encuentra correctamente alineada con los estándares y con las mejores prácticas actuales.

RECOMENDACIONES

- Tomar responsabilidad sobre el desempeño del proceso de desarrollo de la arquitectura de información.

- Identificar las métricas básicas e implementar un sistema de medición.
- Reforzar de forma consistente la arquitectura de información a todos los niveles.

ESTÁNDARES RELACIONADOS AL PROCESO ANALIZADO:

- TOGAF 9

Recursos en TI necesarios para alcanzar los objetivos de negocio:

OBJETIVOS DE CONTROL DE COBIT		RECURSOS DE TI			
—		Personas	Información	Aplicación	Infraestructura
	ALINEAR, PLANIFICAR Y ORGANIZAR				
APO03	Evaluar y administrar riesgos de TI		X	X	X

Figura 28:" Recursos de TI APO03"
Elaborado por: RVRG

Tabla 7: Modelo de Madurez APO11

DOMINIO: ALINEAR, PLANIFICAR Y ORGANIZAR
APO11 Gestionar la Calidad
Descripción: 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.
Propósito del Proceso: Asegurar la entrega consistente de soluciones y servicios que cumplan con los requisitos de la organización y que satisfagan las necesidades de las partes interesadas.
APO11.01 Establecer un sistema de gestión de la calidad (SGC).
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.

NIVEL DE LOS MODELOS DE MADUREZ / **CRITERIO**		**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
Nivel 0 ***Incompleto***	La organización no ha reconocido que existe un problema que debe ser reconocido.	X		**GRADO DE MADUREZ** El proceso de Gestionar la Calidad está en el nivel de madurez **1.**
Nivel 1 ***Ejecutado***	Hay evidencia de que la organización ha reconocido que los problemas existen y que necesiten ser resueltos. Sin embargo, no hay procesos estandarizados pero en cambio hay métodos iniciales que tienen a ser aplicados en forma individual o caso por caso. El método general de la administración es desorganizado.	X		
Nivel 2 ***Gestionado***	Los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. Hasta un alto grado de confianza en los conocimientos de las		X	

	personas y por lo tanto es probable que haya errores.	
Nivel 3 ***Establecido***	Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.	X
Nivel 4 ***Predecible***	Es posible monitorear y medir el cumplimiento de los procedimientos y emprender acción donde los procesos parecen no estar funcionando efectivamente. Los procesos están bajo constante mejoramiento y proveen buena práctica.	X
Nivel 5 ***Optimizado***	Los procesos han sido refinados hasta un nivel de la mejor práctica, basados en los resultados de mejoramiento continuo y	X

	diseño de la madurez con otras organizaciones.

Fuente: Poder Judicial del Santa - Chimbote
Elaborado por: RVRG

HALLAZGOS

- No hay capacitación o comunicación formal de procedimientos estándar y la responsabilidad se deja a la persona.

RECOMENDACIONES

- Comunicar, estandarizar y documentar los procedimientos a través de capacitación.
- Monitorear y medir el cumplimiento de los procedimientos y emprender acción donde los procesos parecen no estar funcionando efectivamente.

ESTÁNDARES RELACIONADOS AL PROCESO ANALIZADO:

- ISO/IEC 9001:2008

Recursos en TI necesarios para alcanzar los objetivos de negocio:

OBJETIVOS DE CONTROL DE COBIT		RECURSOS DE TI			
		Personas	Información	Aplicación	Infraestructura
ALINEAR, PLANIFICAR Y ORGANIZAR					
APO11	Gestionar La Calidad	X		X	

Figura 29:" Recursos de TI APO11".

Tabla 8: Modelo de Madurez APO12

DOMINIO: ALINEAR, PLANIFICAR Y ORGANIZAR			
APO12 Gestionar el Riesgo *Descripción: 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 con TI con la gestión de riesgos empresarial general (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI.* *APO12.01 Recopilar datos.* *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 riesgo.* *APO12.06 Responder al riesgo.*			
NIVEL DE MODELOS DE MADUREZ / **CRITERIO**	**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
Nivel 0 ***Incompleto***	La estimación del riesgo para los procesos y las decisiones del negocio no ocurre. La organización no considera los impactos del negocio asociados con vulnerabilidades de la seguridad y con inseguridades de proyectos de desarrollo. Es improbable que la administración de riesgos sea identificada dentro del pan de un proyecto o sea asignado a	X	**GRADO DE MADUREZ** El proceso de Gestionar el Riesgo está en el nivel de madurez **2.**

	administradores específicos involucrados en el proyecto.		
Nivel 1 ***Ejecutado***	La organización está consciente de sus responsabilidades y obligaciones legales y contractuales, pero considera los riesgos de TI de manera inicial, sin seguir procesos o políticas definidas. Tienen lugar evaluaciones informales del riesgo de proyecto a medida que lo determina cada proyecto. No es probable que las evaluaciones de riesgo sean identificadas específicamente dentro del plan de un proyecto o a ser asignado a administradores específicos involucrados en el proyecto.	X	
Nivel 2 ***Gestionado***	Existe un enfoque de evaluación de riesgos en desarrollo y se implementa a discreción de los gerentes de proyecto. La administración de riesgos se da por lo general a alto nivel y típicamente se aplica solo a proyectos grandes o como respuesta a problemas.	X	•

Nivel 3 ***Establecido***	La política de manejo del riesgo a nivel de toda una organización define cuando y como llevar a cabo evaluaciones de riesgo. La evaluación del riesgo sigue un proceso definido que está documentado y disponible para todo persona a través de entrenamiento. La metodología es convincente y saludable, y asegura que los riesgos clave del negocio probablemente sean identificados.	X
Nivel 4 ***Predecible***	La evaluación del riesgo es un procedimiento estándar y las excepciones a seguir el procedimiento serian anunciadas por la administración de TI. Es probable que la administración del riesgo sea una función definida de la administración con responsabilidad a nivel general. La administración puede monitorear la posición del riesgo y tomar decisiones inteligentes respecto a la exposición que está dispuesta a aceptar.	X

Nivel 5 ***Optimizado***	La evaluación de los riesgos se ha desarrollado hasta una etapa en que un proceso estructurado, en toda la organización, es ejecutado, seguido y bien administrado. La tormenta de ideas y el análisis de la causa que originó el riesgo, que involucra a personas expertas, se aplican en toda la organización. La administración del riesgo está verdaderamente integrada en todas las operaciones y negocios de TI es bien aceptada e involucra extensamente a los usuarios de servicios de TI.	X

Fuente: Poder Judicial del Santa - Chimbote
Elaborado por: RVRG

HALLAZGOS

- La evaluación del riesgo no sigue un proceso definido.

RECOMENDACIONES

- Implementar un proceso definido para la evaluación del riesgo, documentarlo y poner disponibilidad para todo persona a través de entrenamiento.
- Realizar una metodología convincente y saludable, para asegurar que los riesgos claves del negocio sean identificados.
- Establecer una base de datos de administración de Riesgos.

ESTÁNDARES RELACIONADOS AL PROCESO ANALIZADO:

- ISO/IEC 27001:2005: Sistemas de gestión de la seguridad de información - Requerimientos, Sección 4
- ISO/IEC 27002:2011
- ISO/IEC 31000: 6. Procesos para la Gestión del Riesgos

Recursos en TI necesarios para alcanzar los objetivos de negocio:

OBJETIVOS DE CONTROL DE COBIT		RECURSOS DE TI			
		Personas	Información	Aplicación	Infraestructura
ALINEAR, PLANIFICAR Y ORGANIZAR					
APO12	Gestionar El Riesgo	X	X	X	X

Figura 30:" Recursos de TI APO12"

Tabla 9: Modelo de Madurez BAI03

DOMINIO: CONSTRUIR, ADQUIRIR E IMPLEMENTAR
BAI03 Gestionar la Identificación y la Construcción de Soluciones
Descripción: Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.
Propósito del Proceso: Establecer soluciones puntuales y rentables capaces de soportar la estrategia de negocio y objetivos operacionales.
BAI03.01 Diseñar soluciones de alto nivel.
BAI03.02 Diseñar los componentes detallados de la solución.
BAI03.03 Desarrollar los componentes de la solución.
BAI03.04 Obtener los componentes de la solución.

BAI03.05 Construir soluciones.

BAI03.06 Realizar controles de calidad.

BAI03.07 Preparar pruebas de la soluciones.

BAI03.08 Ejecutar pruebas de la solución.

BAI03.09 Gestionar cambios a los requerimientos.

BAI03.10 Mantener soluciones.

BAI03.11 Definir los servicios TI y mantener el catálogo de servicios.

NIVEL DE MODELOS DE MADUREZ / CRITERIO		CUMPLE	NO CUMPLE	OBSERVACIONES
Nivel 0 ***Incompleto***	No se reconoce la administración de la infraestructura de tecnología como un asunto importante al cual deba ser resuelto. Típicamente, las aplicaciones se obtienen con base en ofertas de proveedores, en el reconocimiento de la marca o en la familiaridad del personal de TI con productos específicos, considerando poco o nada los requerimientos actuales.	X		**GRADO DE MADUREZ** El proceso de Gestionar el Riesgo está en el nivel de madurez **2.**
Nivel 1 ***Ejecutado***	Se realizan cambios a la infraestructura para cada nueva aplicación, sin ningún plan de conjunto. La actividad de mantenimiento reacciona a necesidades de	X		

	corto plazo. Es probable que se hayan adquirido en forma independiente una variedad de soluciones individuales para requerimientos particulares del negocio, teniendo como resultado ineficiencias en el mantenimiento y soporte.		
Nivel 2 ***Gestionado***	Existen procesos de adquisición y mantenimiento de aplicaciones con diferencias, pero similares, en base a la experiencia dentro de la operación de TI. La adquisición y mantenimiento de la infraestructura de TI no se basa en una estrategia definida y no considera las necesidades de las aplicaciones del negocio que ser debe respaldar.	X	
Nivel 3 ***Establecido***	Existe un proceso claro, definido y de comprensión general para la adquisición y mantenimiento de software aplicativo. Este proceso va de acuerdo con la estrategia		X

	de TI y del negocio. El proceso respalda las necesidades de las aplicaciones críticas del negocio y concuerda con la estrategia de negocio de TI, pero no se aplica en forma consistente.	
Nivel 4 ***Predecible***	Se desarrolla el proceso de adquisición y mantenimiento de la infraestructura de tecnología a tal punto que funciona bien para la mayoría. El proceso está bien organizado y es preventivo. Existe una metodología formal y bien comprendida que incluye un proceso de diseño y especificación, un criterio de adquisición, un proceso de prueba y requerimientos para la documentación.	X

Nivel 5 ***Optimizado***	Las buenas prácticas se aplican en toda la organización. El enfoque se extiende para toda la empresa. La metodología de adquisición y mantenimiento presenta un buen avance y permite un posicionamiento estratégico rápido, que permite un alto grado de reacción y flexibilidad para responder a requerimientos cambiantes del negocio.	X

Fuente: Poder Judicial del Santa – Chimbote
Elaborado por: RVRG

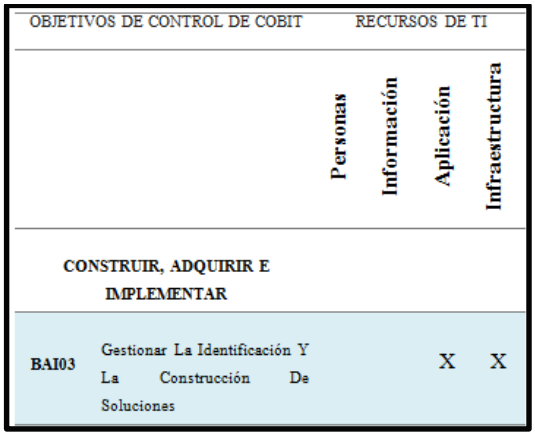
HALLAZGOS

- La adquisición y mantenimiento de la infraestructura de TI no se basa en una estrategia definida y no considera las necesidades de las aplicaciones del negocio que ser deben respaldar.

RECOMENDACIONES

- Dar existencia a un proceso de acuerdo con la estrategia de TI y del negocio; claro, definido, y de comprensión general para la adquisición y mantenimiento de software aplicativo.
- Automatizar altamente la captura, análisis y reporte de los datos de administración de riesgos.

Recursos en TI necesarios para alcanzar los objetivos de negocio:



OBJETIVOS DE CONTROL DE COBIT		RECURSOS DE TI			
		Personas	Información	Aplicación	Infraestructura
CONSTRUIR, ADQUIRIR E IMPLEMENTAR					
BAI03	Gestionar La Identificación Y La Construcción De Soluciones			X	X

Figura 31:" Recursos de TI BAI03".

Tabla 10: Modelo de Madurez BAI06

DOMINIO: CONSTRUIR, ADQUIRIR E IMPLEMENTAR

BAI06 Gestionar los cambios

Descripción: Gestione todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación.

Propósito del Proceso: Posibilitar una entrega de los cambios rápida y fiable para el negocio, a la vez que se mitiga cualquier riesgo que impacte negativamente en la estabilidad e integridad del entorno en que se aplica el cambio.

BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio.

BAI06.02 Gestionar cambios de emergencia.

BAI06.03 Hacer seguimiento e informar de cambios de estado.

BAI06.04 Cerrar y documentar los cambios.

NIVEL DE MODELOS DE MADUREZ / CRITERIO	CUMPLE	NO CUMPLE	OBSERVACIONES

Nivel 0 ***Incompleto***	No hay un proceso definido de administración de cambios y se pueden hacer cambios prácticamente sin control alguno. No hay conciencia de que los cambios pueden causar interrupciones tanto para TI como para las operaciones de negocios, y ninguna conciencia de los beneficios de una buena administración de cambios.	X	
Nivel 1 ***Ejecutado***	Se reconoce que los cambios deben ser administrados y controlados, pero no hay un proceso consistente para seguimiento. Las prácticas varían y es probable que ocurran cambios no autorizados. Hay documentación insuficiente o inexistente de cambios, y la documentación de configuración está incompleta y no es confiable. Es probable que ocurran errores junto con interrupciones en el entorno de producciones	X	**GRADO DE MADUREZ** El proceso de Gestionar los Cambios está en el nivel de madurez 2.

	causadas por una administración deficiente del cambio.	
Nivel 2 ***Gestionado***	Hay un proceso informal de administración de cambios y la mayoría de los cambios siguen este método sin embargo, el mismo no está estructurado, es rudimentario y esta propenso a error. La precisión de la documentación de configuración es inconsistente y solo tiene lugar una planeación y un estudio de impacto limitados antes de un cambio. Hay considerable ineficiencia y repetición de trabajo.	X
Nivel 3 ***Establecido***	Está establecido un proceso formal de administración de cambios, que incluye procedimientos de categorización, priorización, emergencia, autorización y administración de cambios,	X

	pero no se impone su cumplimiento. El proceso definido no siempre es visto como adecuado o practico y, en consecuencia, ocurren trabajos paralelos y los procesos son desviados.	
Nivel 4 ***Predecible***	El proceso de administración de cambios está bien desarrollado y es seguido de manera consistente para todos los cambios, y la administración confía en que no hay excepciones. El proceso es eficiente y efectivo, pero se basa en considerables procedimientos y controles manuales para asegurar que se logre la calidad. La documentación de la configuración está generalmente actualizada.	X
Nivel 5 ***Optimizado***	El proceso de administración de cambios es revisado y actualizado regularmente para	X

	mantener en línea con las mejores prácticas. La información de configuración es automatizada y provee control de versiones. La administración de configuración y liberación y rastreo de cambios es sofisticado e incluye herramientas para detectar software no autorizado y sin licencia.	

Fuente: Poder Judicial del Santa - Chimbote
Elaborado por: RVRG

HALLAZGOS

- No está establecido un proceso formal de administración de cambios.

RECOMENDACIONES

- Establecer un proceso formal de administración de cambios, que incluya procedimientos de categorización, priorización, emergencia, autorización y administración de cambios e imponer su cumplimiento.
- Una mayor coordinación entre la administración de cambios de TI y el rediseño del proceso de negocios.

ESTÁNDARES RELACIONADOS AL PROCESO ANALIZADO:

- ISO/IEC 20000: 9.2 Gestión de cambios
- ITIL V3 2011: 13. Gestión de cambios

Recursos en TI necesarios para alcanzar los objetivos de negocio:

OBJETIVOS DE CONTROL DE COBIT		RECURSOS DE TI			
		Personas	Información	Aplicación	Infraestructura
CONSTRUIR, ADQUIRIR E IMPLEMENTAR					
BAI06	Gestionar Los Cambios	X	X	X	X

Figura 32:" Recursos de TI BAI06".

Tabla 11: Modelo de Madurez DSS01

DOMINIO: ENTREGA, SERVICIO Y SOPORTE

DSS01 Gestionar Operaciones

Descripción: Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.

Propósito del Proceso: Entregar los resultados del servicio operativo de TI, según lo planificado.

DSS01.01 Ejecutar procedimientos operativos.

DSS01.02 Gestionar servicios externalizados de TI

DSS01.03 Supervisar la infraestructura de TI.

DSS01.04 Gestionar el entorno.

DSS01.05 Gestionar las instalaciones.

NIVEL DE MADUREZ / CRITERIO	CUMPLE	NO CUMPLE	OBSERVACIONES

Nivel 0 ***Incompleto***	No hay conciencia sobre la necesidad de proteger las instalaciones o la inversión en recursos de cómputo. Los factores ambientales tales como protección contra fuego, polvo, tierra y exceso de calor y humedad no se controlan ni se monitorean.	X	**GRADO DE MADUREZ** El proceso de Gestionar las operaciones está en el nivel de madurez 2.
Nivel 1 ***Ejecutado***	La organización reconoce la necesidad de contar con un ambiente físico que proteja los recursos y el personal contra peligros naturales y causados por el hombre. La administración de instalaciones y de equipo depende de las habilidades de Individuos clave.	X	
Nivel 2 ***Gestionado***	Los controles ambientales se implementan y monitorean por parte del personal de operaciones. La seguridad física es un proceso informal, realizado	X	

	por un pequeño grupo de empleados con alto nivel de preocupación por asegurar las instalaciones Físicas.	
Nivel 3 ***Establecido***	Se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de cómputo controlado. Los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con presupuesto autorizado y rastreado Por la gerencia.	X
Nivel 4 ***Predecible***	Se establecen criterios formales y estandarizados para definir los términos de un acuerdo, incluyendo alcance del trabajo, servicios/entregables a suministrar, suposiciones, cronograma, costos, acuerdos de facturación y responsabilidades. Hay un plan acordado a largo plazo para las instalaciones requeridas para soportar el	X

	ambiente cómputo de la organización.	
Nivel 5 ***Optimizado***	Los estándares están definidos para todas las instalaciones, incluyendo la selección del centro de cómputo, construcción, vigilancia, seguridad personal, sistemas eléctricos y mecánicos, protección contra factores ambientales (por ejemplo, fuego, rayos, inundaciones, etc.).	X

Fuente: Poder Judicial del Santa - Chimbote
Elaborado por: RVRG

HALLAZGOS

- No hay un plan largo para las instalaciones que se requiriesen que soporte el entorno de informática de la organización.

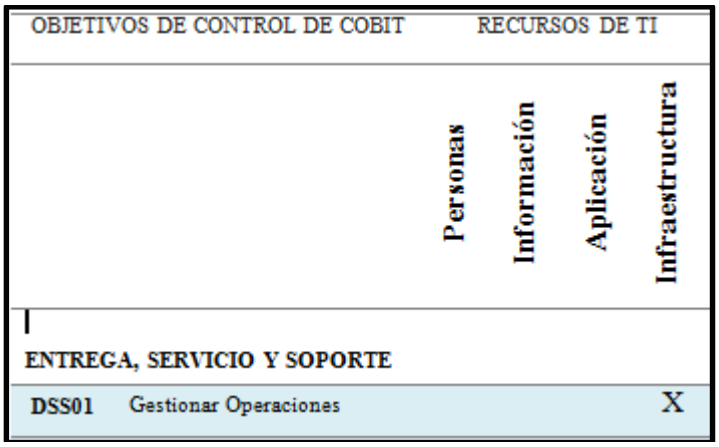
RECOMENDACIONES

- Los requerimientos ambientales y de seguridad física deban estar documentados y el acceso tiene que ser estrictamente controlado y monitoreado.
- Definir Las normas para todas las instalaciones, abarcando la selección del sitio, la construcción, custodia, seguridad de personal, sistemas mecánico y eléctrico, protección contra incendio, rayo e inundación

ESTÁNDARES RELACIONADOS AL PROCESO ANALIZADO:

- ITIL V3 2011: 19. Gestión de Eventos y 24. Gestión de Operaciones

Recursos en TI necesarios para alcanzar los objetivos de negocio:



OBJETIVOS DE CONTROL DE COBIT		RECURSOS DE TI			
		Personas	Información	Aplicación	Infraestructura
ENTREGA, SERVICIO Y SOPORTE					
DSS01	Gestionar Operaciones				X

Figura 33:" Recursos de TI DSS01".

Tabla 12: Modelo de Madurez DSS03

DOMINIO: ENTREGAR, SERVICIO Y SOPORTE *DS10*			
DSS03 Gestionar Problemas *Descripción: Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.* *Propósito del Proceso: Incrementar la disponibilidad, mejorar los niveles de servicio, reducir costes, y mejorar la comodidad y satisfacción del cliente reduciendo el número de problemas operativos.* DSS03.01 Identificar y clasificar problemas DSS03.02 Investigar y diagnosticar problemas. DSS03.03 Levantar errores conocidos. DSS03.04 Resolver y cerrar problemas. DSS03.05 Realizar una gestión de problemas proactiva.			
NIVEL DE LOS MODELOS DE MADUREZ / **CRITERIO**	**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
Nivel 0 ***Incompleto***	No hay conciencia sobre la necesidad de administrar problemas, y no hay diferencia entre problemas	X	**GRADO DE MADUREZ** El proceso de Gestionar Problemas está en el nivel de madurez 2.

	e incidentes. Por lo tanto, no se han hecho intentos por identificar la causa raíz de los incidentes		
Nivel 1 ***Ejecutado***	Los individuos reconocen la necesidad de administrar los problemas y de revolver las causas de fondo. Algunos individuos expertos clave brindan asesoría sobre problemas relacionados a su área de experiencia, pero no está asignada la responsabilidad para la administración de problemas.	X	
Nivel 2 ***Gestionado***	Hay una amplia conciencia sobre la necesidad y los beneficios de administrar los problemas relacionados con TI, tanto dentro de las áreas de negocio como en la función de servicios de información.	X	
Nivel 3 ***Establecido***	Se acepta la necesidad de un sistema integrado de administración de problemas y se evidencia con el apoyo de la gerencia		X

	y la asignación de presupuesto para personal y habilitación. Se estandarizan los procesos de escalamiento y resolución de problemas.	
Nivel 4 ***Predecible***	El proceso de administración de problemas se entiende a todos los niveles de la organización. Las responsabilidades y la propiedad de los problemas están claramente establecidas.	X
Nivel 5 ***Optimizado***	El proceso de administración de problemas ha evolucionado a un proceso proactivo y preventivo, que contribuye con los objetivos de TI. Los problemas se anticipan y previenen. El conocimiento respecto a patrones de problemas pasados y futuros se mantiene a través de contactos regulares con proveedores y expertos.	X

Fuente: Poder Judicial del Santa - Chimbote

Elaborado por: RVRG

HALLAZGOS

- No se cuenta con un sistema integrado de administración de problemas.

RECOMENDACIONES

- Implementar un sistema integrado de administración de problemas con el apoyo de la gerencia y la asignación de presupuesto para personal y habilitación.
- Documentar, comunicar y medir los métodos y los procedimientos para evaluar la efectividad.

ESTÁNDARES RELACIONADOS AL PROCESO ANALIZADO:

- ISO/IEC 20000: 8.3 Gestión de problemas
- ITIL V3 2011: 22. Gestión de Problemas

Recursos en TI necesarios para alcanzar los objetivos de negocio:

OBJETIVOS DE CONTROL DE COBIT		RECURSOS DE TI			
		Personas	Información	Aplicación	Infraestructura
ENTREGA, SERVICIO Y SOPORTE					
DSS03	Gestionar Problemas	X	X	X	X

Figura 34:" Recursos de TI DSS03".

Tabla 13: Modelo de Madurez DSS04

DOMINIO: ENTREGA, SERVICIO Y SOPORTE
DSS04 Gestionar la Continuidad
Descripción: Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener

la disponibilidad de la información a un nivel aceptable para la empresa.

<u>Propósito del Proceso</u>: Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa

DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance.

DSS04.02 Mantener una estrategia de continuidad.

DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.

DSS04.04 Ejercitar, probar y revisar el plan de continuidad.

DSS04.05 Revisar, mantener y mejorar el plan de continuidad.

DSS04.06 Proporcionar formación en el plan de continuidad.

DSS04.07 Gestionar acuerdos de respaldo.

DSS04.08 Ejecutar revisiones post-reanudación.

NIVEL DE MADUREZ / CRITERIO		CUMPLE	NO CUMPLE	OBSERVACIONES
Nivel 0 ***Incompleto***	No hay entendimiento de los riesgos, vulnerabilidades y amenazas de las operaciones de TI o del impacto de la pérdida de los servicios de TI para el negocio. Los datos no son reconocidos como parte de los recursos y los activos de la empresa. No está asignada la propiedad sobre los datos o sobre la rendición de cuentas individual sobre la	X		**GRADO DE MADUREZ** El proceso de Gestionar la Continuidad está en el nivel de madurez 2.

	administración de los datos. La calidad y la seguridad de los datos son deficientes o inexistentes.	
Nivel 1 ***Ejecutado***	Las responsabilidades de servicio continuo son informales, con autoridad limitada. La administración se está volviendo consciente de los riesgos relacionados con el servicio continuo y de la necesidad de éste. La organización reconoce la necesidad de una correcta administración de los datos. Hay un método adecuado para especificar requerimientos de seguridad en la administración de datos, pero no hay procedimientos implementados de comunicación formal.	X
Nivel 2 ***Gestionado***	La responsabilidad del servicio continuo está asignada. Los enfoques del servicio continuo son	X

	fragmentados. El reporte sobre la disponibilidad del sistema es incompleto y no toma en cuenta el impacto sobre el negocio. Existe un inventario razonablemente confiable de sistemas críticos y componentes. A lo largo de toda la organización existe conciencia sobre la necesidad de una adecuada administración de los datos. A un alto nivel empieza a observarse la propiedad o responsabilidad sobre los datos.	
Nivel 3 ***Establecido***	Los planes están documentados y se basan en la importancia del sistema y en el impacto sobre el negocio. Se mantiene rigurosamente un inventario de sistemas críticos y componentes. Se entiende y acepta la necesidad de la administración de datos, tanto dentro de TI como a lo largo de toda la	X

	organización. Se establece la responsabilidad sobre la administración de los datos. Se asigna la propiedad sobre los datos a la parte responsable que controla la integridad y la seguridad.	
Nivel 4 ***Predecible***	Se hacen cumplir las responsabilidades y las normas para el servicio continuo. Los incidentes de falta de continuidad son clasificados y el paso cada vez mayor de escala para cada uno es bien conocido para todos los que están involucrados. Se entiende la necesidad de la administración de los datos y las acciones requeridas son aceptadas a lo largo de toda la organización. La responsabilidad de la propiedad y la administración de los datos están definidas, asignada y comunicada de forma clara en la organización.	X

Nivel 5 ***Optimizado***	Los procesos de servicio continuo son proactivo, se ajustan solos, son automatizados y auto analíticos y toman en cuenta puntos de referencia y las mejores prácticas externas. Se entiende y acepta dentro de la organización la necesidad de realizar todas las actividades requeridas para la administración de datos. Las necesidades y los requerimientos futuros son explorados de manera proactiva.	X

Fuente: Poder Judicial del Santa - Chimbote
Elaborado por: RVRG

HALLAZGOS

- El reporte sobre la disponibilidad es incompleto y no toma en cuenta el impacto sobre el negocio.

RECOMENDACIONES

- Mantener rigurosamente un inventario de sistemas críticos y componentes.
- Asignar la responsabilidad de mantener el plan de servicio continuo.
- Recopilar, analizar, reportar y ejecutar datos estructurados sobre el servicio continuo.

ESTÁNDARES RELACIONADOS AL PROCESO ANALIZADO:

- BS 25999:2007: Norma de Continuidad de Negocio
- ISO/IEC 20000: 6.3 Gestión de la continuidad y disponibilidad de servicios.
- ISO/IEC 27002:2011: 14. Gestión de la Continuidad de Negocio
- ITL V3 2011: 9. Gestión de la Continuidad de Servicios de TI

Recursos en TI necesarios para alcanzar los objetivos de negocio:

OBJETIVOS DE CONTROL DE COBIT		RECURSOS DE TI			
		Personas	Información	Aplicación	Infraestructura
ENTREGA, SERVICIO Y SOPORTE					
DSS04	Gestionar La Continuidad	X	X	X	X

Figura 35:" Recursos de TI DSS04"

Tabla 14: Modelo de Madurez DSS05

DOMINIO: ENTREGAR, SERVICIO Y SOPORTE

DSS05 Gestionar los Servicios de Seguridad

Descripción: Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.

Propósito del Proceso: Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.

DSS05.01 Proteger contra software malicioso (malware).

DSS05.02 Gestionar la seguridad de la red y las conexiones.

DSS05.03 Gestionar la seguridad de los puestos de usuario final.

DSS05.04 Gestionar la identidad del usuario y el acceso lógico.

DSS05.05 Gestionar el acceso físico a los activos de TI.

DSS05.06 Gestionar documentos sensibles y dispositivos de salida.

DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con

la seguridad.

NIVEL DE MODELOS DE MADUREZ / CRITERIO		CUMPLE	NO CUMPLE	OBSERVACIONES
Nivel 0 ***Incompleto***	La organización no reconoce la necesidad de la seguridad de TI. Las responsabilidades y las obligaciones de reportar no están asignadas para asegurar la seguridad. No están implementadas medidas que soporten la administración de la seguridad de TI. Hay una carencia total de un proceso reconocible de administración de seguridad de sistemas.	X		**GRADO DE MADUREZ** El proceso de Gestionar los Servicios de Seguridad está en el nivel de madurez 2.
Nivel 1 ***Ejecutado***	La organización reconoce la necesidad de la seguridad de TI, pero la conciencia de la seguridad depende de la persona. La seguridad de TI está resuelta de manera reactiva y no se mide. Las respuestas a las violaciones de seguridad de TI invocan respuestas de "señalamiento" si se detectan, porque las responsabilidades no están claras.	X		

Nivel 2 ***Gestionado***	Las responsabilidades y obligaciones de la seguridad de TI están asignadas a un coordinador de seguridad de TI que no tiene autoridad de administración. La conciencia de seguridad es fragmentada y limitada. La información de seguridad de TI es generada, pero no es analizada. Se están desarrollando políticas de seguridad, pero aún se siguen usando habilidades y herramientas inadecuadas. El reporte de seguridad de TI es incompleto, engañoso y no es pertinente.	X
Nivel 3 ***Establecido***	Existe conciencia de la seguridad y la misma es promovida por la administración. Se han estandarizado y formalizados reportes de conocimientos de la seguridad. Los procedimientos de seguridad de TI están definidos y encajan en una estructura para políticas y procedimientos de seguridad. Las responsabilidades de seguridad de TI están	

	asignadas, pero no se hacen cumplir de manera consistente. El reporte de seguridad de TI está concentrado en TI, en lugar de concentrarse en el negocio.	
Nivel 4 ***Predecible***	Las responsabilidades de la seguridad de TI están claramente asignadas, administradas y se hacen cumplir. El análisis de riesgo e impacto de seguridad se lleva a cabo de manera consistente. Las políticas y prácticas de seguridad son completadas con bases específicas de seguridad. Los reportes de conocimientos de seguridad se han vuelto obligatorios. El reporte de TI está vinculado con los objetivos del negocio.	X
Nivel 5 ***Optimizado***	La seguridad de TI es una responsabilidad conjunta del negocio y de la administración de TI y está integrada con objetivos de seguridad corporativa del negocio. Los requisitos de seguridad están claramente definidos. Los	X

	procesos y las tecnologías de seguridad están integrados en toda la organización.	

Fuente: Poder Judicial del Santa - Chimbote
Elaborado por: RVRG

HALLAZGOS

- No hay un claro plan de análisis de TI, que impulsa el análisis del riesgo y soluciones de seguridad.

RECOMENDACIONES

- Las responsabilidades de la seguridad de TI deben ser claramente asignadas, administradas y se hacerse cumplir.
- Estandarizar la identificación, autentificación y autorización de usuario.
- Hacer evaluaciones periódicas de seguridad para evaluar la efectividad de la implementación del plan de seguridad.
- Recoger y analizar sistemáticamente la información sobre nuevas amenazas y vulnerabilidades para implementar prontamente los controles adecuados de mitigación.

ESTÁNDARES RELACIONADOS AL PROCESO ANALIZADO:

- ISO/IEC 27002:2011: Código de prácticas para la gestión de la seguridad de la información
- NIST SP800-53 Rev 1: Controles de Seguridad Recomendados para los Sistemas de Información Federales en EE.UU.
- ITIL V3 2011: Operación de Servicio, 4.5. Gestión de Acceso

Recursos en TI necesarios para alcanzar los objetivos de negocio:

OBJETIVOS DE CONTROL DE COBIT				RECURSOS DE TI			
				Personas	Información	Aplicación	Infraestructura
ENTREGA, SERVICIO Y SOPORTE							
DSS05	Gestionar Seguridad	Servicios	De	X	X	X	X

Figura 36:" Recursos de TI DSS05".

Tabla 15: Resultados del Grado de Madurez de la Evaluación de la Seguridad del Centro de Datos

Procesos		Niveles					
		Incompleto	Ejecutado	Gestionado	Establecido	Predecible	Optimizado
		0	1	2	3	4	5
APO03	Administrar la Arquitectura Empresarial						
APO11	Gestionar la Calidad						
APO12	Gestionar el Riesgo						
BAI03	Gestionar la Identificación y la Construcción de Soluciones						
BAI06	Gestionar los cambios						
DSS01	Gestionar Operaciones						
DSS03	Gestionar Problemas						

DSS04	Gestionar la Continuidad	
DSS05	Gestionar los Servicios de Seguridad	

Elaborado por: RVRG

	LEYENDA PARA LOS SIMBOLOS USADOS	LEYENDA PARA LAS CLASIFICACIONES USADAS	
	Situación actual de la Institución.	Nivel 0 Incompleto	El proceso no se ha implementado o no logra su propósito.
		Nivel 1 Ejecutado	El proceso implementado logra su propósito.
		Nivel 2 Gestionado	El proceso realizado ahora se implementa de manera gestionada.
		Nivel 3 Establecido	El proceso gestionado ahora se implementa mediante un proceso definido.
		Nivel 4 Predecible	El proceso establecido ahora opera dentro de los límites definidos.
		Nivel 5 Optimizado	El proceso predecible se mejora continuamente para cumplir con las metas de la institución.

Elaborado por: RVRG

Tabla 16: Resumen de procesos y criterios de información por impacto

		CRITERIO DE INFORMACIÓN							
PROCESOS		Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	NIVEL DE MADUREZ
ALINEAR, PLANIFICAR Y ORGANIZAR									
APO 03	Evaluar y administrar riesgos de TI	0.86	0.63	0.63	0.63	0.00	0.00.	0.00	
Total real (impacto* nivel real)		2.58	1.89	1.89	1.89	0.00	0.00	0.00	3
Total ideal (impacto* nivel ideal)		4.30	3.15	3.15	3.15	0.00	0.00	0.00	5
APO 11	Gestionar La Calidad	0.86	0.63	0.00	0.00	0.86	0.63	0.00	
Total real (impacto* nivel real)		0.86	0.63	0.00	0.00	0.86	0.63	0.00	1
Total ideal (impacto* nivel ideal)		4.30	3.15	0.00	0.00	4.30	3.15	0.00	5
APO 12	Gestionar El Riesgo	0.63	0.63	0.86	0.86	0.86	0.63	0.63	
Total real (impacto* nivel real)		1.26	1.26	1.72	1.72	1.72	1.26	1.26	2
Total ideal (impacto* nivel ideal)		3.15	3.15	4.30	4.30	4.30	3.15	3.15	5
CONSTRUIR, ADQUIRIR E IMPLEMENTAR									
BAI 03	Gestionar La Identificación Y La Construcción De Soluciones	0.86	0.86	0.00	0.63	0.00	0.63	0.63	
Total real (impacto* nivel real)		1.72	1.72	0.00	1.26	0.00	1.26	1.26	2
Total ideal (impacto* nivel ideal)		4.30	4.30	0.00	3.15	0.00	3.15	3.15	5
BAI	Gestionar Los Cambios	0.86	0.86	0.00	0.86	0.63	0.00	0.63	

06									
Total real (impacto* nivel real)		1.72	1.72	0.00	1.72	1.26	0.00	1.26	2
Total ideal (impacto* nivel ideal)		4.30	4.30	0.00	4.30	3.15	0.00	3.15	5
ENTREGA, SERVICIO Y SOPORTE									
DSS 01	Gestionar Operaciones	0.00	0.00	0.00	0.86	0.86	0.00	0.00	
Total real (impacto* nivel real)		0.00	0.00	0.00	1.72	1.72	0.00	0.00	2
Total ideal (impacto* nivel ideal)		0.00	0.00	0.00	4.30	4.30	0.00	0.00	5
DSS 03	Gestionar Problemas	0.86	0.86	0.00	0.63	0.00	0.00	0.00	
Total real (impacto* nivel real)		1.72	1.72	0.00	1.26	0.00	0.00	0.00	2
Total ideal (impacto* nivel ideal)		4.30	4.30	0.00	3.15	0.00	0.00	0.00	5
DSS 04	Gestionar La Continuidad	0.86	0.86	0.00	0.00	0.86	0.00	0.00	
Total real (impacto* nivel real)		1.72	1.72	0.00	0.00	0.00	0.00	0.00	2
Total ideal (impacto* nivel ideal)		4.30	4.30	0.00	0.00	4.30	0.00	0.00	5
DSS 05	Gestionar Servicios De Seguridad	0.00	0.00	0.86	0.86	0.63	0.63	0.63	
Total real (impacto* nivel real)		0.00	0.00	1.72	1.72	1.26	1.26	1.26	2
Total ideal (impacto* nivel ideal)		0.00	0.00	4.30	4.30	3.15	3.15	3.15	5

Elaborado por: RVRG

Después de analizar los resultados que nos da la tabla de criterios de información por impacto, se realiza una nueva tabla con los resultados totales, haciendo sumatoria de cada uno de los totales reales en cada criterio evaluado por columna; de la misma manera se suman los totales ideales, y por último el porcentaje alcanzado se halla dividiendo el total real entre el total ideal y al resultado multiplicarlo por 100.

TOTAL REAL	Sumatoria de los totales reales en cada criterio evaluado por columna
TOTAL IDEAL	Sumatoria de los totales ideales en cada criterio evaluado por columna

$$Porcentaje\ Alcanzado = \frac{Total\ Real}{Total\ Ideal} \times 100$$

Tabla 17: Resultados finales del impacto sobre los criterios de información

TOTAL REAL	11.58	10.66	5.33	11.29	6.82	4.41	5.04	
TOTAL IDEAL	28.95	26.65	11.75	26.65	23.50	12.60	12.60	
PORCENTAJE ALCANZADO	40.00	40.00	45.36	42.36	29.02	35.00	40.00	**44.37**

Elaborado por: RVRG

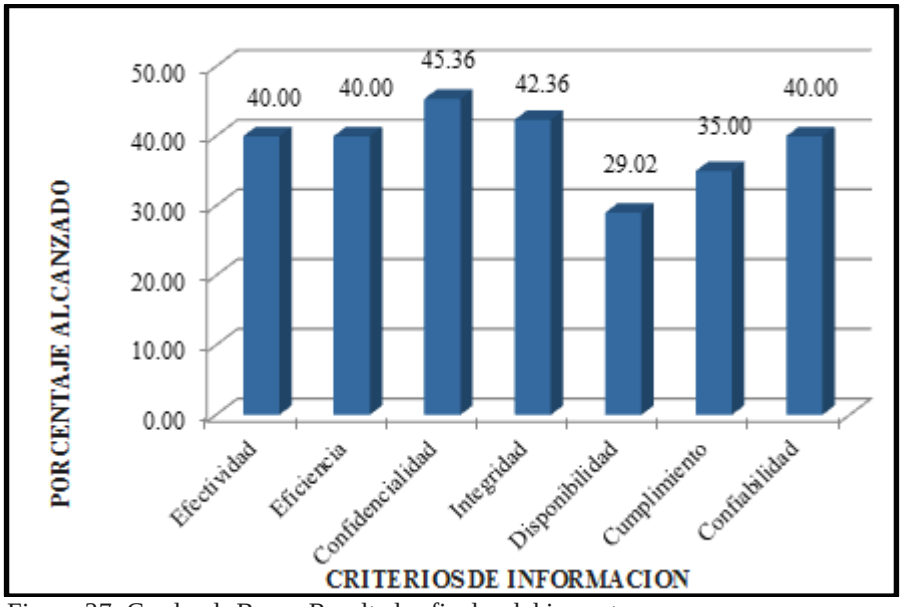


Figura 37: Cuadro de Barras Resultados finales del impacto
Elaborado por: RVRG

A continuación analizamos cada uno de los criterios de la información:

EFECTIVIDAD.- Para este criterio de información se obtuvo un porcentaje del 40.00%

sobre 100%, es decir que la información que es de importancia para el Poder Judicial Del Santa, Chimbote, que tiene incidencia en los procesos del negocio y debe ser entregada de forma oportuna, consistente, y veraz tiene un porcentaje del 40.00% (Ver Tabla 17).

EFICIENCIA.- Para este criterio de información se obtuvo un porcentaje del 40.00% sobre el 100%, es decir que la información que debe generar el uso óptimo de los recursos del Poder Judicial Del Santa, Chimbote tiene un porcentaje del 40.00% (Ver Tabla 17).

CONFIDENCIALIDAD.- Para este criterio de información se obtuvo un porcentaje del 45.36% sobre el 100%, es decir que la protección de la información del Poder Judicial Del Santa para que esta no sea divulgada a personas o sectores extraños a este tiene un porcentaje del 45.36% (Ver Tabla 17).

INTEGRIDAD.- Para este criterio de información se obtuvo un porcentaje del 42.36% sobre el 100%, es decir la distribución de la información exacta y correcta, así como su validez con las expectativas de la empresa tiene un porcentaje del 42.36% (Ver Tabla 17).

DISPONIBILIDAD.- Para este criterio de la información se obtuvo un porcentaje del 29.02% sobre el 100%, es decir la accesibilidad de la información cuando esta sea requerida por los procesos del negocio y a la salvaguarda de los recursos y capacidades asociadas a la misma en del Poder Judicial Del Santa, tiene porcentaje del 29.02% (Ver Tabla 17).

CUMPLIMIENTO.- Para este criterio de la información se obtuvo un porcentaje del 35.00% sobre el 100%, es decir que el cumplimiento de las leyes, regulaciones, y compromisos contractuales con los cuales está comprometido del Poder Judicial Del Santa, tiene un porcentaje del 35.00% (Ver Tabla 17).

CONFIABILIDAD.- Para este criterio de la información se obtuvo un porcentaje del 40.00% sobre el 100%, es decir proveer la información apropiada para que la administración tome decisiones adecuadas para manejar del Poder Judicial Del Santa y cumplir con sus responsabilidades, tiene porcentaje del 40.00% (Ver Tabla 17).

Basándonos en los Resultados de nuestra Evaluación plantearemos Planes de acción de algunos procesos ya analizados en nuestro informe:

Tabla 18: Plan de acción al proceso APO11

PLAN DE ACCIÓN			
DOMINIO	ALINEAR, PLANIFICAR Y ORGANIZAR	PROCESO:	**APO11 GESTIONAR LA CALIDAD**
CONTROLES			
Control a implementar APO11-C1	POLÍTICAS Y PROCEDIMIENTOS RELACIONADOS CON EL ASEGURAMIENTO DE LA CALIDAD		
	La organización deberá desarrollar, diseminar, y periódicamente revisar/actualizar: - Una política de administración del Plan General de la Calidad formalmente definida y documentada. - Procedimientos documentados para facilitar la implantación de la política del plan general de calidad y los controles asociados.		
Responsables de implementación	Encargado de la seguridad de Sistemas		
Plazo (tiempo de ejecución)	2 meses		
implementar APO11-C2	MARCO REFERENCIAL DE ADQUISICIÓN Y MANTENIMIENTO PARA LA INFRAESTRUCTURA DE TECNOLOGÍA		
	La organización deberá construir un marco referencial que incluya pasos a seguir como: adquisición, programación, documentación y pruebas, establecimientos de parámetros y aplicación de		

	correcciones, estos pasos deben estar alineados dentro del marco referencial.
Responsables de implementación	Encargado de la seguridad de Sistemas
Plazo (tiempo de ejecución)	2 meses

Elaborado por: RVRG

Tabla 19: Plan de acción al proceso APO12

PLAN DE ACCIÓN			
DOMINIO	ALINEAR, PLANIFICAR Y ORGANIZAR	PROCESO:	**APO12 GESTIONAR EL RIESGO**
CONTROLES			
Control a implementar APO12-C1	POLÍTICAS Y PROCEDIMIENTOS DE EVALUACIÓN DE RIESGOS		
	La administración deberá establecer un foro Gerencial, para asegurarse que exista una dirección clara de las iniciativas de seguridad. - Metodología - Frecuencias de evaluación - Evaluaciones de riesgo a nivel global y de sistemas - Mantener actualizadas las evaluaciones de riesgo, resultados de auditorías, inspecciones e incidentes.		
Responsables de implementación	Jefe de Oficina de Informática		
Plazo (tiempo de ejecución)	9 meses		

Elaborado por: RVRG

Tabla 20: Plan de acción al proceso BAI06

PLAN DE ACCIÓN			
DOMINIO	COSNTRUIR, ADQUIRIR E IMPLEMENTAR	PROCESO:	**BAI06 GESTIONAR LOS CAMBIOS**
CONTROLES			
Control a implementar BAI06-C1	SOFTWARE INSTALADOS POR EL USUARIO		
	La organización deberá dar restricciones explícitas para descargar e instalar software por parte de los usuarios.		
Responsables de implementación	Encargado de la seguridad de Sistemas		
Plazo (tiempo de ejecución)	1 mes		
implementar BAI06-C2	RESTRICCIONES DE USO DE SOFTWARE		
	La organización deberá obedecer a las restricciones de uso de software		
Responsables de implementación	Encargado de la seguridad de Sistemas		
Plazo (tiempo de ejecución)	4 meses		
Control a implementar BAI06-C3	DOCUMENTACIÓN DE LOS SISTEMAS DE INFORMACIÓN		
	La organización deberá asegurar que esté disponible la adecuada documentación para el sistema de información y sus componentes constitutivos, protegida cuando es requerido, y distribuida al personal autorizado.		

Responsables de implementación	Encargado de la seguridad de Sistemas
Plazo (tiempo de ejecución)	1 mes
Control a implementar BAI06-C4	POLÍTICAS Y PROCEDIMIENTOS DE ADMINISTRACIÓN DE LA CONFIGURACIÓN
	La organización deberá desarrollar, diseminar, y periódicamente revisar/ actualizar: - Una política de administración de la configuración formalmente definida y documentada. - Procedimientos documentados para facilitar la implantación de la política de administración de la configuración y los controles asociados.
Responsables de implementación	Encargado de la seguridad de Sistemas
Plazo (tiempo de ejecución)	3 meses

Elaborado por: RVRG

Tabla 21: Plan de acción al proceso DSS01

PLAN DE ACCIÓN			
DOMINIO	ENTREGAR, ADQUIRIR E IMPLEMENTAR	PROCESO:	**DSS01 GESTIONAR LAS OPERACIONES**
CONTROLES			
Control a implementar DSS01-C1	POLÍTICAS Y PROCEDIMIENTOS DE MANTENIMIENTOS DE SISTEMAS		
	La organización deberá desarrollar, diseminar, y periódicamente		

	revisar/ actualizar: - Una política de mantenimiento de sistemas formalmente definida y documentada - Procedimientos documentados para facilitar la implantación de la política de mantenimiento de sistemas y los controles asociados.
Responsables de implementación	Encargado de la seguridad de Sistemas
Plazo (tiempo de ejecución)	1 mes
implementar DSS01-C2	MANTENIMIENTO PERIÓDICO
	La organización deberá fijar, realizar, y documentar el preventivo, rutinario y regular mantenimiento en los componentes de los sistemas de información de acuerdo con las especificaciones del fabricante o vendedor y/o las de los requerimientos internos.
Responsables de implementación	Encargado de la seguridad de Sistemas
Plazo (tiempo de ejecución)	2 meses
Control a implementar DSS01-C3	AUTORIZACIÓN DE ACCESO FÍSICO
	La organización deberá desarrollar y conservar listas actualizadas del personal con acceso autorizado a los recursos de los sistemas de información y deberán portar credenciales apropiadas de autorización (ej. Insignias, tarjetas de identificación). El encargado de la seguridad de sistemas debe revisar y aprobar la lista de acceso y la autorización de credenciales.

Responsables de implementación	Encargado de la seguridad de Sistemas
Plazo (tiempo de ejecución)	2 semanas
implementar DSS01-C4	PROTECCIÓN CONTRA INCENDIOS
	La organización deberá emplear y mantener un sistemas automático de luces de emergencia que se activan de un fallo de poder o ruptura y que cubre salidas de emergencia y rutas de evacuación.
Responsables de implementación	Encargado de la seguridad de Sistemas
Plazo (tiempo de ejecución)	7 meses

Elaborado por: RVRG

Tabla 22: Plan de acción al proceso DSS04

PLAN DE ACCIÓN			
DOMINIO	ENTREGAR, ADQUIRIR E IMPLEMENTAR	PROCESO:	**DSS04 GESTIONAR LA CONTINUIDAD**
CONTROLES			
Control a implementar DSS04-C1	POLÍTICAS Y PROCEDIMIENTOS DEL PLAN DE CONTIGENCIA		
	La organización deberá dar desarrollar, diseminar, y periódicamente revisar/ actualizar: - Una política del plan de contingencia con el propósito de identificar los roles, responsabilidades y cumplimiento. - Procedimientos documentados para facilitar la implantación de las políticas del plan de continuidad del		

	negocio y los controles asociados.
Responsables de implementación	Encargado de la seguridad de Sistemas
Plazo (tiempo de ejecución)	1 mes
implementar DSS04-C2	ACTUALIZACION DEL PLAN DE CONTIGENCIA
	La organización debe revisar el plan de contingencia, los cambios o problemas encontrados durante la implementación, ejecución o prueba del plan.
Responsables de implementación	Encargado de la seguridad de Sistemas
Plazo (tiempo de ejecución)	1 mes
Control a implementar DSS04-C3	SITIO ALTERNO DE ALMACENAMIENTO
	La organización debe identificar un sitito alterno de almacenamiento e iniciar acuerdo necesarios que permitan almacenar la información de respaldo. El sitio alterno debe de estar configurado de manera que sea oportuna y efectiva la recuperación de la información.
Responsables de implementación	Encargado de la seguridad de Sistemas
Plazo (tiempo de ejecución)	1 mes

Elaborado por: RVRG

Tabla 23: Plan de acción al proceso DSS05

PLAN DE ACCIÓN			
DOMINIO	ENTREGAR, ADQUIRIR E IMPLEMENTAR	PROCESO:	**DSS05 GESTIONAR LA CONTINUIDAD**
CONTROLES			
Control a implementar DSS05-C1	PLAN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN		
	La organización debería desarrollar e implementar un plan de seguridad para los sistemas de información que proporciona una apreciación global de los requisitos de seguridad para los sistemas y una descripción de los controles de seguridad que existen o están planeados implantar.		
Responsables de implementación	Encargado de la seguridad de Sistemas		
Plazo (tiempo de ejecución)	3 meses		
implementar DSS05-C2	ACTUALIZAR PLAN DE SISTEMA DE SEGURIDAD DE LA INFORMACIÓN		
	La organización debería revisar el plan de seguridad para los sistemas de información, para detectar cualquier desviación o efectuar alguna corrección.		
Responsables de implementación	Encargado de la seguridad de Sistemas		
Plazo (tiempo de ejecución)	3 meses		

Control a implementar DSS05-C3	CONTROL DE LOS USUARIOS SOBRE SUS CUENTAS
	Los usuarios deberán controlar en forma sistemática la actividad de sus propias cuentas. También se deberán establecer mecanismos de información para permitirles supervisar la actividad normal, así como alertarlos oportunamente sobre actividades inusuales.
Responsables de implementación	Encargado de la seguridad de Sistemas
Plazo (tiempo de ejecución)	3 meses

Elaborado por: RVRG

4. ANÁLISIS Y DISCUSIÓN

Después de haber trabajado los resultados detalladamente haciendo uso de los instrumentos que apoyaron para la recolección de la información, se puede afirmar que un 54.54% de la población que fue evaluada confirma que los procesos que se desarrollan en el Centro de Datos son documentados y que serán elementos importantes para el desarrollo de la evaluación informática; mientras que un 45.45% desconoce de estos elementos, cosa que resulta alarmante para esta área ya que impide realizar una evaluación adecuada de los procesos más importantes que se desarrollan en ella.

Asimismo también se indica que un 90.90% de la población estiman que se realizan inventarios de los equipos en el Centro de Datos, y un 9.09% de la población indican que no se realizan inventarios de los equipos en el Centro de Datos ; esto nos indica que la aplicación del marco de trabajo COBIT será de gran relevancia para poder hacer el diagnóstico enfocados en criterios tales como efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad; es por esto que se coincide Anasi Y Paspuel (2013) ,al tener como marco de referencia para la realización de una evaluación , usando COBIT, que en su caso fue aplicada a la Unidad de TI de la Cooperativa de Ahorro y Crédito TEXTIL14 DE MARZO para realizar el análisis de los resultados y se proponer mejoras para la gestión informática de los procesos seleccionados. Finalmente, se exponen las conclusiones y recomendaciones obtenidas con la realización del presente proyecto lo cual se asemeja con este trabajo de investigación variando en el centro de investigación y los tipos de procesos que se ejecutan dentro de ella.

También resulta interesante el trabajo de Narváez (2012), ya que también utiliza El Estándar Internacional COBIT incluyendo con esto modelos de madurez que le apoyaron para alcanzar un nivel óptimo de administración en las TI, su trabajo de investigación sirvió de gran apoyo para esta evaluación pudiendo de estar manera crear planes tácticos de TI, compartiendo el mismo fin que se requiere para medir y controlar el desarrollo y aplicación de los procesos tecnológicos para que permitan mejorar la trayectoria estratégica y operativa.

Otra coincidencia importante fue aquel que realizo Gualsaquí (2013), porque aplica el marco de Referencia COBIT con la finalidad de realizar una correcta y aplicada gestión del área de información tecnológica permitiendo no solo el aseguramiento y aprovechamiento de los diferentes recursos que la misma posee sino también como por ejemplo controlar el acceso no apropiado y autorizado de personas que estén hábiles de manipular intencionalmente o no datos e información significativa de cualquier organización o empresa logrando sus objetivos basados en la gestión de Gobierno y de las TI corporativas, creando valores óptimos desde TI generando beneficios y optimizando el riesgo y uso de recursos.

Por último y no menos importante consideramos de gran apoyo el trabajo de Cáceres y García (2014), porque me permitieron aplicar el marco de Referencia COBIT con la finalidad de realizar una evaluación de la Gestión de la Información en la Oficina de Servicios Informáticos con la cual se logra encontrar aspectos que no permiten la optimización y la buena gestión de la Información en dicha oficina la cual fueron observadas para la evaluación correspondiente.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

1. Al realizar la aplicación de las herramientas como lo son las entrevista al personal especializado, visitas presenciales y la encuesta del marco de referencia COBIT, se pudo cumplir con una precisa recolección de datos que eran necesarios para lograr hacer el diagnostico de los procesos obteniendo resultados no favorables, logrando de tal forma identificar el estado actual en cuanto al control en los mecanismos de seguridad del Centro de Datos en el área de Informática, así como la evaluación de riesgos que se requieren para la evaluación de seguridad.

2. Al evaluar los procesos siete de ellos alcanzaron un nivel 2, es decir los procesos llegan a ser gestionados pero no establecidos en la cual la evaluación de riesgo no sigue un proceso definido, teniendo un reporte sobre la disponibilidad incompleta no tomando en cuenta el impacto sobre el negocio.

3. Por último se concluye que no existe un claro plan de análisis de TI en la oficina de informática para la seguridad del centro de datos, que impulsa el análisis del riesgo y soluciones de seguridad.

RECOMENDACIONES:

1. La oficina de informática debe tomar consideración en cuanto a los porcentajes obtenidos por medio del marco de trabajo COBIT realizando un plan estratégico y de esta manera mejorar sus procesos ya que hemos podido analizar que la información, la coordinación y la arquitectura de información que se tiene dentro de la oficina no es tan confiable para la toma de decisiones ni correctamente alineada con los estándares y con las mejores prácticas actuales, para poder alcanzar el valor ideal que es el 100%.

2. Debería considerarse implementar un proceso definido para la evaluación de riesgo estableciendo una base de datos de administración de riesgos y asignar la responsabilidad de realizar evaluaciones periódicas dentro del Centro de Datos, con el fin de medir la efectividad de cada uno de los procesos que se trabajan en esta área,

para de esta manera obtener una mejora continua en cuanto a dichos procesos y el área en general.

3. La oficina debe de estar preparado para cualquier riesgo que ocurra dentro de ella, es decir que se debe monitorear y medir el cumplimiento de los procedimientos y emprender acción donde los procesos parecen no estar funcionando efectivamente, y de esta manera buscar soluciones y mejoras para mantener la seguridad de la información del centro de datos en la entidad.

AGRADECIMIENTOS

En primer lugar agradecer a Dios por darme la capacidad y habilidad necesaria para poder llevar a cabo la realización de este trabajo de investigación, agradecer especialmente a mis padres por estar siempre ahí insistiéndome en lograr mis objetivos y brindándome su apoyo incondicional y también a todos mis seres queridos que estuvieron en mi camino en los buenos momentos como en los malos ofreciéndome siempre su apoyo incondicional.

REFERENCIA BIBLIOGRAFÍA

Gualsaqui Vivar, Juan Carlos (2013). *Proyecto de Desarrollo del marco de referencia COBIT 5.0 para la Gestión del área de TI de la empresa Blue Card, Tesis de Título*. Pontificia Universidad Nacional Católica del Ecuador, Ecuador.

Rescatado de: http://repositorio.puce.edu.ec/handle/22000/6078

Narváez Mejía, John Alexis. (2012). *Proyecto de Evaluación técnica informática del COMIL 10 Abdón Calderón, utilizando el estándar internacional COBIT* Tesis de Título. Universidad Nacional Santiago Antúnez de Mayolo, Huaraz, Perú.

Rescatado de: http://repositorio.espe.edu.ec/xmlui/handle/21000/5908

Nogueira Solís, J. (2013).*Procedimientos para auditoría física y medio ambiental de un Data Center basado en la clasificación y estándar internacional TIER*. Tesis de Título. Pontificia Universidad Católica del Perú, Lima, Perú.

Rescatado de:
http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/4978/NOGUEIRA_JOCELYNE_PROCEDIMIENTOS_AUDITORIA_FISICA_MEDIO_AMBIENTAL_DATA_CENTER_CLASIFICACION_ESTANDAR_INTERNACIONAL_TIER.pdf?sequence=1

Paspuel Morales, Paulina Tatiana (2013). *Proyecto de Evaluación de la Gestión Informática de la Unidad de TI de la Cooperativa de Ahorro y Crédito "TEXTIL 14 DE MARZO" usando COBIT 4.1, Tesis de Título. Quito – Ecuador. Rescatado de: http://bibdigital.epn.edu.ec/handle/15000/6672?mode=full*

Viteri Díaz, Sofía Monserrath (2013*). Proyecto de Evaluación técnica de la seguridad informática del Data Center de la brigada de fuerzas especiales Nº 9 Patria* Tesis de Título. Universidad Nacional Santiago Antúnez de Mayolo, Huaraz, Perú.

Rescatado de: https://repositorio.espe.edu.ec/handle/21000/6811

ANEXOS

ANEXO 1: ENTREVISTA

ENTREVISTA A LOS USUARIOS DEL AREA DE INFORMATICA

UNIVERSIDAD PRIVADA SAN PEDRO – CHIMBOTE

FACULTAD DE INGENIERIA

ESCUELA DE INGENIERIA DE INFORMATICA Y SISTEMAS

INTRODUCCION:

El siguiente está elaborado con la finalidad de recopilar información sobre las políticas de seguridad al centro de datos con la que actualmente El Poder Judicial del Santa.

Preguntas:

1. ¿Los procesos que se desarrollan en el Centro de Datos son documentados?
   Si ( ) No ( )

2. ¿Se realizan inventarios de los equipos en el Centro de Datos?
   Si ( ) No ( )
3. ¿Se cuenta con manuales por cada Sistema Implantado o software que se utiliza?
   Si ( ) No ( )

4. ¿Existe un reglamento para el personal de sistemas sobre el acceso al Centro de Datos?
   Si ( ) No ( )

5. ¿Se cuenta con un plan operativo?
   Si ( ) No ( )

6. ¿La infraestructura del Centro de Datos está construido con un material confiable?

Si ( ) No ( )

7. ¿El lugar en donde se encuentran los equipos es seguro?
   Si ( ) No ( )

8. ¿Existe algún tipo de material que sea inflamable o pueda resultar peligroso para los equipos?
   Si ( ) No ( )

9. ¿Existe algún tipo de mantenimiento preventivo para los equipos del Centro de Datos?
   Si ( ) No ( )

10. ¿Está conforme con la infraestructura del Centro de Datos?
    1. En desacuerdo……..( )
    2. De acuerdo……( )

11. ¿Considera importante las salidas de emergencia en el lugar en donde se encuentran los equipos?
    Si ( ) No ( )

12. ¿Está conforme con la seguridad física y tecnológica de vigilancia dentro del Centro de Datos?
    1. En desacuerdo…….( )
    2. De acuerdo……..( )

13. ¿Cómo considera el cableado y las vías del cuarto de equipo en relación con los estándares generales?
    1. En desacuerdo…….( )
    2. De acuerdo……..( )

14. ¿Está conforme con los etiquetados de cada uno de los equipos dentro del Centro de Datos?
    1. En desacuerdo……..( )

2. De acuerdo……...( )

15. ¿Está conforme con la distribución de las vías de distribución dentro del lugar de los equipos?
    1. En desacuerdo……...( )
    2. De acuerdo……( )

16. ¿Considera que las tuberías de agua están a buena distancia del el lugar donde se encuentran los equipos?
    1. En desacuerdo……..( )
    2. De acuerdo…….. ( )

17. ¿El control de humedad es efectivo dentro del lugar de los equipos?

Si ( ) No ( )