UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

“Evaluación de la seguridad informática en el área de sistemas de la Municipalidad Distrital de Nuevo Chimbote”

“TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERA EN INFORMÁTICA Y DE SISTEMAS”

AUTOR

Bach. Llerena Huamán Rosa Betzabé

ASESOR

Ing. Miguel Arturo Valle Peláez

Chimbote – Perú

2018

ÍNDICE

PALABRAS CLAVE

Tema	EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA
Especialidad	Gestión

KEYWORDS

Topic	EVALUATION OF COMPUTER SECURITY
Specialty	Management

LINEA DE INVESTIGACIÓN

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

Evaluación de la seguridad informática en el área de sistemas de la Municipalidad Distrital de Nuevo Chimbote

RESUMEN

La presente investigación tuvo como objetivo final Evaluar la Seguridad Informática al Área de Sistemas de la Municipalidad Distrital de Nuevo Chimbote, identificando todo tipo de vulnerabilidades y las medidas preventivas para la mejora del mismo.

Esta investigación es documental-descriptiva, no experimental, para la recolección de los datos se empleó técnicas de campo, observación, análisis, encuestas, entrevistas y documentación de libros; para la evaluación de la seguridad informática, se utilizó el marco de trabajo Cobit 5, para determinar si existe integridad, confidencialidad y disponibilidad de la información, como también el cumplimiento de las normas y estándares internacionales, considerando el mejoramiento continuo de la seguridad.

Dicha investigación describe la situación actual en la cual se encuentra la empresa en mención, en lo referente a toda vulnerabilidad; y por consiguiente se realiza las debidas recomendaciones, que garantizan la continuidad de los servicios y logre una mejora en el control de procesos para el manejo de riesgos.

ABSTRACT

The present investigation had the final objective to evaluate the Computer Security to the Systems Area of the Municipal District of Nuevo Chimbote, identifying all types of vulnerabilities and the preventive measures for the improvement of the same.

This research is documentary-descriptive, non-experimental, for the collection of data field techniques, observation, analysis, surveys, interviews and book documentation; for the assessment of computer security, the Cobit 5 framework was used to determine if there is integrity, confidentiality and availability of information, as well as compliance with international standards and standards, considering the continuous improvement of security.

This investigation describes the current situation in which the company in question is located, regarding any vulnerability; and consequently the necessary recommendations are made, which guarantee the continuity of the services and achieve an improvement in the control of processes for the management of risks.

1. INTRODUCCIÓN

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

La elaboración del trabajo de investigación se rescata el de Anasi Suntasig, Karina Isabel y Pasquel Morales, Paulina Tatiana (2013), Quito-Ecuador, En su tesis "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 consiste 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.

También el de Andrade España, Diana Lissette (2016) Esmeralda-Ecuador, en su tesis "Evaluación del Sistema de Gestión de Seguridad de la Información del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas (GADPE) tuvo como objetivo central, evaluar el sistema de gestión de seguridad de la información del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas (GADPE), identificando las vulnerabilidades y oportunidades de mejora del mismo. Aplicando como metodología de evaluación, la norma ISO 27001:2013 y como referencia al estándar COBIT para la elaboración del instrumento de evaluación del sistema de gestión seguridad de la información.

Otro ejemplo más son de Díaz Marcelo, Maricela Janet Y Ugarte Espinoza, Yesenia Abigail (2013) En Huacho-Perú, en su tesis "Auditoria de Seguridad Informática aplicada a la Municipalidad Provincial Huaura - Huacho", el objetivo de la auditoria de seguridad informática aplicada a la Municipalidad Provincial Huaura – Huacho es evaluar la eficiencia y eficacia respecto a la seguridad física, lógica y los procesos Informáticos en

la Municipalidad Provincia Huaura- Huacho y así poder detectar vulnerabilidades existentes en lo relativo a controles de seguridad.

Tomando como referencia el Marco de trabajo Cobit. El resultado de su tesis hizo que se logre una obtención de reducción en el ambiente de riesgos vigentes e incremento de la confiabilidad, integridad y disponibilidad de la información.

Asimismo se encontró la investigación de 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.

Un ejemplo más es de Yan Carranza Y Zavala Vásquez, (2013) En Trujillo - Perú, en su tesis de grado denominado, "Plan De Mejora De La Seguridad De Información Y Continuidad Del Centro De Datos De La Gerencia Regional de Educación La Libertad Aplicando Lineamientos ISO 27001 Y Buenas Prácticas COBIT", tuvo como finalidad elaborar un plan de mejora de seguridad de la información y continuidad del centro de datos, y mostrar los resultados obtenidos de la auditoria de sistemas, utilizando la metodología MAIGTI, el marco de trabajo y las directrices de auditoria propuestas por lineamientos ISO 27001 y buenas practicas COBIT 4.0.

Para esta investigación, el nivel fue descriptivo y su diseño fue no experimental. El resultado esperado fue de brindar las recomendaciones necesarias para superar las falencias encontradas según las buenas prácticas y alineamientos por COBIT 5.

Esta investigación se justifica en lo social, ya que los trabajadores del área de sistemas de la Municipalidad de Nuevo Chimbote, porque la información que posee la empresa, está expuesta a todo tipo de riesgos. Y debido a la vulneración de la información deben someterse a un control estricto que pueda garantizar que los sistemas de

información que posee, funcionen correctamente., así podrán desarrollar de una manera eficiente cualquier tipo de actividades informáticas que realizan a diario, y a su vez tengan la confiabilidad, veracidad, para proteger y utilizar adecuadamente cada uno de las actividades y evitando las amenazas que puedan surgir en ellas, por lo consiguiente asegurar la satisfacción de los otro usuarios.

La investigación aportará en lo científico porque busca conocimientos, procedimientos y técnicas sistematizadas para el desarrollo de la Evaluación de la Seguridad Informática, el cual se usó como herramienta de apoyo el marco de trabajo COBIT 5 que es precisamente un modelo para evaluar la gestión y control de los sistemas de información y tecnología con la finalidad de lograr un Plan de Mejora para ser evaluado por la institución y así poder implementarlo.

En la Municipalidad Distrital de Nuevo Chimbote, la seguridad informática es la que debe garantizar la integridad y confiabilidad de los activos humanos, hardware y software que existe en el área de sistemas de la empresa, la investigación aportará en lo científico, porque permitirá poner en práctica los conocimientos adquiridos en la materia, diseñar ciertos métodos, normas, procedimientos y técnicas con el fin de conseguir un sistema de información seguro y confiable. Se usará el marco de trabajo COBIT como una herramienta de apoyo.

De manera general, esta investigación encauzará en salvaguardar la información, equipos físicos y personal con el único fin de que la municipalidad obtenga una política de seguridad de acuerdo a los estándares de certificación.

Actualmente las tecnologías y los sistemas de información vienen padeciendo un incremento importante que ha ido perjudicando a nuestra sociedad. Las tecnologías, se presentan ya, como una necesidad frente a modificaciones rápidas y el crecimiento desmedido de información por ende las convierte en una exigencia para la organización.

Las instituciones tanto públicas como privadas se evidencian el uso de pequeños o grandes sistemas informáticos que a diario generan información, datos, reportes, actas y material que son de gran importancia para las empresas.

Como es el caso de La Municipalidad de Nuevo Chimbote, específicamente el área de sistemas. Cabe resaltar que cada cierto tiempo o cambio de Alcalde, cambian de

personal, solo los estables, son los que permanecen en la empresa y cuentan con experiencia, por este cambio, conlleva a no cumplir con las normas técnicas, ni con documentación para controlar la eficacia de sus procesos.

Cuenta con un plan de seguridad de la información, pero normalmente se ve expuesta a un nivel de amenaza muy alto, lo cual peligra la pérdida de la información en cada uno de los procesos internos, no hay estandarización de controles que lleven a disminuir los delitos informáticos a los que están en peligro los datos comprometiendo la confidencialidad, integridad y disponibilidad de la información, lo cual da origen a que planteara el problema de la siguiente manera:

¿Cómo desarrollar una Evaluación de la Seguridad Informática de la Municipalidad Distrital de Nuevo Chimbote en el Área de Sistemas"

Después de haber formulado la problemática, es necesario tener algunos conceptos básicos de: Área de Informática, Seguridad Informática, COBIT, ISO

Área de Informática, Es el encargado de administrar los recursos informáticos de la empresa, el proceso electrónico de datos, así como el soporte y mantenimiento de los elementos o servicios básicos de información de la empresa, también denominados como infraestructura tecnológica.

La organización de este departamento debe cubrir funciones relativas a seguridad, desarrollo y mantenimiento de aplicaciones, soporte técnico para administración de redes y sistemas, así como operaciones.

La importancia del departamento de informática radica en la dependencia de los procesos del negocio en la tecnología informática, donde el debido cumplimiento de las funciones de este departamento influye directamente en el logro de sus objetivos.

El área de informática está formada básicamente por los siguientes cuatro elementos:

- **El equipo físico o "hardware"** utilizado para operar el sistema. Incluye unidades centrales de proceso o "CPU", servidores de datos y aplicaciones, infraestructura de telecomunicaciones, accesorios de interfaz con el usuario, como monitores,

teclados, ratones, bocinas, audífonos, unidades de energía de respaldo o "ups", impresoras y otros.

- **Los sistemas o "software"** que incluyen el sistema principal y las aplicaciones específicas o paquetes computacionales, sistemas de comunicación y otros.
- **Los datos**, que constituyen la materia prima para generar la información. Aunque muchas veces estos dos términos se utilizan indistintamente, la diferencia entre dato e información es que los datos son señales individuales en bruto y sin ningún significado que son manipuladas por el computador (hardware y software) para producir la información deseada.
- **El recurso humano** necesario para administrar y dar mantenimiento a los elementos anteriores.

La Seguridad Informática concierne a la protección de la información, que se encuentra en una computadora o en una red de ellas y también a la protección del acceso a todos los recursos del sistema (*Baldeón, 2012*).

Para ello, se deben evaluar y cuantificar los bienes a proteger, y en función de análisis, implantar medidas preventivas y correctivas que eliminen los riegos asociados o que los reduzcan hasta niveles manejables (*Morlanes, 2012*).

La seguridad debe ser apropiada y proporcionada al valor de los sistemas, al grado de dependencia de la organización a sus servicios y a la probabilidad y dimensión de los daños potenciales. Los requerimientos de seguridad variarán, por tanto, dependiendo de cada organización y de cada sistema en particular (*Castro, 2009*).

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". *(Ramió J, 2006),*

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 **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.

COBIT, acrónimo de "Control Objectives for Information and related Technology" (Objetivos de Control para la Información y Tecnologías Relacionadas), es un estándar desarrollado por la Information Systems Audit and Control Foundation (ISACA), la cual fue fundada en 1969 en EE.UU., y que se preocupa de temas como gobernabilidad, control, aseguramiento y auditorias para TIC. Es uno de los estándares más utilizados actualmente, como base en la realización de una metodología de control interno en el ambiente de tecnología informática. Es un marco de referencia y se fundamenta en los objetivos de control existentes de la Information Systems Audit and Control Foundation (ISACF), y se encuentra alineado con otros estándares de control y auditoria como COSO, IFAC, IIA, ISACA, AICPA1.

El Marco de Referencia COBIT otorga especial importancia a los requerimientos de negocios en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad que deben ser satisfechos. El desarrollo de este marco de referencia ha sido limitado a objetivos de control de alto nivel en forma de necesidades de negocio dentro de un proceso de tecnología informática particular, cuyo logro es posible a través del establecimiento de controles, para el cual deben considerarse controles aplicables potenciales.

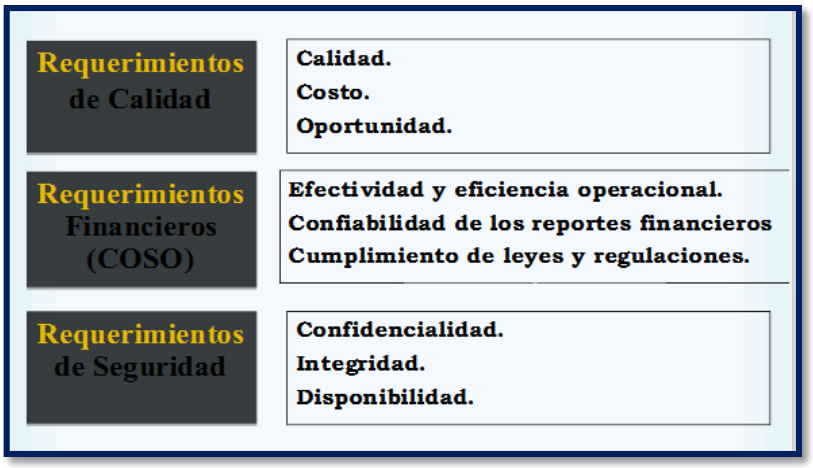


Figura 01: "Requerimiento de la Información – COBIT".

Fuente: Marco de Trabajo Cobit

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 06

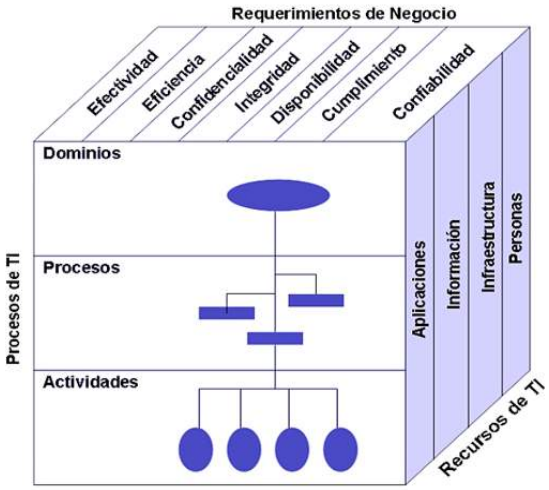


Figura 02: CUBO COBIT

Fuente: Marco de Referencia COBIT

Según **ISACA (2012)** en su libro **COBIT 5**, refiere que COBIT 5 es producto de la mejora estratégica de ISACA impulsando la próxima generación de guías sobre el Gobierno y la Administración de la información y los Activos Tecnológicos de las Organizaciones. Construido sobre más de 15 años de aplicación práctica, ISACA desarrolló COBIT 5 para cubrir las necesidades de los interesados, y alinearse a las actuales tendencias sobre técnicas de gobierno y administración relacionadas con la TI.

El Marco COBIT 5, Ayuda a las empresas a crear/obtener valor óptimo de la TI, manteniendo un balance entre los beneficios, riesgos y recursos. COBIT 5 tiene un enfoque holístico para administrar y gobernar la información y tecnología relacionada en toda la empresa. COBIT 5 establece principios y habilitadores genéricos que son útiles para empresas de todos tamaños y giros.

Marco de referencia COBIT 5, Es el principal producto, que cubre (overarching) a los demás de la familia COBIT 5. Contiene el resumen ejecutivo y la descripción completa de los componentes del marco COBIT 5:

- Los 5 principios de COBIT 5
- Los 7 habilitadores de COBIT 5
- Y Una introducción a la guía de implementación de COBIT 5
- Una introducción al COBIT Assessment Programme (no especifico a COBIT 5)

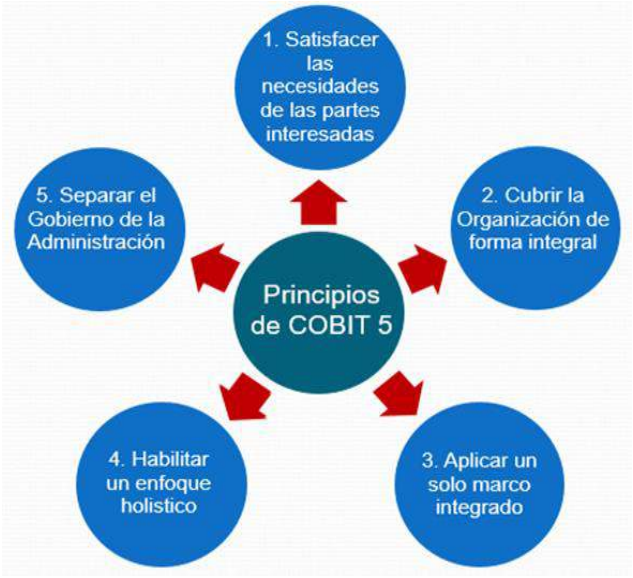


Figura 03: Principios COBIT 5

Fuente: COBIT 5 – figura2-2012 ISACA

Habilitadores de COBIT 5

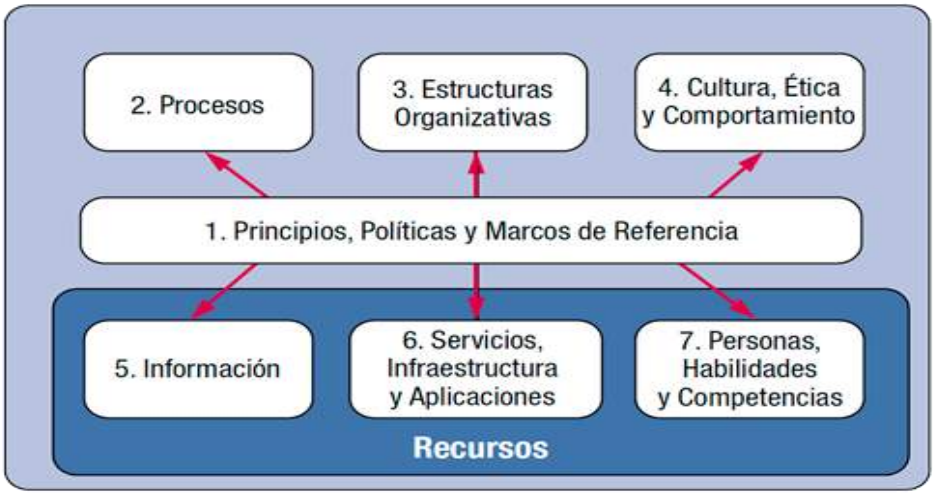


Figura 04 – Habilitadores COBIT 5

Fuente: COBIT 5-2012 ISACA

Modelo de Referencia de Procesos de COBIT 5

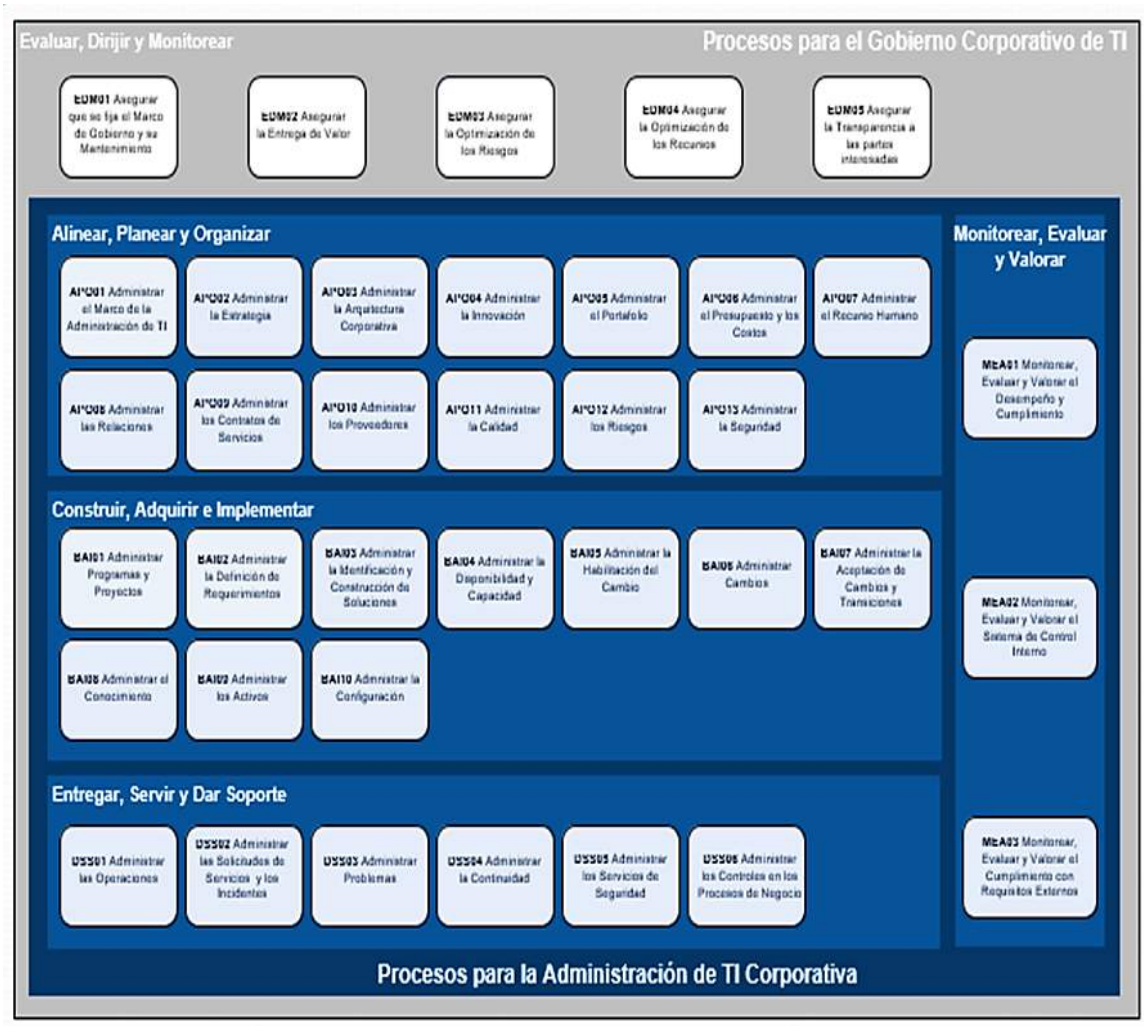


Figura 05 – Modelo de Referencia – Cobit 5

Fuente: COBIT 5 – figura16-2012 ISACA

Según, La Guía de Implementación COBIT 5 (ISACA, 2012) cubre los siguientes temas:

- Posicionar al Gobierno de IT dentro de la organización
- Tomar los primeros pasos hacia un Gobierno de IT superador
- Desafíos de implementación y factores de éxitos
- Facilitar la gestión del cambio
- Implementar la mejora continua
- La utilización del COBIT 5 y sus componentes.

Tomada de ISACA (2012) COBIT 5, Niveles de Capacidad, 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.

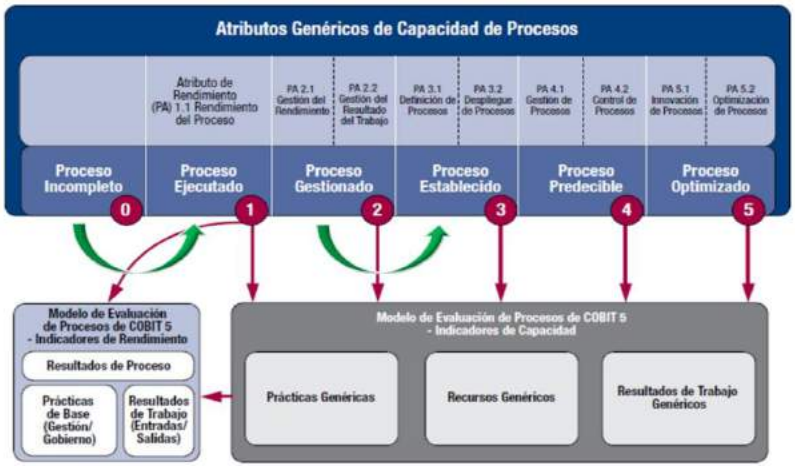


Figura 06 – Resumen del Modelo Capacidad de Procesos

Fuente: COBIT 5 – figura19-2012 ISACA

Para lograrlo, nos basamos en el marco de referencia Cobit (actualmente versión 5), quien sugiere medir la madurez de los procesos a través del "Process Capability Model", el cual está basado en el **estándar "ISO/IEC 15504** Software Engineering – Process Assessment Standard". Esta evaluación es muy exigente respecto a lo que debe cumplir cada proceso para ascender de nivel, y permite, entre otras cosas, lo siguiente:

Establecer un punto de referencia para la evaluación de la capacidad.

- ✓ Realizar revisiones sobre “el estado actual” y “el estado objetivo” para asistir al órgano de Gobierno y de Gestión de la empresa en la toma de decisiones de inversiones para la mejora de procesos.
- ✓ Realizar un análisis de carencias e información sobre la planificación de mejoras para apoyar la definición de proyectos de mejora justificables.
- ✓ Proporcionar al órgano de Gobierno y de Gestión de la empresa los porcentajes de evaluación para medir y monitorizar la capacidad actual.
- ✓ Este modelo se basa en dos dimensiones, donde se integran las Capacidades que evalúa la ISO 15504 y los Procesos propuestos por Cobit:

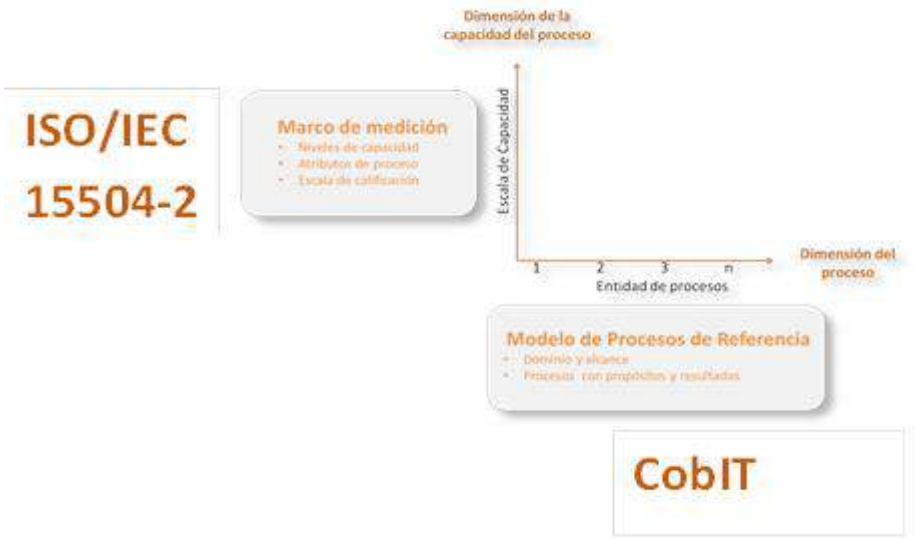


Figura 07 – Capacidades de Evaluación Según ISO 15504-2

Fuente: COBIT 5 – figura2-2012 ISACA

- **Dimensión del proceso:** en esta dimensión se definen un conjunto de procesos característicos con declaraciones de propósitos y resultado de cada proceso.
- **Dimensión de la capacidad del proceso:** consiste en el marco de medición que abarca los seis niveles de capacidad de proceso y sus atributos de proceso.

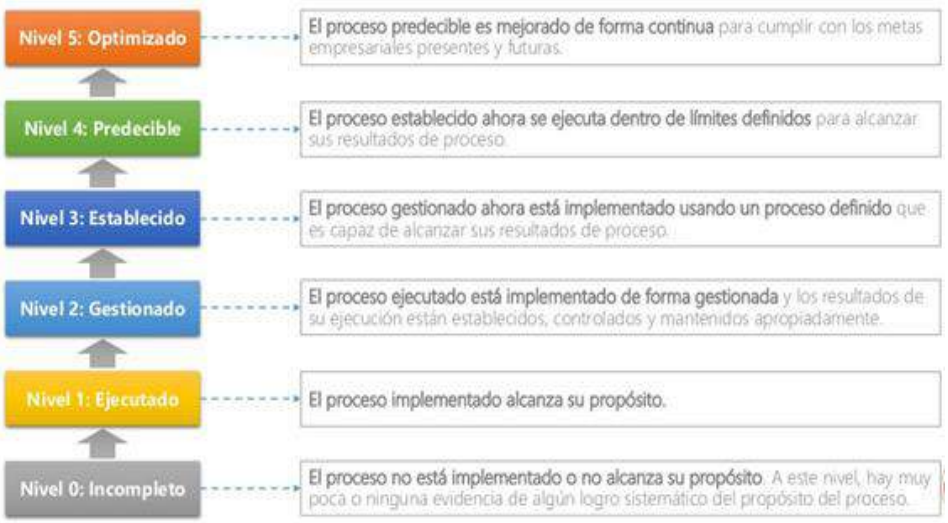


Figura 08- Niveles De Madurez

Fuente: COBIT 5

Lo que deseamos con este tipo de evaluación, es conocer la capacidad de los procesos implementados por una organización, lo que se traduce en determinar la información y los datos que los caracterizan, y el grado en el cual estos logran el propósito para el cual fueron desarrollados. Este grado será medido de acuerdo a un conjunto de Atributos de Procesos (PA), donde cada uno de estos mide un aspecto particular de su capacidad.

Figura 09: Niveles y Atributos

Fuente: COBIT 5

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.

La investigación es de tipo descriptivo, tiene como alcance la Evaluación de la Seguridad del Área de Sistemas de la Municipalidad Distrital de Nuevo Chimbote, no se planteará una hipótesis, por la tanto la hipótesis es Implícita

En la investigación se planteó como objetivo general: Evaluar la Seguridad Informática al Área de Sistemas de la Municipalidad Distrital de Nuevo Chimbote. Y como objetivos específicos: 1) Establecer el marco de trabajo para la medición de la gestión de seguridad del Área de Sistemas. 2) Realizar el proceso de evaluación utilizando el marco de trabajo COBIT 5 para medición del proceso de seguridad. 3) Elaborar los Planes de Acción para la Mejora del Área de Sistemas de la Municipalidad Distrital de Nuevo Chimbote.

2. METODOLOGÍA DEL TRABAJO

El presente trabajo de investigación de acuerdo a su orientación es Aplicada y de acuerdo a su nivel de estudio Descriptivo considerando, que es necesario la recolección de información relacionada con la Evaluación de La Seguridad Informática del Área De Sistemas de La Municipalidad Distrital De Nuevo 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 auditoría.

Para la aplicación del instrumento de recopilación de datos se tomará la muestra igual a la población de los colaboradores del área de Sistemas de la Municipalidad Distrital de Nuevo Chimbote, la cual cuenta con una cantidad de 7 personas, involucrados directamente con el sistema quienes responderán al instrumento.

En esta oportunidad se utilizará una muestra de tipo no probabilístico.

El muestreo por conveniencia. La muestra serán los empleados que trabajan dentro del área de Sistemas de la Municipalidad Distrital de Nuevo Chimbote.

Muestra=07 trabajadores del área de sistemas.

TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN:

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	
Entrevistas	Cuestionario de preguntas	Se realizó al personal del área de sistemas, siete (07)
Análisis documental	Análisis documental.	Se revisó textos, tesis, revistas y estudios previos, necesarios para el desarrollo de la evaluación.
Observación	Visitas presenciales	Utilizado para reconocer el área de trabajo

Fuente: Elaboración Propia.

DOMINIOS DEL MARCO DE TRABAJO COBIT 5

COBIT presenta treinta y siete objetivos generales, uno para cada uno de los procesos de las TI, estos procesos están agrupados en cinco dominios como lo muestra la Fig. 06

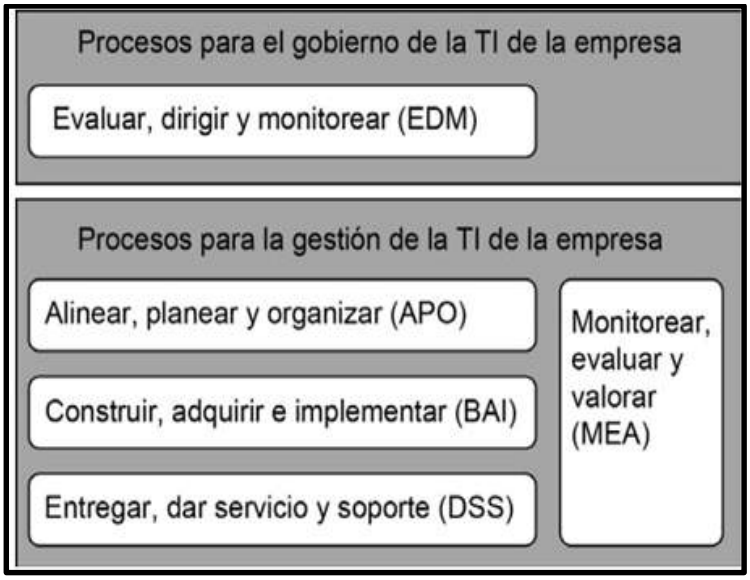


Figura 10: Los Cinco Dominios de COBIT

Fuente: Marco Referencia COBIT 5

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 de a 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.

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)

3. RESULTADOS

La entrevista fue realizada al personal del Área de Sistemas de la Municipalidad Distrital de Nuevo Chimbote, consta de 20 preguntas el cual se encuentra en Anexos. Solo se tomó algunas preguntas para poder realizar el trabajo de investigación.

Pregunta 1:

¿Conoce el organigrama de la empresa?

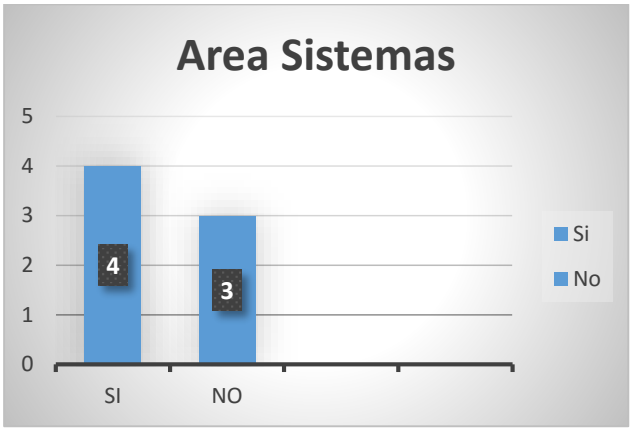


Figura 11: Grafico desarrollo actividades

Fuente: Elaboración Propia.

Interpretación: En el presente gráfico podemos observar que solo 4 (57%) empleados conocen organigrama de la empresa, y 3 (43%) no tienen conocimiento de dicho organigrama.

Como se ve casi la mitad de los empleados desconocen dicho organigrama.

Pregunta 2:

¿Tiene conocimiento si hay manuales o procedimientos en la empresa aprobados por la gerencia?

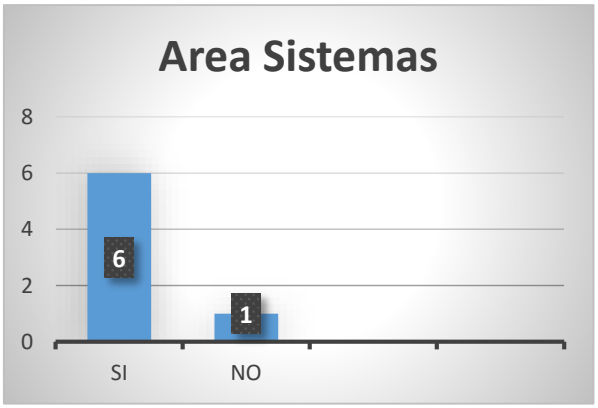


Figura 12: Grafico desarrollo actividades

Fuente: Elaboración Propia

Análisis: En el presente gráfico podemos observar que solo 6 (86%) empleados tienen conocimiento de manuales aprobados por la empresa, y 1 (14%) no tienen conocimiento de dicho manual o procedimiento

La mayoría de los empleados conocen los manuales y procedimientos aprobados por la gerencia.

Pregunta 3:

¿En el área donde labora, cuenta con procedimientos, manuales, instructivos establecidos para el manejo de información del sistema?

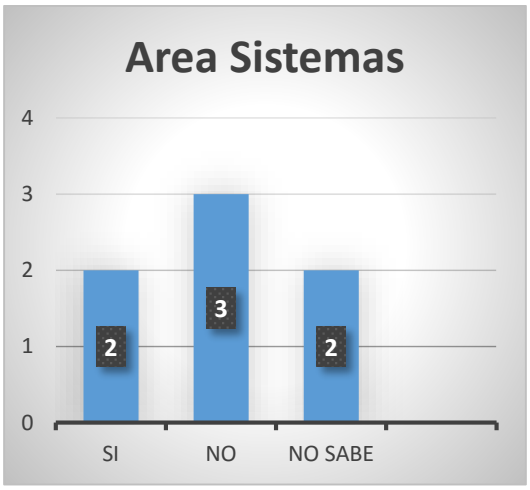


Figura 13: Grafico desarrollo actividades

Fuente: Elaboración Propia

Análisis: En el presente gráfico podemos observar que solo 2 (29%) empleados dice que el área cuenta con procedimientos, manuales, etc. Para el manejo de información del sistema y 3 (42%) dicen que no cuenta con manuales o instructivos para el manejo de la información del sistema y 2 (29%) que no sabe si hay.

Como se ve la mayor parte de los empleados desconocen los procedimientos, o manuales establecidos para el manejo de información del sistema.

Pregunta 4:

¿Existe algún manual de contingencia elaborado y aprobado por la gerencia?

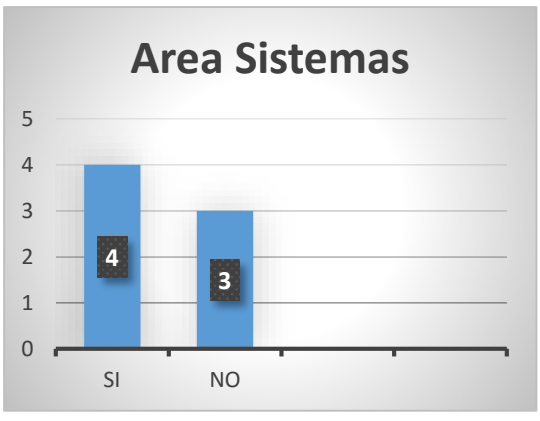


Figura 14: Grafico desarrollo actividades

Fuente: Elaboración Propia

Análisis:

En el presente gráfico podemos observar que solo 4 (57%) empleados saben la existencia de manual de contingencia y 3 (43%) no tienen conocimiento de dicho manual

Como se ve la mayor parte de los empleados tienen conocimiento de que existe un manual de contingencia.

Pregunta 5:

¿Existen prohibiciones sobre la instalación o uso de programas no autorizados en los equipos de la empresa?

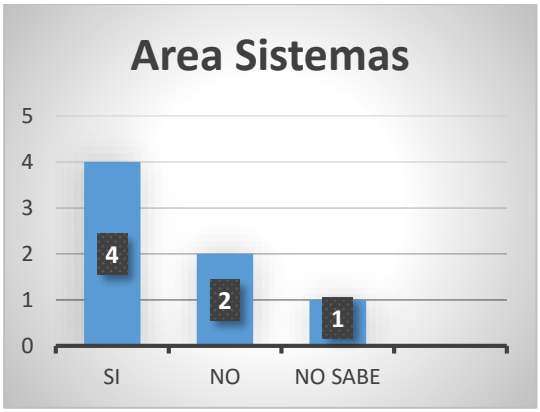


Figura 15: Grafico desarrollo actividades

Fuente: Elaboración Propia

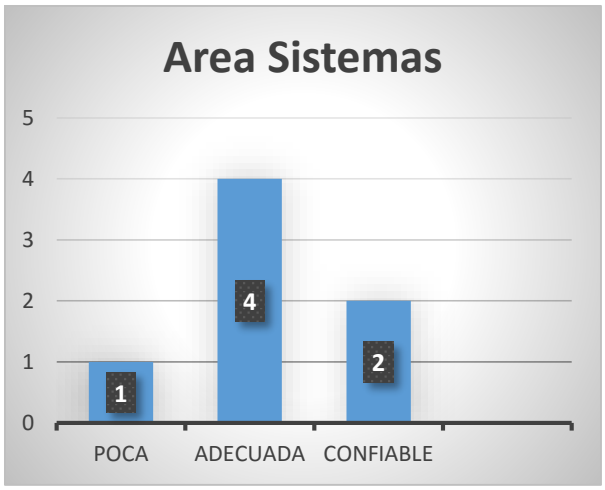
Análisis:

En el grafico podemos observar que 4 (57%) empleados dicen que hay prohibiciones y mientras que 2 (28.50%) empleados que no hay prohibiciones y 1 (14.50%) empleados que no sabe.

Como se puede observar que la mayoría de los empleados afirman que si hay prohibiciones.

Pregunta 6:

¿La información que facilita el sistema es?



En el grafico podemos observar que 4 (57%) empleados dicen facilita el sistema es adecuada 2 (28.50%) empleados que es confiables y 1 (14.50%) empleados que no sabe.

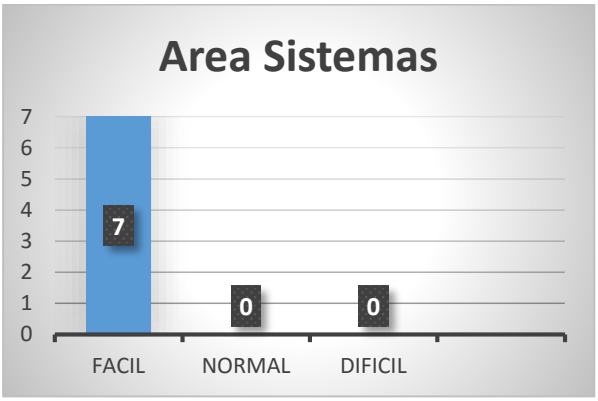
Como se puede observar que la mayoría de los empleados afirman que si hay prohibiciones.

Figura 16: Grafico desarrollo actividades

Fuente: Elaboración Propia

Pregunta 7:

¿El manejo del Sistema es?



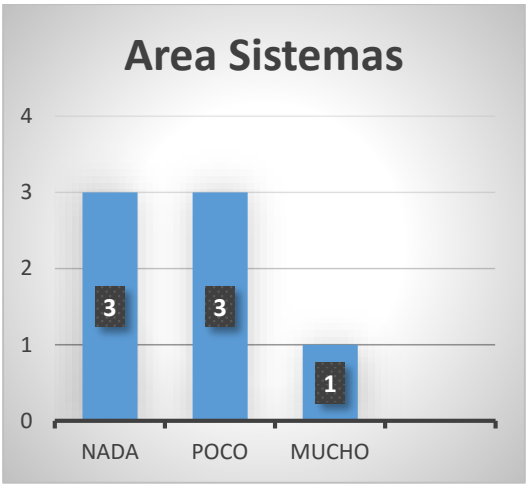
Análisis: En el presente gráfico podemos observar que los 7(100%) empleados dice que el manejo del sistema e fácil.

Figura 17: Grafico desarrollo actividades

Fuente: Elaboración Propia

Pregunta 8:

¿Se presentan dificultades o inconvenientes en el sistema?



Análisis: En el presente gráfico podemos observar que 3 (42.85%) empleados dice que no se presenta dificultades en el sistema, y 3 (42.85%) empleados dice que no se presenta poca dificultad en el sistema y 1(14.30%) dice que si se presenta con mucho inconveniente

Figura 18: Grafico desarrollo actividades

Fuente: Elaboración Propia

Pregunta 9:

¿Con que frecuencia existen las dificultades?

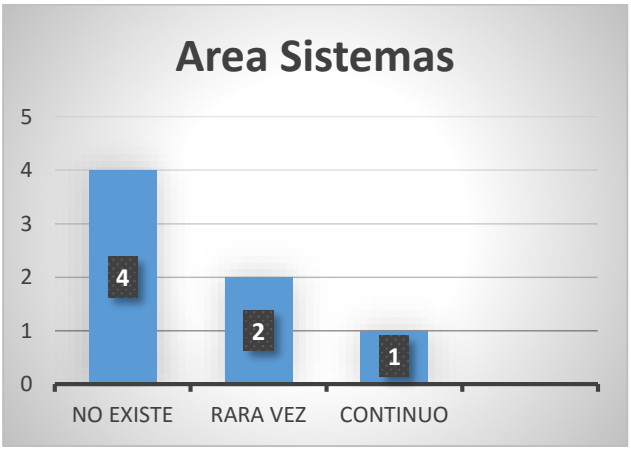


Figura 19: Grafico desarrollo actividades

Fuente: Elaboración Propia

Interpretación: En el grafico podemos observar que 4 (57%) empleados dicen no existe dificultades y 2 (28.50%) empleados dicen que rara vez 1 (14.50%) empleado dice que es continuo

Como se puede observar que la mayoría de los empleados afirman que no existen dificultades

Pregunta 8:

¿Si hubiera dificultad en el sistema, en cuánto tiempo se resuelve?

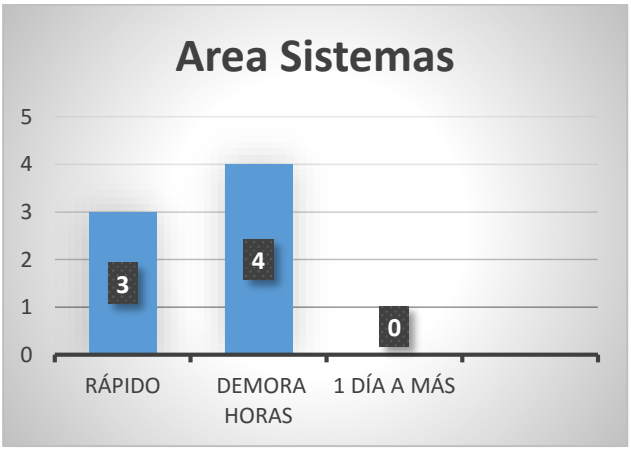


Figura 20: Grafico desarrollo actividades

Fuente: Elaboración Propia

Interpretación: En el grafico podemos observar que 4 (57%) empleados dicen que demora horas en resolver alguna dificultad y 3 (43%) empleados dicen que rápido lo resuelven

Como se puede observar que la mayoría de los empleados afirman que demoran horas en resolverlo

Pregunta 9:

¿Puede recuperar sus datos si por alguna razón se borran o falla el sistema?

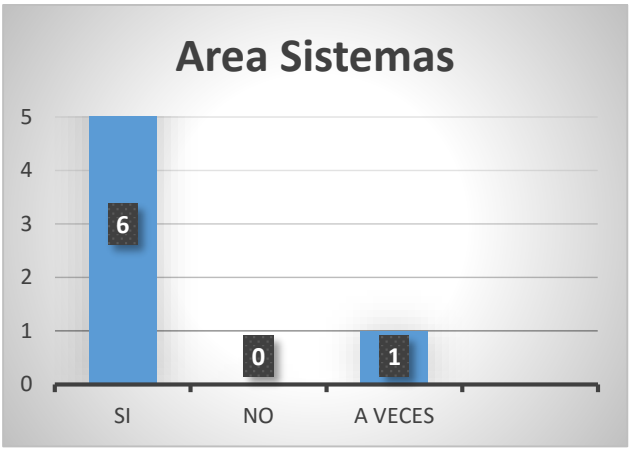


Figura 21: Grafico desarrollo actividades

Fuente: Elaboración Propia

Interpretación: En el grafico podemos observar que 6 (85.70%) empleados dicen que pueden recuperar sus datos (información) 1 (14.30%) empleado dicen que a veces

Como se puede observar que la mayoría de los empleados afirman que si pueden recuperar sus datos

Pregunta 10:

¿Se presentan dificultades o inconvenientes en el sistema?

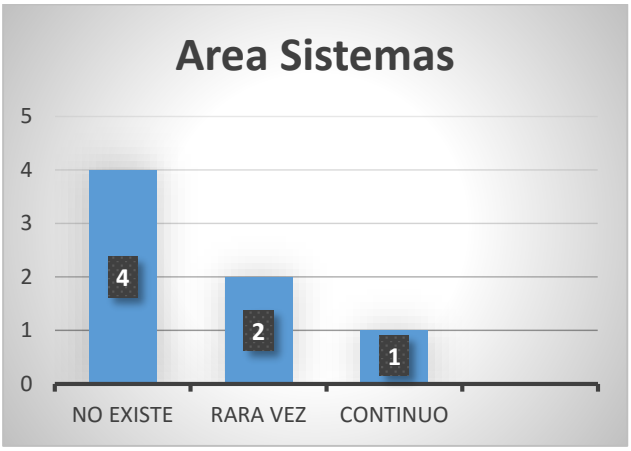


Figura 22: Grafico desarrollo actividades

Fuente: Elaboración Propia

Interpretación: En el grafico podemos observar que 4 (57%) empleados dicen no existe dificultades y 2 (28.50%) empleados dicen que rara vez 1 (14.50%) empleado dice que es continuo

Como se puede observar que la mayoría de los empleados afirman que no existen dificultades

Pregunta 11:

¿El acceso a la información del sistema es?

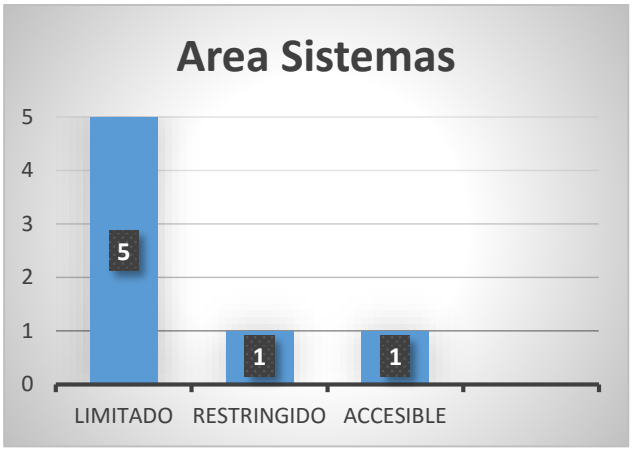


Figura 23: Grafico desarrollo actividades

Fuente: Elaboración Propia

Interpretación: En el grafico podemos observar que 5 (71.40%) empleados dicen la información es limitada y 1 (14.30%) empleados dicen que es restringido 1 (14.30%) empleado dice que es accesible

Como se puede observar que la mayoría de los empleados afirman la información es limitada

Pregunta 12:

¿Brindan capacitaciones o asesoramientos, cuando implementan algún sistema?

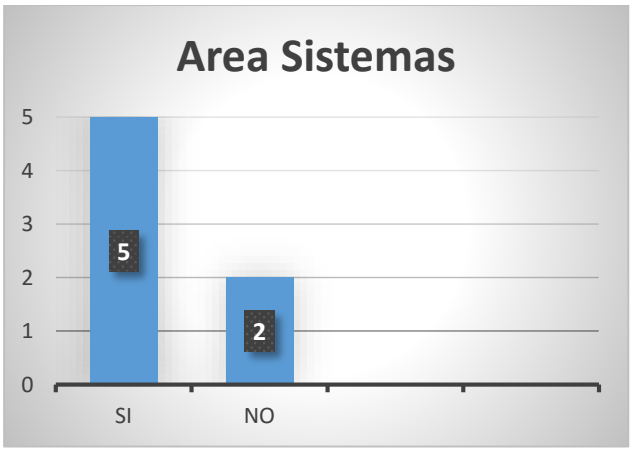


Figura 24: Grafico desarrollo actividades

Fuente: Elaboración Propia

Interpretación: En el grafico podemos observar que 5 (71.40%) empleados dicen hay capacitaciones y 2 (28.60%) empleados dicen que no

Como se puede observar que la mayoría de los empleados afirman que si hay capacitaciones cuando implementan un sistema.

Pregunta 13:

¿Se realizan inventarios del hardware?

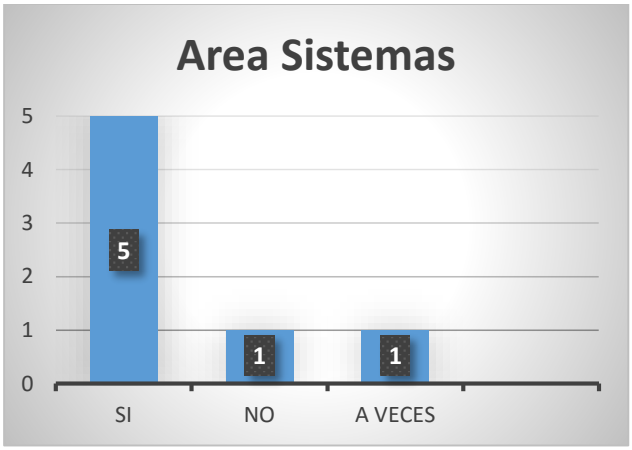


Figura 25: Grafico desarrollo actividades

Fuente: Elaboración Propia

Interpretación: En el grafico podemos observar que 5 (71.40%) empleados dicen si hacen inventarios de hardware y 1 (14.30%) empleados dicen que no 1 (14.30%) dice que a veces

Como se puede observar que la mayoría de los empleados afirman que si realizan inventarios de hardware

Pregunta 14:

¿Se realizan mantenimiento preventivo y correctivo del software y hardware?

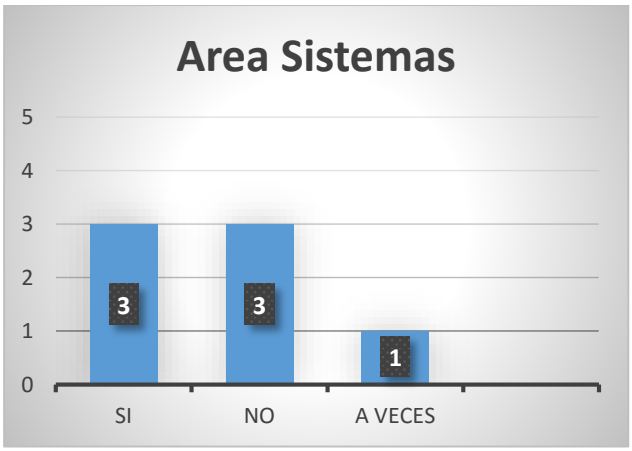


Figura 26: Grafico desarrollo actividades

Fuente: Elaboración Propia

Interpretación: En el presente gráfico podemos observar que 3 (42.85%) empleados dice que si hay mantenimiento preventivo y correctivo y 3 (42.85) empleados dicen que no lo realizan y el 1(14.30%) dice que a veces.

Pregunta 17:

¿Cuentan con un plan estratégico en TI?

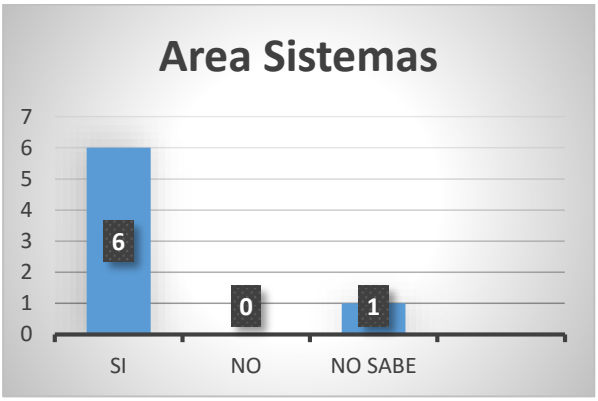


Figura 27: Grafico desarrollo actividades

Fuente: Elaboración Propia

Análisis: En el presente gráfico podemos observar que solo 6 (86%) empleados dicen que cuentan con un plan estratégico 1 (14%) no sabe si existe

Como se ve la mayor parte de los empleados conocen que hay un plan estratégico

Pregunta 20:

¿Cree usted que la realización de una evaluación o auditoría, brindará beneficios en el desarrollo de su trabajo?

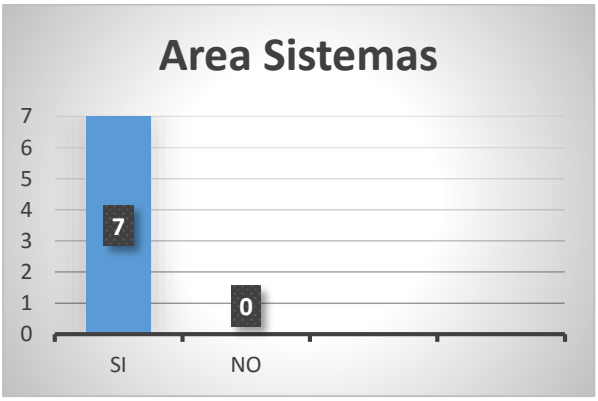


Figura 28: Grafico desarrollo actividades

Elaborado por: LLHRB

Análisis: En el presente gráfico podemos observar que los 7(100%) empleados dice que al aplicar una evaluación o auditoría minimizaría los riesgos que pueda ver

SELECCIÓN DE LOS PROCESOS COBIT A APLICAR

Resultaría demasiado extenso el aplicar la auditoria en todos los procesos y objetivos de control que abarca el marco de referencia de COBIT 5, es por ese motivo que se hizo una evaluación de la seguridad, por lo que se decidió realizar una selección de los procesos basados en los resultados de las observaciones, cuestionarios y entrevistas, tomando como principal sustento lo que las personas entrevistadas consideraron más importantes.

Para la evaluación de la seguridad informática del área de sistemas de la Municipalidad Distrital de Nuevo Chimbote, referente al marco de trabajo COBIT el cual tiene 5 dominios y 37 procesos, se realizó la tabla de Diagnóstico de Procesos de acuerdo al grado de importancia, los cuales solo se tomarán los de Grado 5 (Muy Alto).

Tabla 2: Tabla de Diagnóstico de Procesos

TABLA DE DIAGNOSTICO DE PROCESOS

OBJETIVOS DE CONTROL	GRADOS O NIVEL 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 Referencia de Gobierno*		X			
EDM02 *Asegurar La Entrega De Beneficios*		X			
EDM03 *Asegurar La Optimización Del Riesgo*	X				
EDM04 *Asegurar La Optimización De 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 Operaciones*		X		

DSS02 *Gestionar Peticiones e Incidentes De Servicio*	X		
DSS03 *Gestionar Problemas*			X
DSS04 *Gestionar La Continuidad*			X
DSS05 *Gestionar Servicios De Seguridad*			X
DSS06 *Gestionar Controles De Proceso De Negocio*		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		

Fuente: Elaboración Propia

DOMINIO Y PROCESOS A EVALUAR SEGÚN EL GRADO O NIVEL DE IMPORTANCIA (MÁS ALTO)

ALINEAR, PLANEAR Y ORGANIZAR

APO01 Gestionar el Marco de la Administración de TI

APO04 Gestionar la Innovación

APO12 Gestionar el Riesgo

APO13 Gestionar la Seguridad

CONSTRUIR, ADQUIRIR E IMPLEMENTAR

BAI06 Gestionar los Cambios

BAI07 Gestionar la Aceptación del Cambio y la Transición

BAI08 Gestionar el Conocimiento

ENTREGAR, SERVIR Y DAR SOPORTE

DSS03 Gestionar Problemas

DSS04 Gestionar la Continuidad

DSS05 Gestionar los Servicios de Seguridad

MONITOREAR, EVALUAR Y VALORAR

MEA01 Monitorear, Evaluar y Valorar el Desempeño y Cumplimiento

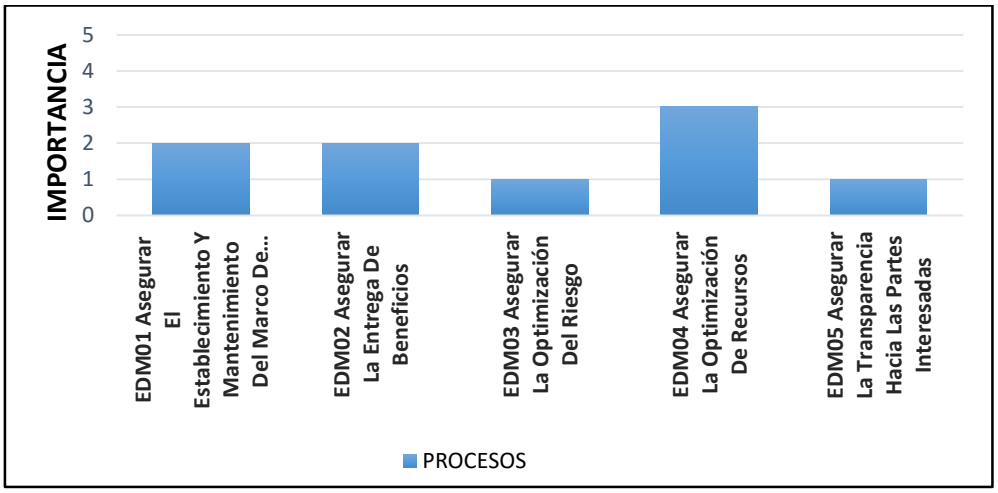
MEA02 Supervisar, evaluar y valorar el sistema de control interno

COBIT no solo se puede usar como herramienta de auditoria, sino también como una buena práctica de control periódico, seguimiento y evaluación de riesgos en lo que respecta a Tecnologías de Información.

En base a los datos obtenidos se obtuvieron los siguientes criterios de evaluación de acuerdo al nivel alcanzado:

Dominio EDM: EVALUAR, ORIENTAR Y SUPERVISAR

Tabla 3: CUADRO EXTRAIDO DE LA TABLA DE DIAGNÓSTICO DE PROCESOS(Tabla6)

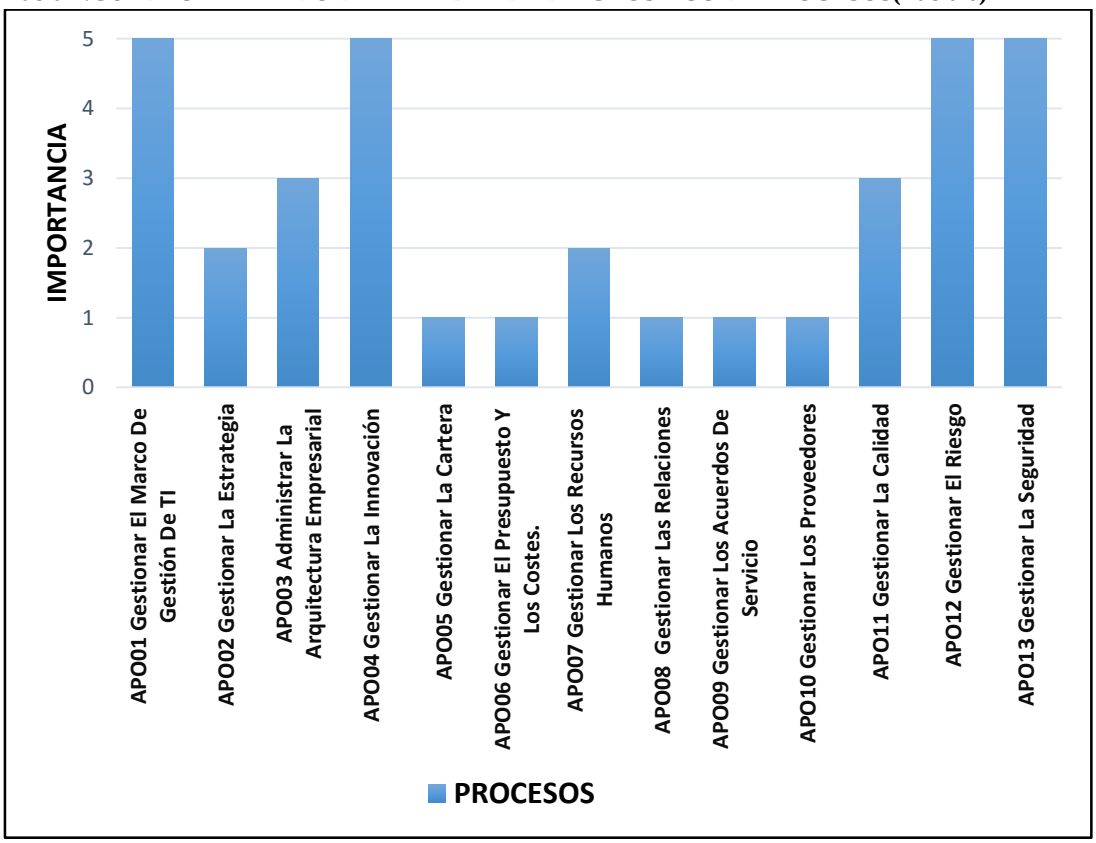


Fuente: Elaboración Propia

Del gráfico del Dominio EDM, se tomará en cuenta los procesos con grado de importancia Muy Alto. Se observó en el cuadro, de que no hay ningún proceso con grado de importancia Muy Alto. No lo tomaremos en cuenta.

Dominio APO: ALINEAR, PLANIFICAR Y ORGANIZAR

Tabla 4:CUADRO EXTRAIDO DE LA TABLA DE DIAGNÓSTICO DE PROCESOS(Tabla 6)



Fuente: Elaboración Propia

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

APO01 Gestionar el Marco de Gestión de TI.

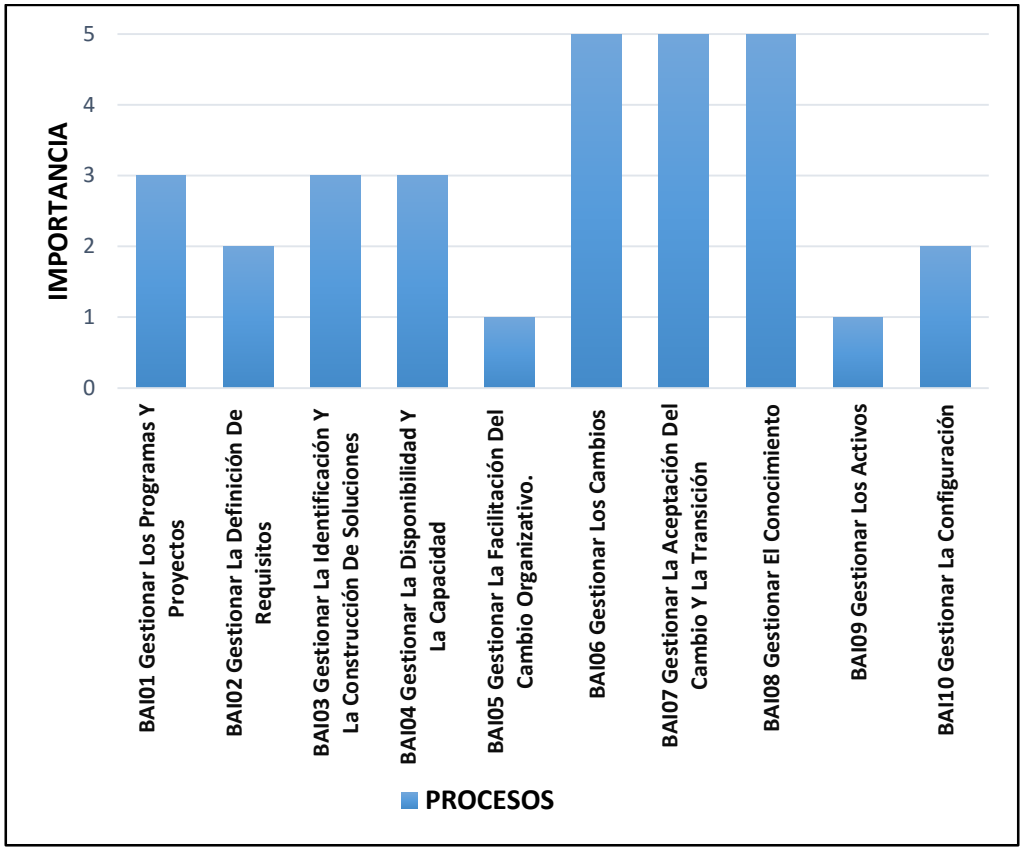
APO04 Gestionar la Innovación.

APO12 Gestionar el Riesgo.

APO13 Gestionar la Seguridad.

Dominio: BAI CONSTRUIR, ADQUIRIR E IMPLEMENTAR

Tabla 5 : CUADRO EXTRAIDO DE LA TABLA DE DIAGNÓSTICO DE PROCESOS (tabla 6)



Fuente: Elaboración Propia

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

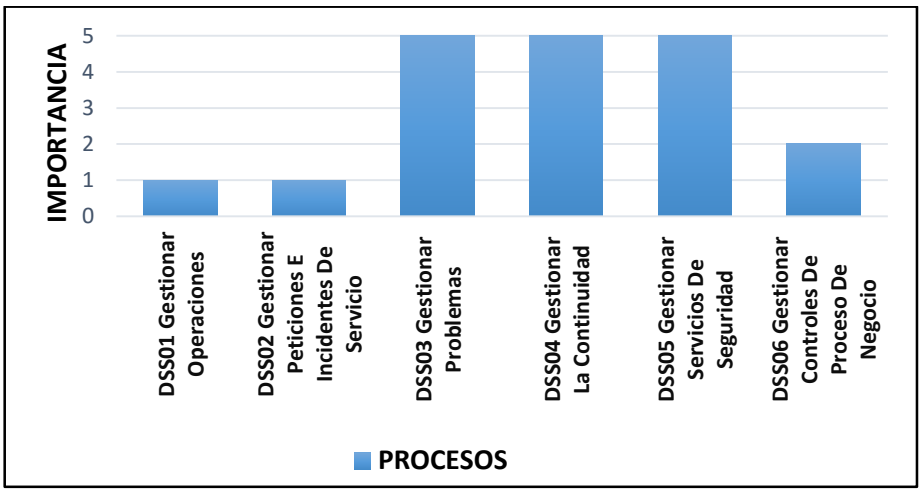
BAI06 Gestionar los Cambios

BAI07 Gestionar la Aceptación del Cambio y la Transición

BAI08 Gestionar el Conocimiento

Dominio: DSS ENTREGA, SERVICIO Y SOPORTE

TABLA 6: Cuadro Extraido de la Tabla de Diagnóstico De Procesos(Tabla6)



Fuente: Elaboración Propia

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

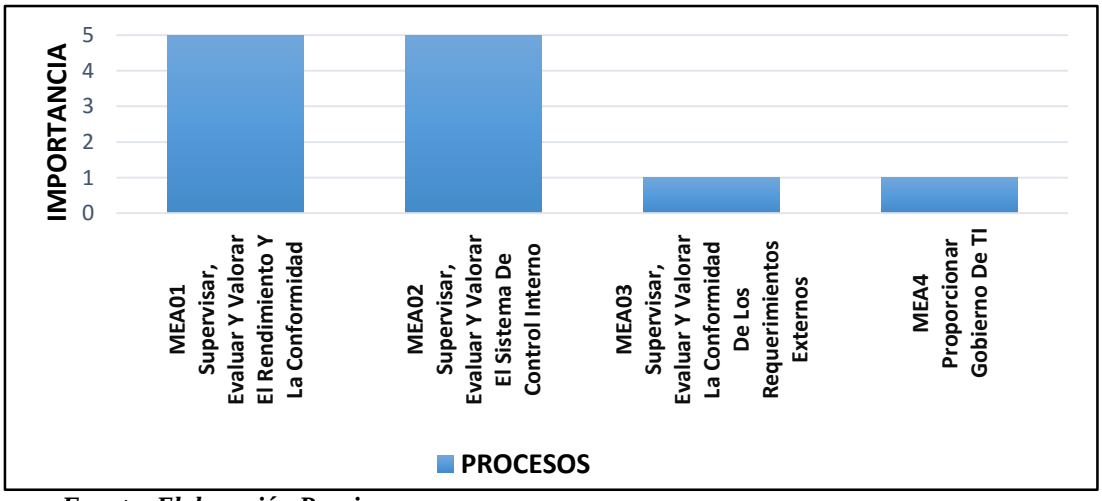
DSS03 Gestionar Problemas

DSS04 Gestionar la Continuidad

DSS05 Gestionar los Servicios de Seguridad

Dominio: MEA SUPERVISAR EVALUAR Y VALORAR

TABLA 7: CUADRO EXTRAIDO DE LA TABLA DE DIAGNÓSTICO DE PROCESOS (Tabla 6)



Fuente: Elaboración Propia

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

MEA01 Monitorear, Evaluar y Valorar el Desempeño y Cumplimiento
MEA02 Supervisar, evaluar y valorar el sistema de control interno

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

Dominio APO: Alinear, Planificar y Organizar

APO01 Gestionar el Marco de Gestión de TI.

APO01.01 Definir la estructura organizativa.
APO01.02 Establecer roles y responsabilidades.
APO01.03 Mantener los elementos catalizadores del sistema de gestión.
APO01.04 Comunicar los objetivos y la dirección de gestión.
APO01.05 Optimizar la ubicación de la función de TI.
APO01.06 Definir la propiedad de la información (datos) y del sistema.
APO01.07 Gestionar la mejora continua de los procesos.
APO01.08 Mantener el cumplimiento con las políticas y procedimientos.

APO04 Gestionar la Innovación.

APO04.01 Crear un entorno favorable para la innovación.
APO04.02 Mantener un entendimiento del entorno de la empresa.
APO04.03 Supervisar y explorar el entorno tecnológico.
APO04.04 Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras.
APO04.05 Recomendar iniciativas apropiadas adicionales.
APO04.06 Supervisar la implementación y el uso de la innovación.

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 riesgos.

APO12.06 Responder al riesgo

APO13 Gestionar la Seguridad.

APO13.01 Establecer y mantener un SGSI

APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.

APO13.03 Supervisar y revisar el SGSI

Dominio BAI: Construir, Adquirir e Implementar

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.

BAI07 Gestionar la Aceptación del Cambio y la Transición

BAI07.01 Establecer un plan de implementación.

BAI07.02 Planificar la conversión de procesos de negocio, sistemas y datos.

BAI07.03 Planificar pruebas de aceptación.

BAI07.04 Establecer un entorno de pruebas.

BAI07.05 Ejecutar pruebas de aceptación

BAI07.06 Pasar a producción y gestionar los lanzamientos.

BAI07.07 Proporcionar soporte en producción desde el primer momento.

BAI07.08 Ejecutar una revisión post implantación.

BAI08 Gestionar el Conocimiento

BAI08.01 Cultivar y facilitar una cultura de intercambio de conocimientos.

BAI08.02 Identificar y clasificar las fuentes de información.

BAI08.03 Organizar y contextualizar la información, transformándola en conocimiento.

BAI08.04 Utilizar y compartir el conocimiento.

BAI08.05 Evaluar y retirar la información.

DOMINIO DSS ENTREGAR, SERVIR Y DAR SOPORTE

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.

DOMINIO MEA MONITOREAR, EVALUAR Y VALORAR

MEA01 Monitorear, Evaluar y Valorar el Desempeño y Cumplimiento

MEA01.01 Establecer un enfoque de la supervisión.

MEA01.02 Establecer los objetivos de cumplimiento y rendimiento.

MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento.

MEA01.04 Analizar e informar sobre el rendimiento.

MEA01.05 Asegurar la implantación de medidas correctivas.

MEA02 Supervisar, evaluar y valorar el sistema de control interno

MEA02.01 Supervisar el control interno.

MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio.

MEA02.03 Realizar autoevaluaciones de control.

MEA02.04 Identificar y comunicar las deficiencias de control.

MEA02.05 Garantizar que los proveedores de aseguramiento son independientes y están cualificados.

MEA02.06 Planificar iniciativas de aseguramiento.

MEA02.07 Estudiar las iniciativas de aseguramiento.

MEA02.08 Ejecutar las iniciativas de aseguramiento.

MODELO DE MADUREZ A NIVEL CUALITATIVO (COSO)

Según el grado de Importancia (Nivel Alto)

Tabla 8: **MODELO DE MADUREZ A NIVEL CUALITATIVO**

OBJETIVOS DE CONTROL DE COBIT		**CRITERIO DE INFORMACIÓN**							**RECURSOS DE TI**			
		Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Aplicaciones	Información	Infraestructura	Personas
EVALUAR, ORIENTAR Y SUPERVISAR												
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, PLANIFICAR Y ORGANIZAR												
APO01	Administrar los recursos humanos de TI	P	S	P		S			X	X		X
APO02	Administrar Calidad											
APO03	Evaluar y administrar riesgos de TI											
APO04	Administrar proyectos	P	P	S					X			X
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	S	S	P	P	S		S	X	X		X
APO13	Gestionar La Seguridad	S	S	P	S	P		S	X	X	X	X
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											
BAI04	Gestionar La Disponibilidad Y La Capacidad											
BAI05	Gestionar La Facilitación Del Cambio Organizativo											
BAI06	Gestionar Los Cambios	P	S	S	S	S	S		X	X	X	X
BAI07	Gestionar La Aceptación Del Cambio Y La Transición	P	S		S	S	S			X		X
BAI08	Gestionar El Conocimiento	S	S		P	S	P		X	X		X
BAI09	Gestionar Los Activo											
BAI10	Gestionar La Configuración											
ENTREGA, SERVICIO Y SOPORTE												
DSS01	Gestionar Operaciones											
DSS02	Gestionar Peticiones E Incidentes De Servicio											
DSS03	Gestionar Problemas	P	P		S				X	X	X	X
DSS04	Gestionar La Continuidad	P	S			P			X	X	X	X

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

Fuente: Elaboración Propia

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 29: 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.

IMPACTO	PROMEDIO
Bajo	32%
Medio	63%
Alto	86%

Figura 30: Promedio de Impacto
Fuente: COBIT

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

Tabla 09: Resumen de Procesos y Criterios de Información por Impacto- Valores promedios

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 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, PLANIFICAR Y ORGANIZAR								
APO01	Administrar los recursos humanos de TI	0.86	0.63	0.86		0.63		
APO02	Administrar Calidad							
APO03	Evaluar y administrar riesgos de TI							

APO04	Administrar proyectos	0.86	0.86	0.63			
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	0.63	0.63	0.86	0.86	0.63	0.63
APO13	Gestionar La Seguridad	0.63	0.63	0.86	0.63	0.86	0.63
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						
BAI04	Gestionar La Disponibilidad Y La Capacidad						
BAI05	Gestionar La Facilitación Del Cambio Organizativo						
BAI06	Gestionar Los Cambios	0.86	0.63	0.63	0.63	0.63	
BAI07	Gestionar La Aceptación Del Cambio Y La Transición	0.86	0.63		0.63	0.63	0.63
BAI08	Gestionar El Conocimiento	0.63	0.63		0.86	0.63	0.86
BAI09	Gestionar Los Activos						
BAI10	Gestionar La Configuración						
ENTREGA, SERVICIO Y SOPORTE							

DSS01	Gestionar Operaciones							
DSS02	Gestionar Peticiones E Incidentes De Servicio							
DSS03	Gestionar Problemas	0.86	0.86		0.63			
DSS04	Gestionar La Continuidad	0.86	0.63			0.86		
DSS05	Gestionar Servicios De Seguridad			0.86	0.86	0.63	0.63	0.63
DSS06	Gestionar Controles De Proceso De Negocio							
SUPERVISAR, EVALUAR Y VALORAR								
MEA01	Supervisar, Evaluar Y Valorar El Rendimiento Y La Conformidad	0.86	0.86	0.63	0.63		0.63	
MEA02	Supervisar, Evaluar Y Valorar El Sistema De Control Interno	0.86	0.86	0.63		0.63		
MEA03	Supervisar, Evaluar Y Valorar La Conformidad De Los Requerimientos Externos							

Fuente: Elaboración Propia

Teniendo los valores de los criterios de información de los procesos tomados en cuenta, se procederá a utilizarlos en un cálculo entre el nivel de Madurez de los procesos mencionados y que son establecidos por COBIT 5, y el nivel de impacto que tiene cada criterio de información, para luego proceder a realizar la suma de los valores encontrados en cada uno de los criterios, obteniendo un total real del criterio de información, el cual será comparado con el total ideal.

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.

Tabla 10: Modelo de Madurez APO01

DOMINIO: ALINEAR, PLANEAR Y ORGANIZAR
APO01 Administrar el Marco de la Administración de TI *Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.* ***APO01.01 Definir la estructura organizativa.*** ***APO01.02 Establecer roles y responsabilidades.*** ***APO01.03 Mantener los elementos catalizadores del sistema de gestión.*** ***APO01.04 Comunicar los objetivos y la dirección de gestión.*** ***APO01.05 Optimizar la ubicación de la función de TI.*** ***APO01.06 Definir la propiedad de la información (datos) y del sistema.*** ***APO01.07 Gestionar la mejora continua de los procesos.*** ***APO01.08 Mantener el cumplimiento con las políticas y procedimientos.***

NIVEL DE MADUREZ / **CRITERIO**		**CUMPLE**	**NO CUMPLE**
Nivel 0 Incompleto	No está implementado, poca o inexistente evidencia de cualquier logro de los objetivos, roles o responsabilidades por parte de la empresa o el área encargada	√	
Nivel 1 Ejecutado	Los objetivos, responsabilidades logran cumplir su propósito de acuerdo a las políticas y procedimientos.	√	
Nivel 2 Gestionado	Los procesos del área, responsabilidades y los productos resultantes se establecen, controlan y mantienen apropiadamente	√	
Nivel 3 Establecido	El área, utiliza procesos definidos basados en estándares y es capaz de alcanzar sus		√

	resultados de procesos (planifica, documenta, ejecuta, monitoriza y controla)	
Nivel 4 Predecible	El proceso establecido y las operaciones de los sistemas, están en una mejora continua y proporcionan mejores prácticas para el área encargada.	√
Nivel 5 Optimizado	El proceso predecible es mejorado en forma continua para cumplir los correspondientes objetivos actuales y proyectados de la empresa.	√

GRADO DE MADUREZ

El proceso de Administrar el Marco de la Administración de TI está en el **nivel de madurez 2.**

HALLAZGOS

* No tienen el total apoyo de la dirección ejecutiva.
*No hay una mejora en los objetivos de los procesos
∗No hay lineamientos entre el plan estratégico de la empresa con el de tecnología
∗No hay una mejora continua en seguimiento del cumplimiento con políticas y procedimientos.

RECOMENDACIONES:

Tomar decisiones estratégicas entre la dirección ejecutiva y el área de sistemas

Realizar una evaluación de los objetivos existentes en corto plazo, como también al personal.

Crear planes tácticos que involucren el plan estratégico con el de tecnología.

Fuente: Elaboración Propia

Tabla 11: Modelo de Madurez APO04

DOMINIO: ALINEAR, PLANEAR Y ORGANIZAR
APO04 Administrar la Innovación *Mantener un conocimiento de la tecnología de la información y las tendencias relacionadas con el servicio, identificar las oportunidades de innovación y planificar la manera de beneficiarse de la innovación en relación con las necesidades del negocio. Analizar cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI, así como a través de las tecnologías ya existentes y por la innovación en procesos empresariales y de TI. Influir en la planificación estratégica y en las decisiones de la arquitectura de empresa* ***APO04.01 Crear un entorno favorable para la innovación.*** ***APO04.02 Mantener un entendimiento del entorno de la empresa*** ***APO04.03 Supervisar y explorar el entorno tecnológico.*** ***APO04.04 Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras.*** ***APO04.05 Recomendar iniciativas apropiadas adicionales.*** ***APO04.06 Supervisar la implementación y el uso de la innovación.***

NIVEL DE MADUREZ / **CRITERIO**		**CUMPLE**	**NO CUMPLE**
Nivel 0 Incompleto	No existe un entorno tecnológico favorable y tampoco existe conciencia sobre la importancia de la planeación estratégica.	√	
Nivel 1 **Ejecutado**	Los objetivos del área se cumplen por la mejora de la calidad, y la gerencia reconoce la necesidad de planear la infraestructura tecnológica.	√	

Nivel 2 Gestionado	Los procesos y objetivos del área son ejecutados y puestos en marcha, surgen técnicas y estándares comunes para el desarrollo de componentes de la infraestructura.		√
Nivel 3 Establecido	El área, utiliza procesos definidos ya gestionados, documentados, basados en estándares y es capaz de alcanzar sus resultados de proceso		√
Nivel 4 Predecible	El área de informática, tiene un proceso establecido, cuenta con experiencia y habilidades para desarrollar y administrar la innovación, están en una mejora continua.		√
Nivel 5 Optimizado	El proceso predecible es mejorado y continuo en forma continua y el área cuenta un buen plan de infraestructura e innovación, la cual refleja los requerimientos establecidos por el TI.		√

GRADO DE MADUREZ

El proceso de Administrar la Innovación está en el nivel de Madurez 1

HALLAZGOS:

* No existe un plan de infraestructura e innovación tecnológica.

* Falta de interés de la directiva en adoptar nuevas innovaciones tecnológicas

* No hay una mejora en la innovación, no existe un programa que permita que los trabajadores presenten ideas innovadoras para poder evaluar y aplicarlas en la empresa

RECOMENDACIONES:

- ✓ Elaborar un plan de infraestructura e innovación tecnológica.
- ✓ Recopilar las ideas innovadoras del personal de TI
- ✓ Realizar estudios y analizar el entorno exterior, incluyendo sitios web, foros, conferencias, para identificar tecnologías emergentes.

Fuente: Elaboración Propia

Tabla 12: Modelo de Madurez APO12

DOMINIO: ALINEAR, PLANEAR Y ORGANIZAR			
APO12 Gestionar el Riesgo *Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa* ***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 MADUREZ	**CRITERIO**	**CUMPLE**	**NO CUMPLE**
Nivel 0 Incompleto	No hay una estimación, ni reducción de riesgos relacionados al TI en el área de sistemas.	√	
Nivel 1 Ejecutado	El área de sistemas, logra cumplir su propósito de acuerdo a las políticas y procedimientos para evaluar y reducir los riesgos relacionados con el TI	√	
Nivel 2 **Gestionado**	Los procesos de gestión de riesgos del área de sistemas, se establecen, controlan y mantienen apropiadamente una evaluación de acción de gestión de riesgo.	√	
Nivel 3 Establecido	El área, utiliza procesos definidos basados en estándares capaz de minimizar, monitorear, ejecutar e identificar el riesgo en las TI		√

Nivel 4 Predecible	El proceso de gestión de riesgo establecido está en una mejora continua y proporcionan mejores prácticas donde se puede monitorear y tomar decisiones para analizar y responder al riesgo relacionado con el TI.		√
Nivel 5 Optimizado	El proceso de gestión de Riesgo gestionado, predecible, es mejorado en forma continua y bien administrado. La administración del riesgo está totalmente integrada en todos los procesos de negocio del TI		√

GRADO DE MADUREZ

El proceso de **Gestionar el Riesgo** está en el nivel de madurez 2.

HALLAZGOS

* No hay un proceso definido capaz que minimice y monitoree la gestión de riesgo.

*No hay una mejora continua en las acciones de gestión para los riesgos del TI.

RECOMENDACIONES:

- ✓ Implementar un proceso de gestión de riesgo, documentarlo y poner en práctica en todas las personas encargadas del área de sistemas
- ✓ Ejecutar análisis periódicos de gestión de riesgo para identificar los posibles riesgos que pueden existir.
- ✓ Definir un conjunto de propuestas de proyectos diseñadas para reducir el riesgo en las TI.

Fuente: Elaboración Propia

Tabla 13: Modelo de Madurez APO13

DOMINIO: ALINEAR, PLANEAR Y ORGANIZAR

APO013 Gestionar la Seguridad

Definir, operar y supervisar un sistema para la gestión de la seguridad de la información

APO013.01 Establecer y mantener un SGSI

APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.

APO013.03 Supervisar y revisar el SGSI

NIVEL DE MADUREZ / CRITERIO		CUMPLE	NO CUMPLE
Nivel 0 Incompleto	No hay un sistema de gestión de la seguridad. O existe poca o inexistente evidencia para gestionar un plan de tratamiento de riesgo de la seguridad de la información	√	
Nivel 1 Ejecutado	Los procesos de gestión de seguridad logra cumplir su propósito	√	
Nivel 2 Gestionado	Los procesos de gestión de seguridad del área de sistemas, se establecen, aceptan, controlan y mantienen apropiadamente un plan de seguridad.		√
Nivel 3 Establecido	El área de sistema, utiliza procesos definidos basados en estándares y es capaz de alcanzar y mantener un SGSI en forma continua.		√
Nivel 4 Predecible	El proceso establecido y las operaciones del SGSI, están en una mejora continua y alineadas que proporcionan mejores prácticas en la gestión de seguridad de la empresa		√

Nivel 5 Optimizado	El proceso de gestión de seguridad predecible es mejorado en forma continua para cumplir e integrar la planificación, diseño e implementación de los procedimientos de seguridad de información.	√

GRADO DE MADUREZ

El proceso de Gestionar la Seguridad está en **el nivel de madurez 1.**

HALLAZGOS

*Falta de comunicación de los roles y responsabilidades de SGSI

*Falta de interés de la directiva para implementar y operar o hacer cambios en el SGSI

*Propuestas escasas para la implementación de un plan de contingencia para riesgos relacionados con la seguridad

RECOMENDACIONES

- ✓ Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información.
- ✓ Desarrollar un sistema que permita implementar un plan de seguridad.
- ✓ Definir y alinear el SGSI de acuerdo con la política de empresa.
- ✓ Identificar resultados obtenidos el uso del sistema de gestión de la seguridad de la información, para dar a conocer a los directivos.

Fuente: Elaboración Propia

Tabla 14: Modelo de Madurez BAI06

DOMINIO: CONSTRUIR, ADQUIRIR E IMPLEMENTAR			
BAI06 Gestionar los Cambios *Gestiona 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.* ***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.***			
NIVEL DE MADUREZ	**CRITERIO**	**CUMPLE**	**NO CUMPLE**
Nivel 0 Incompleto	No hay un proceso definido de gestión de cambios, , poca o inexistente evidencia de cualquier logro o cambio sin control alguno	√	
Nivel 1 Ejecutado	Los procesos de gestión de cambio son reconocidos y administrados bajo un control, pero aún le falta consistencia para llevar un seguimiento. Hay documentación incompleta o escasa al cambio, es poco confiable.	√	
Nivel 2 Gestionado	Los procesos de gestión de cambio del área de sistemas, está ejecutado pero no estructurado, los productos resultantes se establecen, pero no son realizados de acuerdo a sus cronogramas.		√
Nivel 3 Establecido	El área de sistemas, utiliza procesos de administración de cambios definidos basados en estándares y es capaz de alcanzar sus resultados de proceso que incluye,		√

	procedimientos de categorización, priorización y administración de cambios.	
Nivel 4 Predecible	El proceso de gestión de cambios está establecido y las operaciones de los sistemas, están en una mejora continua, el proceso es eficiente y efectivo.	√
Nivel 5 Optimizado	El proceso de gestión de cambios predecible es mejorado en forma continua para cumplir los objetivos actuales y proyectados. La información es automatizada, hay un seguimiento de control y los cambios son registrados, priorizados, categorizados y programados por la empresa.	√

GRADO DE MADUREZ

El proceso de Gestionar los Cambios está en el nivel de madurez 1.

HALLAZGOS

* Los cambios no son realizados de acuerdo a lo establecido, no hay .una correcta planificación.

* No existe políticas, ni procedimientos establecidos de cambios a programas en la empresa

*Falta de implementación a la gestión de riesgos, debido al cambio

RECOMENDACIONES:

- ✓ Se deben realizar cambios autorizados de acuerdo a sus cronogramas.
- ✓ Incluir los cambios en la documentación de las TI.
- ✓ Programar los cambios aprobados por el área de sistemas.

Fuente: Elaboración Propia

Tabla 15: Modelo de Madurez BAI07

DOMINIO: CONSTRUIR, ADQUIRIR E IMPLEMENTAR

BAI07 Gestionar la Aceptación del Cambio y la Transición

Aceptar formalmente y hacer operativas las nuevas soluciones, incluyendo la planificación de la implementación, la conversión de los datos y los sistemas, las pruebas de aceptación, la comunicación, la preparación del lanzamiento, el paso a producción de procesos de negocio o servicios TI nuevos o modificados, el soporte temprano en producción y una revisión post-implementación.

BAI07.01 Establecer un plan de implementación.

BAI07.02 Planificar la conversión de procesos de negocio, sistemas y datos.

BAI07.03 Planificar pruebas de aceptación.

BAI07.04 Establecer un entorno de pruebas.

BAI07.05 Ejecutar pruebas de aceptación

BAI07.06 Pasar a producción y gestionar los lanzamientos.

BAI07.07 Proporcionar soporte en producción desde el primer momento.

BAI07.08 Ejecutar una revisión post implantación.

NIVEL DE MADUREZ / **CRITERIO**		**CUMPLE**	**NO CUMPLE**
Nivel 0 Incompleto	No está implementado, poca o inexistente evidencia de cualquier logro de los procesos de gestión de aceptación al cambio y transición	√	
Nivel 1 Ejecutado	Los procesos logran cumplir su propósito		√
Nivel 2 Gestionado	Los procesos del área, gestiona los procesos y los productos resultantes se establecen, controlan y mantienen apropiadamente		√

Nivel 3 Establecido	El área, utiliza procesos definidos basados en estándares y es capaz de alcanzar sus resultados de proceso(planifica, documenta, ejecuta, monitoriza y controla)	√
Nivel 4 Predecible	El proceso establecido y las operaciones de los sistemas, están en una mejora continua y proporcionan mejores prácticas	√
Nivel 5 Optimizado	El proceso predecible es mejorado en forma continua para cumplir los correspondientes objetivos actuales y proyectados de la empresa.	√

GRADO DE MADUREZ

El proceso de ***Gestionar la Aceptación del Cambio y la Transición*** está en el nivel de madurez 0.

HALLAZGOS

* Plan de implementación incompleto

*No hay aprobación de plan implantado.

No hay políticas definidas de cambios a programas en la organización.

RECOMENDACIONES

Establecer un plan de implementación.

Planificar y ejecutar pruebas de aceptación.

Definir las políticas definidas de cambios a programas.

Fuente: Elaboración Propia

Tabla 16: Modelo de Madurez BAI08

DOMINIO: CONSTRUIR, ADQUIRIR E IMPLEMENTAR

BAI08 Gestionar el Conocimiento

Mantener la disponibilidad de conocimiento relevante, actual, validado y fiable para dar soporte a todas las actividades de los procesos y facilitar la toma de decisiones. Planificar la identificación, recopilación, organización, mantenimiento, uso y retirada de conocimiento.

BAI08.01 Cultivar y facilitar una cultura de intercambio de conocimientos.

BAI08.02 Identificar y clasificar las fuentes de información.

BAI08.03 Organizar y contextualizar la información, transformándola en conocimiento.

BAI08.04 Utilizar y compartir el conocimiento.

BAI08.05 Evaluar y retirar la información

NIVEL DE MADUREZ / CRITERIO		CUMPLE	NO CUMPLE
Nivel 0 Incompleto	No está implementado, poca o inexistente evidencia de cualquier logro de los procesos por parte de la empresa o no alcanza su propósito	√	
Nivel 1 Ejecutado	Los procesos logran cumplir su propósito		√
Nivel 2 Gestionado	Los procesos del área, gestiona los procesos y los productos resultantes se establecen, controlan y mantienen apropiadamente		√
Nivel 3 Establecido	El área, utiliza procesos definidos basados en estándares y es capaz de alcanzar sus		√

	resultados de proceso(planifica, documenta, ejecuta, monitoriza y controla)	
Nivel 4 Predecible	El proceso establecido y las operaciones de los sistemas, están en una mejora continua y proporcionan mejores prácticas	√
Nivel 5 Optimizado	El proceso predecible es mejorado en forma continua para cumplir los correspondientes objetivos actuales y proyectados de la empresa.	√

GRADO DE MADUREZ

El proceso de Gestionar el Conocimiento está en el nivel de madurez 0.

HALLAZGOS

* No hay fuentes de información identificadas y clasificadas.

*No hay herramientas donde se pueda actualizar temas de conocimiento.

No hay herramientas que den soporte a la compartición y transferencia de conocimientos.

RECOMENDACIONES

Identificar las fuentes de información y clasificarlas.

Implantar un esquema para gestionar la información no estructurada.

Traspasar el conocimiento a los usuarios mediante técnicas de aprendizajes y herramientas de acceso.

Fuente: Elaboración Propia

Tabla 17: Modelo de Madurez DSS03

DOMINIO: ENTREGAR, SERVIR Y DAR SOPORTE

DSS03 Gestionar Problemas

Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.

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 MADUREZ / CRITERIO		CUMPLE	NO CUMPLE
Nivel 0 Incompleto	No está implementado, poca o inexistente evidencia de cualquier logro de los procesos por parte de la empresa o no alcanza su propósito	√	
Nivel 1 Ejecutado	Los procesos logran cumplir su propósito	√	
Nivel 2 Gestionado	Los procesos del área, gestiona los procesos y los productos resultantes se establecen, controlan y mantienen apropiadamente		√
Nivel 3 Establecido	El área, utiliza procesos definidos basados en estándares y es capaz de alcanzar sus resultados de proceso(planifica, documenta, ejecuta, monitoriza y controla)		√

Nivel 4 Predecible	El proceso establecido y las operaciones de los sistemas, están en una mejora continua y proporcionan mejores prácticas	√
Nivel 5 Optimizado	El proceso predecible es mejorado en forma continua para cumplir los correspondientes objetivos actuales y proyectados de la empresa.	√

GRADO DE MADUREZ

El proceso de Gestionar Problemas está en el nivel de madurez 1.

HALLAZGOS

* No hay una continua supervisión de los problemas y errores en los servicios.

*Tanto los responsables de los procesos, como los de gestión no se reúnen regularmente para discutir los probables o posibles problemas que existen ni de los futuros cambios planificados.

No existe un seguimiento continuo de las tendencias de los problemas.

RECOMENDACIONES:

Identificar problemas a través de los informes de incidencias.

Definir niveles de prioridad mediante consultas, para poder identificar problemas

Supervisar el continuo impacto de los problemas que pueda haber.

Fuente: Elaboración Propia

Tabla 18: Modelo de Madurez DSS04

DOMINIO: ENTREGAR, SERVIR Y DAR SOPORTE

DSS04 Gestionar la Continuidad

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.

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**
Nivel 0 Incompleto	No está implementado, poca o inexistente evidencia de cualquier logro de los procesos por parte de la empresa o no alcanza su propósito	√	
Nivel 1 Ejecutado	Los procesos logran cumplir su propósito		√
Nivel 2 Gestionado	Los procesos del área, gestiona los procesos y los productos resultantes se establecen, controlan y mantienen apropiadamente		√
Nivel 3 Establecido	El área, utiliza procesos definidos basados en estándares y es capaz de alcanzar sus resultados de proceso(planifica, documenta, ejecuta, monitoriza y controla)		√
Nivel 4 Predecible	El proceso establecido y las operaciones de los sistemas, están en una mejora continua y proporcionan mejores prácticas		√
Nivel 5 Optimizado	El proceso predecible es mejorado en forma continua para cumplir los correspondientes objetivos actuales y proyectados de la empresa.		√

GRADO DE MADUREZ

El proceso de Gestionar la Continuidad está en el nivel de madurez 0.

HALLAZGOS

* No hay un plan de continuidad de TI documentado con los objetivos de negocio. Por lo tanto no identifican los requerimientos. Solo está el compromiso de realizar las recomendaciones por las partes interesadas,

*No existe un seguimiento continuo de las tendencias de los problemas.

RECOMENDACIONES

Identificar procesos de negocios internos, de soporte y actividades de servicio.

Desarrollar y mantener planes de continuidad de negocios operativos.

Documentar los requerimientos de información de respaldo.

Asignar roles y responsabilidades para realizar ejercicios y pruebas de plan de continuidad.

Fuente: Elaboración Propia

Tabla 19: Modelo de Madurez DSS05

DOMINIO: ENTREGAR, SERVIR Y DAR SOPORTE
DSS05 Gestionar los Servicios de Seguridad
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.
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 MADUREZ	CRITERIO	CUMPLE	NO CUMPLE
Nivel 0 Incompleto	No está implementado, poca o inexistente evidencia de cualquier logro de los procesos por parte de la empresa o no alcanza su propósito	√	
Nivel 1 Ejecutado	Los procesos logran cumplir su propósito		√
Nivel 2 Gestionado	Los procesos del área, gestiona los procesos y los productos resultantes se establecen, controlan y mantienen apropiadamente		√
Nivel 3 Establecido	El área, utiliza procesos definidos basados en estándares y es capaz de alcanzar sus resultados de proceso(planifica, documenta, ejecuta, monitoriza y controla)		√
Nivel 4 Predecible	El proceso establecido y las operaciones de los sistemas, están en una mejora continua y proporcionan mejores prácticas		√
Nivel 5 Optimizado	El proceso predecible es mejorado en forma continua para cumplir los correspondientes objetivos actuales y proyectados de la empresa.		√

OBSERVACIONES

GRADO DE MADUREZ

El proceso de Gestionar los servicios de Seguridad, está en el nivel de madurez 0.

HALLAZGOS

- No evalúan regularmente la información sobre posibles amenazas.
- No hay un filtro para el tráfico entrante, descargas, etc.
- No hay una configuración de los sistemas operativos de forma segura.
- No hay revisiones regulares de gestión de todas las cuentas.

- No hay restricciones a ciertos accesos al sistema.
- No hay una supervisión en los puntos de entrada, como empleados, visitantes, etc.
- No hay un inventario a ciertos dispositivos de salida.

RECOMENDACIONES:

Instalar y activar herramientas de protección frente a software malicioso.

Revisar y evaluar regularmente la información sobre nuevas o posibles amenazas.

Implementar mecanismos de filtrados de red, como cortafuegos.

Gestionar el acceso y configurar la red de forma segura.

Fuente: Elaboración Propia

Tabla 20: Modelo de Madurez MEA01

SUPERVISAR, EVALUAR Y VALORAR (MEA)
MEA01 Monitorear, Evaluar y Valorar el Desempeño y Cumplimiento *Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada* ***MEA01.01 Establecer un enfoque de la supervisión.*** ***MEA01.02 Establecer los objetivos de cumplimiento y rendimiento.*** ***MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento.*** ***MEA01.04 Analizar e informar sobre el rendimiento.*** ***MEA01.05 Asegurar la implantación de medidas correctivas.***

NIVEL DE MADUREZ	**CRITERIO**	**CUMPLE**	**NO CUMPLE**
Nivel 0 Incompleto	No está implementado, poca o inexistente evidencia de cualquier logro de los procesos por parte de la empresa o no alcanza su propósito	√	

Nivel 1 Ejecutado	Los procesos logran cumplir su propósito	√	
Nivel 2 Gestionado	Los procesos del área, gestiona los procesos y los productos resultantes se establecen, controlan y mantienen apropiadamente		√
Nivel 3 Establecido	El área, utiliza procesos definidos basados en estándares y es capaz de alcanzar sus resultados de proceso(planifica, documenta, ejecuta, monitoriza y controla)		√
Nivel 4 Predecible	El proceso establecido y las operaciones de los sistemas, están en una mejora continua y proporcionan mejores prácticas		√
Nivel 5 Optimizado	El proceso predecible es mejorado en forma continua para cumplir los correspondientes objetivos actuales y proyectados de la empresa.		√

OBSERVACIONES

GRADO DE MADUREZ

El proceso de Monitorear, evaluar y valorar el Desempeño y cumplimiento, está en el nivel de madurez 0.

HALLAZGOS

- No hay revisiones regulares de gestión de todas las cuentas.
- No hay restricciones a ciertos accesos al sistema.
- No hay una supervisión en los puntos de entrada, como empleados, visitantes, etc.
- No hay un inventario a ciertos dispositivos de salida.

RECOMENDACIONES

Identificar e involucrar a las partes interesadas de los procesos

Solicitar, priorizar y reservar los recursos para la supervisión

Recopilar datos de los procesos definidos

Utilizar herramientas y sistemas apropiadas para el procesamiento y formateo de datos para su análisis

Fuente: Elaboración Propia

Tabla 21: Modelo de Madurez MEA02

SUPERVISAR, EVALUAR Y VALORAR (MEA)

MEA01 Supervisar, Evaluar y Valorar el Sistema de Control Interno

Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.

MEA02.01 Supervisar el control interno.

MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio.

MEA02.03 Realizar autoevaluaciones de control.

MEA02.04 Identificar y comunicar las deficiencias de control

MEA02.05 Garantizar que los proveedores de aseguramiento son independientes y están cualificados.

MEA02.06 Planificar iniciativas de aseguramiento.

MEA02.07 Estudiar las iniciativas de aseguramiento.

MEA02.08 Ejecutar las iniciativas de aseguramiento.

NIVEL DE MADUREZ / CRITERIO		CUMPLE	NO CUMPLE
Nivel 0 Incompleto	inexistente evidencia para evaluar de forma continua	√	
Nivel 1 Ejecutado	Los procesos, evaluaciones logran cumplir su propósito		√
Nivel 2 Gestionado	Los procesos del área son ejecutados, y facilitan la identificación de deficiencias en el control productos resultantes se establecen, controlan y mantienen apropiadamente		√

Nivel 3 Establecido	Utiliza procesos definidos, gestionados, basados en los estándares, marcos establecidos de gobierno	√
Nivel 4 Predecible	El proceso es establecido y las operaciones de los sistemas, están en una mejora continua y proporcionan mejores prácticas para supervisar y controlar los TI	√
Nivel 5 Optimizado	El proceso predecible es mejorado en forma continua para cumplir los correspondientes objetivos actuales y proyectados de la empresa.	√

OBSERVACIONES

GRADO DE MADUREZ

El proceso de ***Supervisar, Evaluar y Valorar el Sistema de Control Interno*** está en el nivel de madurez 0.

HALLAZGOS

- Hay actividades de evaluación, pero no hay seguimiento y evaluación de la eficiencia.
- No hay una identificación exacta de los controles claves.
- Desarrollan pero no implementan procedimientos eficientes para los procesos.
- No realizan una evaluación de riesgo documentada

RECOMENDACIONES

Hay que hacer un seguimiento a las actividades que se realiza en el área.

Realizar una evaluación de riesgo y evaluar los procesos para poder diagnosticar el riesgo que pueda tener las TI.

Fuente: Elaboración Propia

RESULTADOS DEL GRADO DE MADUREZ DE LA EVALUACIÓN DE LA SEGURIDAD DEL CENTRO DE DATOS

Tabla 22: Resultados del Grado de Madurez

PROCESOS		NIVELES					
		Incompleto	Ejecutado	Gestionado	Establecido	Predecible	Optimizado
		0	1	2	3	4	5
APO01	Gestionar el Marco de Gestión de TI						
APO04	Gestionar la Innovación						
APO12	Gestionar el Riesgo						
APO13	Gestionar la Seguridad						
BAI06	Gestionar los Cambios						
BAI07	Gestionar la Aceptación del Cambio y la Transición						
BAI08	Gestionar el Conocimiento						
DSS03	Gestionar Problemas						
DSS04	Gestionar la Continuidad						
DSS05	Gestionar los Servicios de Seguridad						
MEA01	Monitorear, Evaluar y Valorar el Desempeño y Cumplimiento						
MEA02	Supervisar, evaluar y valorar el Sistema de Control Interno						

Fuente: Elaboración Propia

Tabla 23: Leyenda

	LEYENDA PARA LOS SIMBOLOS USADOS	LEYENDA PARA LAS CLASIFICACIONES USADAS	
	**Situación actual de la Información**	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.

Fuente: Elaboración Propia

RESUMEN DE PROCESOS Y CRITERIOS DE INFORMACIÓN POR IMPACTO

Tabla 24: 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									
APO01	Administrar los recursos humanos de TI	0.86	0.63	0.86	0.00	0.63	0.00	0.00	
Total real(impacto*nivel real)		1.72	1.26	1.72	0.00	1.26	0.00	0.00	2
Total ideal (impacto* nivel ideal)		4.30	3.15	4.30	0.00	3.15	0.00	0.00	5
APO04	Administrar proyectos	0.86	0.86	0.63	0.00	0.00	0.00	0.00	

Total real(impacto*nivel real)		0.86	0.86	0,63	0.00	0.00	0.00	0.00	1
Total ideal (impacto* nivel ideal)		4.30	4.30	3.15	0.00	0.00	0.00	0.00	5
APO12	Gestionar El Riesgo	0.63	0.63	0.86	0.86	0.63	0.00	0.63	
Total real(impacto*nivel real)		1.26	1.26	1.72	1.72	1.26	0.00	1.26	2
Total ideal (impacto* nivel ideal)		3.15	3.15	4.30	4.30	3.15	0.00	3.15	5
APO13	Gestionar La Seguridad	0.63	0.63	0.86	0.63	0.86	0.00	0.63	
Total real(impacto*nivel real)		0.63	0.63	0.86	0.63	0.86	0.00	0.63	1
Total ideal (impacto* nivel ideal)		3.15	3.15	4.30	3.15	4.30	0.00	3.15	5
CONSTRUIR, ADQUIRIR E IMPLEMENTAR									
BAI06	Gestionar Los Cambios	0.86	0.63	0.63	0.63	0.63	0.00	0.00	
Total real(impacto*nivel real)		086	0.63	0.63	0.63	0.63	0.00	0.00	1
Total ideal (impacto* nivel ideal)		4.30	3.15	3.15	3.15	3.15	0.00	0.00	5
BAI07	Gestionar La Aceptación Del Cambio Y La Transición	0.86	0.63	0.00	0.63	0.63	0.63	0.00	
Total real(impacto*nivel real)		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0
Total ideal (impacto* nivel ideal)		4.30	3.15	0.00	3.15	3.15	3.15	0.00	5
BAI08	Gestionar El Conocimiento	0.63	0.63	0.00	0.86	0.63	0.86	0.00	
Total real(impacto*nivel real)		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0
Total ideal (impacto* nivel ideal)		3.15	3.15	0.00	4.30	3.15	4.30	0.00	5
ENTREGA, SERVICIO Y SOPORTE									
DSS03	Gestionar Problemas	0.86	0.86	0.00	0.63	0.00	0.00	0.00	
Total real(impacto*nivel real)		0.86	0.86	0.00	0.63	0.00	0.00	0.00	1
Total ideal (impacto* nivel ideal)		4.30	4.30	0.00	3.15	0.00	0.00	0.00	5
DSS04	Gestionar La Continuidad	0.86	0.63	0.00	0.00	0.86	0.00	0.00	
Total real(impacto*nivel real)		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0

Total ideal (impacto* nivel ideal)		4.30	3.15	0.00	0.00	4.30	0.00	0.00	5
DSS05	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	0.00	0.00	0.00	0.00	0.00	0
Total ideal (impacto* nivel ideal)		0.00	0.00	4.30	4.30	3.15	3.15	3.15	5
SUPERVISAR, EVALUAR Y VALORAR									
MEA01	Supervisar, Evaluar Y Valorar El Rendimiento Y La Conformidad	0.86	0.86	0.63	0.63	0.00	0.63	0.00	
Total real(impacto*nivel real)		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0
Total ideal (impacto* nivel ideal)		4.30	4.30	3.15	3.15	0.00	3.15	0.00	5
MEA02	Supervisar, Evaluar Y Valorar El Sistema De Control Interno	0.86	0.86	0.63	0.00	0.63	0.00	0.00	
Total real(impacto*nivel real)		0.86	0.86	0.63	0.00	0.63	0.00	0.00	1
Total ideal (impacto* nivel ideal)		4.30	4.30	3.15	0.00	3.15	0.00	0.00	5

Fuente: Elaboración Propia

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

Fuente: Elaboración Propia

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

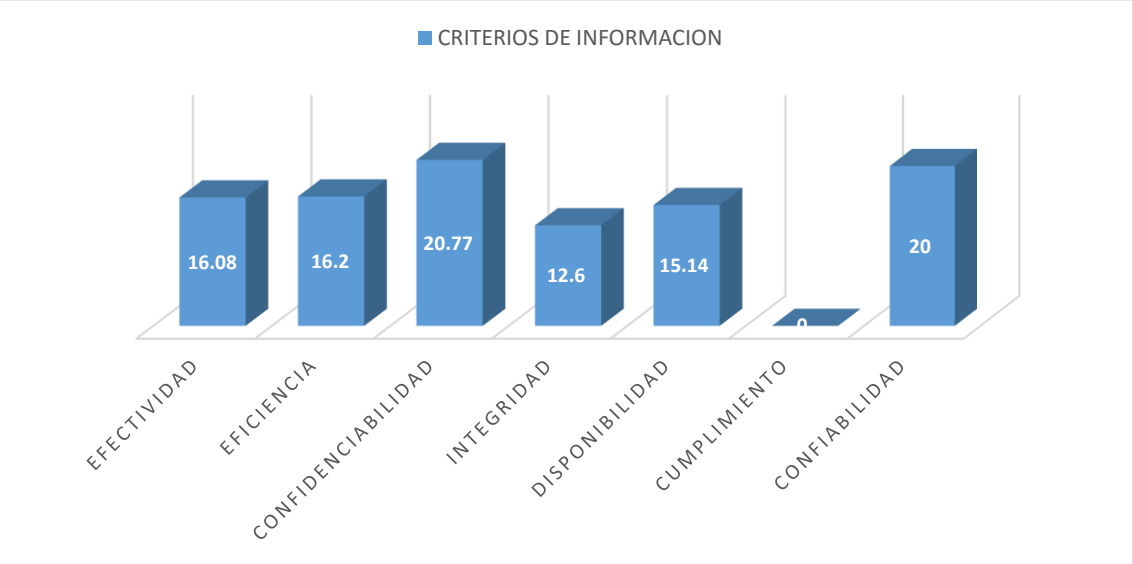
Resultados Finales Del Impacto Sobre Los Criterios De Información

TABLA 25: RESULTADOS DE IMPACTO

TOTAL REAL	7.05	6.36	6.19	3.61	4.64	0.00	1.89	
TOTAL IDEAL	43.85	39.25	29.80	28.65	30.65	13.75	9.45	
PORCENTAJE ALCANZADO	16.08	16.20	20.77	12.60	15.14	0.00	20.00	**14.40**

Fuente: Elaboración Propia

TABLA: 26 Cuadro de Barras –Resultados Finales de Impacto



Fuente: Elaboración Propia

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

EFECTIVIDAD. - Para este criterio de información se obtuvo un porcentaje del 16.08% sobre 100%, es decir que la información de importancia para La Municipalidad Distrital de Nuevo Chimbote, que tiene incidencia en los procesos del negocio y debe ser entregada de forma oportuna, consistente, y veraz tiene un porcentaje del 16.08% (Ver Tabla 30).

EFICIENCIA. - Para este criterio de información se obtuvo un porcentaje del 16.20% sobre el 100%, es decir que la información que debe generar el uso óptimo de los recursos La Municipalidad Distrital de Nuevo Chimbote tiene un porcentaje de16.20% (Ver Tabla 30).

CONFIDENCIALIDAD. - Para este criterio de información se obtuvo un porcentaje del 20.77% sobre el 100%, es decir que la protección de la información La Municipalidad Distrital de Nuevo Chimbote para que esta no sea divulgada a personas o sectores extraños a este tiene un porcentaje del 20.77% (Ver Tabla 30).

INTEGRIDAD. - Para este criterio de información se obtuvo un porcentaje del 12.60% 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 12.60% (Ver Tabla 30).

DISPONIBILIDAD. - Para este criterio de la información se obtuvo un porcentaje del 15.14% 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 La Municipalidad Distrital de Nuevo Chimbote, tiene porcentaje del 15.14% (Ver Tabla 30).

CUMPLIMIENTO. - Para este criterio de la información se obtuvo un porcentaje de l0.00% sobre el 100%, es decir que el cumplimiento de las leyes, regulaciones, y compromisos contractuales con los cuales está comprometido La Municipalidad Distrital de Nuevo Chimbote tiene un porcentaje del0.00% (Ver Tabla 30).

CONFIABILIDAD. - Para este criterio de la información se obtuvo un porcentaje del 20.00% sobre el 100%, es decir proveer la información apropiada para que la administración tome decisiones adecuadas para manejar y cumplir con sus responsabilidades, tiene porcentaje del 20.00% (Ver Tabla 30).

TABLA 27: PLAN DE ACCION

PLAN DE ACCIÓN 1:
GESTIONAR EL MARCO DE GESTION DE TI
Descripción: Teniendo ya un plan estratégico, se deberá establecer un comité estratégico de TI a nivel de la Dirección Ejecutiva de la empresa, como parte del Gobierno corporativo. Brindará asesoramiento sobre la dirección estratégica y apoyas a la demás Áreas. La Municipalidad Distrital de Nuevo Chimbote junto con el Área de Sistemas, deberá definir los elementos básicos de un ambiente de control para TI, que fomente la colaboración entre distintos departamentos y el trabajo en equipo, promueve el cumplimiento y la mejora continua de procesos, y maneje las desviaciones de forma adecuada Mantendrá una estructura óptima, comunicación y coordinación entre las funciones del TI y los interesados dentro y fuera del mismo. Deberá definir cómo se cumplirán y medirán los objetivos, cómo serán autorizados y cómo se asignará la responsabilidad. ACTIVIDADES PRINCIPALES: ✓ Alinear los objetivos de TI y de negocio ✓ Establecer las actividades del comité de TI ✓ Establecer e implementar los roles y responsabilidades de TI ✓ Establecer e implementar las funciones entre TI y otros interesados. ✓ Identificar los dueños de sistemas, procesos y datos

Fuente: Elaboración Propia

TABLA 28: PLAN DE ACCION

PLAN DE ACCIÓN 2:
GESTIONAR EL RIESGO Y SEGURIDAD
Descripción: El Área de Sistemas de la Municipalidad Distrital de Nuevo Chimbote, Sobre todo el jefe del Área deberá establecer ciertos procedimientos y asegurar que exista as acciones de gestión necesarias para los riesgos significativos y estén bajo control, sobre todo que estén implementadas y gestionar las oportunidades para reducir el riesgo a un nivel aceptable. Luego Establecer un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información. **ACTIVIDADES PRINCIPALES:** ✓ Recopilar datos, analizar y responder al riesgo por más insignificativo que sea. ✓ Medir y analizar el tipo de riesgo capturar los datos relevantes sobre incidentes, problemas. ✓ Definir roles, responsabilidades de la gestión de la seguridad de la información. ✓ Mantener un inventario de soluciones implementados para gestionar los riesgos relacionados con la seguridad. ✓ Recomendar programas de formación en seguridad de la información

Fuente: Elaboración Propia

TABLA 29: PLAN DE ACCION

PLAN DE ACCIÓN 3:
GESTIONAR LOS CAMBIOS
Descripción: Los cambios son realizados de acuerdo a los cronogramas respectivo, si hubiera que instalar software, el encargado de la Seguridad del Área de Sistemas de la Municipalidad Distrital de Nuevo Chimbote, deberá dar restricciones explícitas para descargar e instalar software por partes de los demás trabajadores. Deberá dar aplicar las restricciones necesarias para el uso del software que instalen. Supervisar todos los cambios de emergencia y realizar revisiones post-implantación involucrando a todas las partes interesadas **ACTIVIDADES PRINCIPALES:** ✓ Evaluar todas las peticiones de cambio para determinar su impacto en los procesos de negocio y los servicios TI, ✓ Elaborar y documentar informes de cambios. ✓ Planificar y programar todos los cambios aprobados.

Fuente: Elaboración Propia

TABLA 30: PLAN DE ACCION

PLAN DE ACCIÓN 4:
GESTIONAR LA CONTINUIDAD
DESCRIPCIÓN: El Área de Sistemas de la Municipalidad Distrital de Nuevo Chimbote, debe desarrollar un Marco de Trabajo para la continuidad de negocio que ayude a guiar el desarrollo de los planes de recuperación de desastres y de contingencias. El marco de trabajo debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de

contingencia de TI. También se deberá desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñados para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser responder de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable.

ACTIVIDADES PRINCIPALES:

- ✓ Iniciar el proyecto con el apoyo y participación de todas las áreas de la Municipalidad Distrital de Nuevo Chimbote.
- ✓ Evaluar los riesgos ordinarios y extraordinarios que la Empresa enfrenta.
- ✓ Elaboración de un análisis de impacto al negocio y valoración de riesgo
- ✓ Desarrollar y mantener los planes de continuidad de TI.
- ✓ Comunicar y capacitar a los usuarios de interés sobre el plan de continuidad.

Fuente: Elaboración Propia

TABLA 31: PLAN DE ACCION

PLAN DE ACCIÓN 5:
IMPLEMENTAR HERRAMIENTAS AUTOMATIZADAS DE TI
DESCRIPCIÓN: El Área de Sistemas de la Municipalidad Distrital de Nuevo Chimbote, debe implementar el uso de herramientas automatizadas de TI que estén de acuerdo con los requerimientos del negocio que incluya apropiados controles, seguimiento y supervisión de seguridad, soporte y el diseño de las aplicaciones, la inclusión apropiada de controles que brinden un nivel de seguridad y soporte al área de TI. Esto permitirá a la organización apoyar la operatividad del negocio con herramientas automatizadas correctas, como por ejemplo: herramientas de gestión de usuarios y cambios a programas, herramientas de gestión de incidentes y soporte a usuarios, herramientas para la captura y registro de transacciones de usuarios

ACTIVIDADES PRINCIPALES:

- ✓ Brindar a la alta dirección, áreas y usuarios, las claves herramientas automatizadas para clasificar y administrar los sistemas de información.
- ✓ Definir específicamente las herramientas que actualmente se necesitan para el apoyo del Área de Sistemas.
- ✓ Elaboración de un análisis de viabilidad, impacto, costos al negocio y valoración de las herramientas por implementarse.
- ✓ Toda la documentación generada deberá registrarse en una herramienta que permita ser una base de conocimiento para el personal clave de TI y de la organización.

Fuente: Elaboración Propia

4. ANALISIS Y DISCUSION

Después de haber analizado, trabajado los resultados y haciendo uso de los instrumentos que apoyaron para la recolección de datos, se puede afirmar que un 86% de la muestra que fue evaluada tienen conocimiento de manuales aprobados por la empresa, mientras que un 14% desconoce de estos procedimientos, pero en el Área de Sistemas resulta alarmante porque el 29% empleados dice que el área cuenta con manuales, para el manejo de información del sistema, 42% dicen que no cuenta con manuales y 29% que no sabe, eso impide realizar un buen manejo al sistema o a los procesos que pueda haber.

Asimismo también se indica que un 71.40% de los usuarios dicen que la información es limitada, 14.30% que es restringido y el 14.30% dice que es accesible; esto nos indica que la aplicación del marco de trabajo COBIT será de gran relevancia para hacer una evaluación enfocados en criterios tales como efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad; la cual coincide con Díaz, Maricela Y Ugarte, Yesenia (2013) donde evalúa la eficiencia y eficacia respecto a la seguridad física, lógica y los procesos Informáticos en la Municipalidad Provincia Huaura- Huacho y así detectar vulnerabilidades existentes en lo relativo a controles de seguridad. Usando COBIT se logró una obtención de reducción en el ambiente de riesgos vigentes e incremento de la confiabilidad, integridad y disponibilidad de la información.

También resulta muy interesante el trabajo de Gualsaquí, Juan, Quito (2013) que propuso de realizar una correcta y aplicada gestión del área de información tecnológica con el marco de Trabajo Cobit 5, permitiendo no solo el aseguramiento y aprovechamiento de los diferentes recursos, 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. Esto lo contrastamos con la entrevista a los usuarios del área de sistemas donde se puede observar que el 100% empleados dice que al aplicar una evaluación o auditoría con un marco de trabajo adecuado a sus requerimientos minimizaría los riesgos que pueda ver en ella.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Al comparar los marcos de trabajo como: ITIL, CMMI, COSO, COBIT4.1 y COBIT5, escogí Al marco de Trabajo COBIT 5 porque proporciona una guía detallada para TI, es una guía y herramienta útil, que tiene como finalidad generar mayores beneficios y optimizar la ejecución de procesos y uso de recursos en relación con los objetivos del TI, como los niveles de madurez en los procesos del TI, proporciona habilitadores que indican cuándo se necesitan procesos, recursos, aplicaciones, infraestructura, etc.

2. La evaluación realizada a través de los niveles de madurez, ayudó a encontrar hallazgos de los procesos los cuales no llegaron a alcanzar el nivel máximo, los cuales permitieron identificar la vulnerabilidad de las mismas. También determinó el impacto de los procesos de TI, sobre la efectividad, eficiencia, confidencialidad, integridad, disponibilidad y cumplimiento del Área de Sistemas de la Municipalidad Distrital de Nuevo Chimbote

3. Por último, Se elaboró planes de acción para la mejora de Área de Sistemas de los procesos de importancia para tomar conciencia y realizar un plan estratégico y asi poder mejorar sus procesos.

RECOMENDACIONES

1. Adecuar los procedimientos de gestión de información, seguridad y atención a usuarios, a un modelo de trabajo basado en normas de calidad y que se adecuen a la empresa. En el caso de utilizar Cobit cuando la empresa es pequeña puede resultar costosa su implementación y por tanto no se justifica.

2. Disponer a la Alta Gerencia, al jefe del Área de Sistemas, tomar acciones en base a las recomendaciones emitidas en cada nivel de madurez. Realizar evaluaciones periódicas a las TI, sistemas de control, con el fin de medir la eficacia y la eficiencia de cada uno de los procesos que se trabajan en el Área de Sistemas, para así obtener una mejora continua en todas las áreas que depende de ella y que estos criterios alcancen el valor ideal que es el 100%.

3. Poner en marcha los planes de acción recomendadas en cada nivel de madurez, para volver a evaluar y así identificar nuevamente la situación actual de la gestión de área de TI.

AGRADECIMIENTO

Quiero empezar Agradeciendo a Dios por haber permitido estar aquí, por ser mi guía, por brindarme la capacidad de lograr mis objetivos trazados.

Agradecer a mis hijos Luciana, Marifé y Gabriel, por su paciencia, por robarles su tiempo, por comprenderme, porque son mi fuerza y motor para poder seguir adelante.

A mis padres Walter y Rosenda, abuelito, mis hermanos, en especial a Danny por su amor, apoyo y confianza. Este nuevo logro y lo que hoy soy; es gracias a ustedes, los amo.

Al Sr. Gonzalo y Martina por confiar, comprender y apoyarme en todo momento.

A mis profesores ingenieros, a la Universidad San Pedro, a la escuela de Ingeniería Informática y de Sistemas, por ser parte de la culminación de esta tesis y a la empresa que me brindó toda la información necesaria para hacer posible este proyecto.

BIBLIOGRAFÍA

Anasi Suntasig, Karina Isabel y Pasquel 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. Tesis de Título. Escuela Politécnica Nacional, Quito-Ecuador.
Recuperado de http://bibdigital.epn.edu.ec/handle/15000/6672

Andrade España, Diana Lissette (2016*). "Evaluación del Sistema de Gestión de Seguridad de la Información del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas (GADPE)".* Tesis de Título. Universidad Católica del Ecuador, Esmeraldas – Ecuador.

Recuperado de http://hdl.handle.net/123456789/788

Baldeón, M. 2012. Plan maestro de seguridad informática con lineamiento de la norma ISO 27002. p 2. México.

Castro, E. (2009). Tendencias de la auditoria informática. Cali, CO. Revista Ingenlum Ciencia & Tecnología. Vol. 4, Nº 8. P, 69- 98.

Cobit., C. D. (1198). Directrices de Auditoría. (Segunda Edición).

Cobit 5, (2009-2011)- Procesos Catalizadores - 2012 ISACA.
Todos los derechos reservados. Para pautas de uso, ver *www.isaca.org/COBITuse*.

Díaz Marcelo, M. y Ugarte Espinoza, Y. (2013). *Auditoria de Seguridad Informática aplicada a la Municipalidad Provincial Huaura - Huacho*. Tesis de Título. Universidad San Pedro, Huacho, Perú.

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

Morlanes, G. (2012). Seguridad Informática, Matanzas, CU. Revista de Arquitectura e Ingeniería, vol. 6, Nº 2. p. 1-14

Piattini, Del Peso, M. (2008). Auditoria de Tecnologías y Sistemas de Información. 4ed. Madrid, ES. RA-MAl. Vol. 1378. p 38.

Yan y Zavala, (2013). *Plan De Mejora De La Seguridad De Información Y Continuidad Del Centro De Datos De La Gerencia Regional de Educación La Libertad Aplicando Lineamientos ISO 27001 Y Buenas Prácticas COBIT*, Tesis de Título Trujillo-Perú

Recuperado:

http://repositorio.upao.edu.pe/bitstream/upaorep/645/1/YAN_FREDDY_MEJORA_SEGURIDAD_COBIT.pdf

ANEXOS

ANEXO 1: ENTREVISTA

ENTREVISTA A LOS USUARIOS DEL AREA DE SISTEMAS

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 informática del área de sistemas con la que actualmente cuenta Municipalidad Distrital de Nuevo Chimbote.

Pregunta 1:

¿Conoce el organigrama de la empresa?

Pregunta 2:

¿Tiene conocimiento si hay manuales o procedimientos en la empresa aprobados por la gerencia?

Pregunta 3:

¿En el área donde labora, cuenta con procedimientos, manuales, instructivos establecidos para el manejo de información del sistema?

Pregunta 4:

¿Existe algún manual de contingencia elaborado y aprobado por la gerencia?

Pregunta 5:

¿Existen prohibiciones sobre la instalación o uso de programas no autorizados en los equipos de la empresa?

Pregunta 6:

¿La información que facilita el sistema es?

Pregunta 7:

¿El manejo del Sistema es?

Pregunta 8:

¿Se presentan dificultades o inconvenientes en el sistema?

Pregunta 9:

¿Con que frecuencia existen las dificultades?

Pregunta 8:

¿En cuánto tiempo se resuelve las dificultades presentadas en el sistema?

Pregunta 9:

¿Puede recuperar sus datos si por alguna razón se borran o falla el sistema?

Pregunta 10:

¿Se presentan dificultades o inconvenientes en el sistema?

Pregunta 11:

¿El acceso a la información del sistema es?

Pregunta 12:

¿Brindan capacitaciones o asesoramientos, cuando implementan algún sistema?

Pregunta 13:

¿Se realizan inventarios del hardware?

Pregunta 14:

¿Se realizan mantenimiento preventivo y correctivo del software y hardware?

Pregunta 15:

¿Tienen implementado un antivirus en los equipos informáticos?

Pregunta 16:

¿Toma decisiones adecuadas frente a un imprevisto?

Pregunta 17:

¿Cuentan con un plan estratégico en TI?

Pregunta 18:

¿Se han asignado roles, tareas para asegurar el plan estratégico?

Pregunta 19:

Se cumplen con los objetivos de las TI en el plan estratégico

Pregunta 20:

¿Cree usted que la realización de una evaluación o auditoría, brindará beneficios en el desarrollo de su trabajo?