UNIVERSIDAD CATÓLICA DE SANTA MARÍA

Facultad de Ciencias e Ingenierías Físicas y Formales

Escuela Profesional de Ingeniería de Sistemas

MEJORA DE LOS PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN APLICANDO COBIT 5.0 Y LA NORMA TÉCNICA PERUANA NTP-ISO 27001: 2014. CASO: AUTORIDAD AUTÓNOMA DE MAJES.

Tesis presentada por el Bachiller:

Angulo Osorio, Javier Fernando

Para optar el Título Profesional de:

INGENIERO DE SISTEMAS:

ESPECIALIDAD EN SISTEMAS DE INFORMACIÓN

Asesor: Ing. Néstor Torres Gamarra

AREQUIPA - PERÚ

2018

0013

ACTA TITULO PROFESIONAL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

En Arequipa, a los 16 días del mes de enero del 2018 siendo las 12.00 horas, en el local de la Universidad Católica de Santa María, se reunió el Jurado

Presidido por: Ing. César Basilio Baluarte Araya

Integrantes : Ing. Néstor Torres Camarra

Ing. Karina Rosas Paredes

Actuando este último como Secretario con la finalidad de recibir las previas orales del(os) (la) (s) Señor(ita) Bachiller(s)

Javier Fernando Angulo Osorio

Quien(es) pretende(n) optar el Título Profesional de INGENIERO DE SISTEMAS: ESPECIALIDAD EN SISTEMAS DE INFORMACION

Sustentando: la tesis

Titulado"Mejora de los procesos de Tecnologías de la Información aplicando COBIT 5.0 y la norma técnica Peruana NTP-ISO 27001:2014. Caso: Autoridad Autonoma de Majes"

El Presidente del Jurado invitó al (los) Titulando(s) a hacer una exposición de su trabajo, conclusiones y recomendaciones, para luego proceder a realizar las preguntas que los Miembros del Jurado consideraron pertinente plantear. Posteriormente, se pasó a deliberar y emitir su voto en la forma establecida por el Reglamento de Grados y Títulos de la Facultad de Ciencias e Ingenierías Físicas y Formales siendo el resultado el siguiente:

Aprobado por unanimidad

Con lo que se dio por terminado el Acto siendo las 14.00 horas, para dar fe firmamos a continuación los Miembros del Jurado y el (los) Titulado(s).

PRESIDENTE

SECRETARIO

INTEGRANTE

TITULANDO

TITULANDO

09

UNIVERSIDAD CATOLICA DE SANTA MARIA
URB. SAN JOSE S/N - UMACOLLO

FACULTAD DE CIENCIAS E INGENIERIAS FISICAS Y FORMALES

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

INFORME DICTAMEN DE BORRADOR DE TESIS

VISTO

El Borrador de Tesis titulado:

Mejora de los procesos de tecnología de la información aplicando COBIT 5.0 y la norma técnica peruana NTP-ISO 27001:2014: Caso: Autoridad Autónoma de Majes

Presentado por (el) (la) (los) Bachiller (es):

Javier Fernando Angulo Osorio

Nuestro dictamen es:

Progreso

OBSERVACIONES:

Arequipa, 29 de DICIEMBRE de 2017

NESTOR TORRES GAMARRA

CESAR BALUARTE ARAYA

(5154) 382038 (5154) 252542 ucsm@ucsm.edu.pe http://www.ucsm.edu.pe

0441314

PRESENTACIÓN

Director de la Escuela Profesional de Ingeniería de Sistemas

Sres. Miembros del Jurado.

De conformidad con las disposiciones del Reglamento de Grados y Títulos de la Escuela Profesional de Ingeniería de Sistemas, pongo a vuestra consideración el presente trabajo de aplicación titulado:

"MEJORA DE LOS PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN APLICANDO COBIT 5.0 Y LA NORMA TÉCNICA PERUANA NTP-ISO 27001: 2014. CASO: AUTORIDAD AUTÓNOMA DE MAJES.", el mismo que de ser aprobado me permitirá optar el Título Profesional de Ingeniero de Sistemas.

Javier Fernando Angulo Osorio

Bachiller en Ing. de Sistemas

AGRADECIMIENTOS

Agradezco a la UNIVERSIDAD CATÓLICA DE SANTA MARÍA por brindarme los conocimientos teóricos, prácticos y valores éticos y morales para convertirme en un profesional.
A mi asesor de tesis, Ing. Néstor Torres Gamarra, quien me brindó su conocimiento, experiencia y tiempo para la elaboración del presente proyecto.
Agradezco a los docentes de la ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS, que durante toda mi carrera profesional aportaron con mi desarrollo académico.
También agradezco a mis padres, amigos y personas que a lo largo del camino me apoyaron en mi constante mejora como persona y profesional.

EPÍGRAFE

"*Quien piensa en fracasar, ya fracasó antes de intentar; quien piensa en ganar, lleva ya un paso adelante*"

Sigmund Freud

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Con la creación de la Política Nacional de Modernización de la Gestión Pública, el enfoque que deben tomar todas las instituciones del estado debe ser orientado a los procesos, ya que es una efectiva estrategia de gestión, fortaleciendo la capacidad para lograr resultados en un conjunto, sistematizado con el fin de fortalecer el rol de cada uno de los organismos que lo integren.

Por esto que, proporcionar la mejora de los procesos de tecnologías de información en la Autoridad Autónoma de Majes aplicando COBIT 5 y la NTP-ISO 27001:2014, permitirán crear valor a través del uso efectivo e innovador de las tecnologías de información de éste organismo, además de, satisfacer al usuario con el nivel de compromiso, los servicios de tecnologías de información y la mejora en las relaciones entre las necesidades del negocio y las metas de tecnologías de información, todo bajo el enfoque de la seguridad de la información.

Para el presente trabajo, se desarrolló la descripción de servicios informáticos y sus procesos en la actualidad (AS – IS) y las mejoras respectivas basándolas en COBIT 5 y la NTP 27001:2014 (TO – BE).

Palabras Clave

COBIT 5, NTP-ISO 27001:2014.

ABSTRACT

With the creation of the National Policy for the Modernization of Public Management, the approach to be taken by all state institutions must be process-oriented, since it is an effective management strategy, strengthening the capacity to achieve results in a set, systematized in order to strengthen the role of each of the agencies that integrate it.

Therefore, providing the improvement of information technology processes in the Autonomous Authority of Majes applying COBIT 5 and NTP-ISO 27001: 2014, will create value through the effective and innovative use of the information technologies of this organization , in addition to satisfying the user with the level of commitment, the information technology services and the improvement in the relationships between business needs and information technology goals, all under the focus of information security.

For the present work, the description of IT services and their processes at present (AS - IS) and the respective improvements were developed based on COBIT 5 and NTP 27001: 2014 (TO - BE).

Keywords

COBIT 5, NTP-ISO 27001:2014.

INTRODUCCIÓN

Según la Política Nacional de Modernización de la Gestión Pública, la Autoridad Autónoma de Majes cambiará el modelo de organización funcional y migrará hacia una organización por procesos, que asegure un impacto positivo para el ciudadano utilizando todos los recursos disponibles, en el caso de las tecnologías de información, la adopción de marcos de trabajo como COBIT 5 y la aplicación de una norma como la NTP-ISO 27001:2014 permitirán mejorar los procesos de tecnologías de información bajo la gobernanza de tecnologías de información y su enfoque en la seguridad de la información.

Descripción de los capítulos:

Capítulo I.- denominado planteamiento del problema, desarrolla el planteamiento del problema, el objetivo general, los objetivos específicos, las preguntas de aplicación, la línea y sub-línea de investigación, la justificación e importancia, los aportes, alcances y limitaciones, población y muestra o universo y métodos, técnicas e instrumentos empleados.

Capítulo II.- denominado fundamentos teóricos, desarrolla el estado del arte y las bases teóricas del trabajo.

Capítulo III.- denominado mejora de procesos de tecnologías de información, desarrolla el estado actual de la organización (AS – IS) y el estado deseado de la organización (TO –BE).

Capítulo IV.- denominado resultados, desarrolla los hallazgos del presente trabajo.

Capitulo V.- denominado análisis y discusión, desarrolla un análisis de los resultados obtenidos.

CAPÍTULO I:
PLANTEAMIENTO DEL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

La información es un recurso clave para todas las organizaciones, desde las más pequeñas, hasta las grandes multinacionales, no sólo siendo importante cuando es creada o modificada sino hasta cuando es destruida, es por esto que la tecnología es la que juega el rol más importante y más aún cuando está avanzando cada vez más y se ha generalizado en todo entorno.

El área de servicios informáticos de la Autoridad Autónoma de Majes busca la interacción con las demás áreas administrativas para el soporte y gestión de sus requerimientos de bienes y servicios de tecnologías de información, teniendo como objetivos según ISACA(2012):

- Mantener información de calidad para soportar las decisiones de las distintas unidades operativas.
- Generar valor al negocio con las inversiones en tecnologías de información.
- Optimizar el coste de los servicios y tecnologías de información.
- Cumplir constantemente con las crecientes leyes, regulaciones, acuerdos contractuales y políticas aplicables.

Las empresas de éxito mundial han reconocido que las organizaciones deben aceptar a las tecnologías de información como cualquier otra parte importante de la jerarquía del negocio. Los comités y la dirección, tanto en funciones de negocio, como de tecnologías de información deben colaborar y trabajar juntos, de modo que se incluya a las tecnologías de información en el enfoque del gobierno y su gestión. Además, cada vez se aprueban más legislaciones y se implementan regulaciones para cubrir esta necesidad, la aplicación de COBIT 5 provee de un marco de trabajo integral que

ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las tecnologías de información como lo expone ISACA(2012).

ISACA(2012) también propone que COBIT 5 permite a las tecnologías de información ser gobernadas y gestionadas a partir de sus factores externos (como el mercado, la industria, etc.) y factores internos (la cultura organizacional, la gestión de riesgos, etc.) abarcando al negocio por completo de principio a fin y las áreas funcionales de responsabilidad de las tecnologías de información, considerando los intereses relacionados con las tecnologías de información de las partes interesadas internas y externas. COBIT 5 al ser genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público, es válidamente aplicado a la Autoridad Autónoma de Majes ya que, actualmente servicios informáticos no se encuentra en la estructura organizacional de la institución, tampoco cuenta con procesos bien definidos, actualizados, sin gestión de inicidentes y no poseen documentación de las actividades realizadas.

Pero la implementación de COBIT no sólo debe enfocarse en los avances de las tecnologías, en los sistemas de información, las telecomunicaciones y la evolución de la sociedad de la información, ya que las organizaciones se ven expuestas a riesgos que deben ser mitigados, tratados o transferidos. Por lo tanto, basar el presente trabajo en la norma NTP-ISO/IEC 27001:2014 va a permitir a la Autoridad Autónoma de Majes proteger y asegurar su activo más importante: la información, apoyando a la continuidad y controlar las debilidades detectadas en el negocio.

Al enfocar nuestro proyecto en la gestión de la información, es posible la disminución significativa de los riesgos de la información para cada proceso de negocio de la organización sin realizar grandes inversiones que perjudiquen los presupuestos de la Autoridad Autónoma de Majes.

Con la aplicación de la NTP-ISO/IEC 27001:2014 a los procesos mejorados con COBIT 5, se podrán establecer políticas, procedimientos y controles alineados a los

objetivos de negocio con el objetivo de mantener los riesgos de tecnologías de información asumibles por la organización.

1.2. OBJETIVOS DEL PROYECTO

1.2.1. Objetivo General

Mejorar los procesos de tecnologías de la información aplicando COBIT 5.0 y la norma técnica peruana NTP-ISO 27001: 2014. Caso: Autoridad Autónoma de Majes.

1.2.2. Objetivos Específicos

- Definir los procesos de tecnologías de información de la Autoridad Autónoma de Majes.
- Aplicar los principios claves de COBIT 5 a los procesos de tecnologías de información de la Autoridad Autónoma de Majes para su mejora.
- Realizar un análisis y gestión de los riesgos propuestos por la NTP-ISO 27001:2014 basada en los procesos de negocio y servicios de tecnologías de información de la Autoridad Autónoma de Majes.

1.3. PREGUNTAS DE APLICACIÓN

- ¿Cómo se puede mejorar la eficiencia de los procesos de tecnologías de información aplicando COBIT 5.0 y la norma técnica peruana NTP-ISO 27001:2014. Caso: Autoridad Autónoma de Majes?.
- ¿Cómo se pueden alinear la arquitectura de la información y los recursos de tecnologías de la información, con las estrategías y objetivos del negocio, con el fin de mejorar los procesos de tecnologías de la información de la Autoridad Autónoma de Majes aplicando COBIT 5.0 y la norma técnica peruana NTP-ISO 27001:2014.?.

1.4. LÍNEA Y SUB-LÍNEA DEL PROYECTO

1.4.1. Línea

Sistemas de Información y Bases de Datos

1.4.2. Sub-Línea

Tecnologías de Información

1.5. JUSTIFICACIÓN E IMPORTANCIA

ISACA (2012) expone que debido a que la información es un recurso clave, la implementación de COBIT permite mantener información de calidad, generar valor al negocio con las inversiones de tecnologías de información, alcanzar la excelencia operativa, mantener los riesgos en un nivel aceptable, optimizar los costos de servicios y tecnologías de información y cumplir con las regulaciones y políticas aplicables en cualquier tipo de organización.

COBIT permite enlazar las metas del negocio con las metas de tecnologías de información, lo que permite conducir las acciones aportando valor al negocio, además del mejoramiento práctico del uso de las tecnologías de información y el aprovechamiento de los recursos tecnológicos de la Autoridad Autónoma de Majes, tal y como lo explica Cumandá(2015) donde la aplicación de COBIT 5 permite alcanzar los objetivos y metas, optimizando los niveles de riesgo y el uso eficiente de los recursos de tecnologías de información.

Por otro lado, Beingolea (2015) expone que la gestión de activos realizada bajo el enfoque de la seguridad de la información permite la identificación y valoración de los activos de la información utilizados dentro del proceso de negocio, es por esto que la aplicación de COBIT a la Autoridad Autónoma de Majes será enfocada a la seguridad de la información teniendo como referencia a la norma técnica peruana NTP-ISO/IEC 27001:2014 para la gestión de riesgos de los procesos de tecnologías de información.

1.6. ALCANCES Y LIMITACIONES

El presente trabajo tiene como alcance mejorar los procesos de tecnologías de información aplicando COBIT 5.0 y la norma técnica peruana NTP-ISO 27001: 2014, en la Autoridad Autónoma de Majes, con el objeto de alcanzar los objetivos de la empresa e incrementar la eficiencia de los mismos, mientras se equilibran los riesgos de los procesos de tecnologías de información.

No existen limitaciones para el desarrollo del presente trabajo, debido a que se cuenta con el financiamiento necesario para costear los gastos en los que se puedan incurrir, además de tener asesoría en aspectos del conocimiento necesario para realizar la mejora de los procesos de tecnologías de información aplicando COBIT 5.0 y la norma técnica peruana NTP-ISO 27001: 2014 en la Autoridad Autónoma de Majes. Por último, se tiene acceso a la empresa donde se aplicará el proyecto, poniendo en práctica la propuesta y tomar las lecturas que sean necesarias a efectos de obtener resultados que permitan determinar el grado de validez de dicha propuesta.

1.7. APORTES

Mejorar los procesos de tecnologías de información aplicando COBIT 5.0 y la norma técnica peruana NTP-ISO 27001: 2014 en la Autoridad Autónoma de Majes permitirá definir los procesos de tecnologías de información, la aplicación de los principios claves de COBIT 5 para su eficiencia, además de la creación de una Unidad de Tecnologías de Información que dependa directamente de la Oficina de Administración, la definición del procedimiento a seguir para el correcto desarrollo de cada uno de los procesos, la asignación de roles por cada actividad, así como la creación de controles que garanticen el desarrollo de todos los procesos de tecnologías de la información de la Autoridad Autónoma de Majes.

1.8. VARIABLES

1.8.1. Variable Independiente

Aplicación de normas de procesos de tecnologías de información.

1.8.1.1 Indicadores

- Número de catalizadores aplicados del dominio Alinear, Planificar y Organizar de COBIT 5.
- Número de controles cumplidos de la norma técnica peruana NTP-ISO 27001:2014.
- Número de requerimientos cumplidos de la norma técnica peruana NTP-ISO 27001:2014.
- Grado de mitigación de los riesgos de tecnologías de información según la norma técnica peruana NTP-ISO 27001:2014.

1.8.2. Variable Dependiente

Mejora de procesos de tecnologías de información de la Autoridad Autónoma de Majes.

1.8.2.1 Indicadores

- Número de procesos de tecnologías de información mejorados.
- Número de necesidades de recursos y prioridades de recuperación de los procesos de tecnologías de información.
- Número de riesgos evaluados en los procesos de tecnologías de información.

- Número de controles aplicados a los procesos de tecnologías de información.

1.9. HIPÓTESIS

Dado que en la actualidad la política nacional de modernización pública, se ha convertido en una exigencia para las entidades de la administración pública, es probable proponer una mejora de los procesos de tecnologías de la información aplicando COBIT 5.0 y la norma técnica peruana NTP-ISO 27001:2014 para la Autoridad Autónoma de Majes.

1.10. POBLACIÓN Y MUESTRA O UNIVERSO

Para este caso, el marco poblacional sujeto al estudio, tiene la característica de ser una institución pública del Gobierno Regional de Arequipa con una gerencia ejecutiva autónoma. Por consiguiente, el universo está representado por todas las empresas públicas gestionadas por el Gobierno Regional de Arequipa, siendo en su totalidad 14 instituciones, la muestra de éste universo está calculada a partir de la siguiente fórmula:

$$m = \frac{4\,n\,.\,p\,.\,q}{e^2(n-1) + 4\,\mathrm{p}\,.\,\mathrm{q}}$$

Donde:

m = Tamaño de la muestra

p = Probabilidad de aplicar mejora de procesos en una institución pública

q = Probabilidad de no aplicar mejora de procesos en una institución pública

e = Error muestral

$$m = \frac{4\,.\,(\,14\,.\;0{,}95\,.\;0{,}05)}{0.05^2(14-1) + 4\,.\,(0{,}05\,.\;0.95)}$$

$$m = 11.96$$

Siendo el resultado 11.96, es redondeado a 12, sin embargo, a efectos de validar la propuesta, se empleará como muestra no probabilística de tipo dirigida a la Autoridad Autónoma de Majes, al ser la única institución estatal con una organización funcional por gerencias, dependiente del Gobierno Regional de Arequipa.

1.11. MÉTODOS, TÉCNICAS E INSTRUMENTOS EMPLEADOS

Para el presente proyecto se utilizará la técnica de la entrevista para poder establecer contacto con los interesados de la organización, posteriormente se utilizará la encuesta como técnica para establecer un diálogo con el área en observación y por último, se utilizará la técnica del análisis documental para poder obtener información del tipo secundaria de la Autoridad Autónoma de Majes, así como de organizaciones que sean variables de interés para el proyecto.

CAPÍTULO II:
FUNDAMENTOS TEÓRICOS

2.1. ESTADO DEL ARTE

Salazar (2016) explica la importancia de la aplicación del marco de referencia COBIT ya que éste brinda un valor agregado a las tecnologías de información, especialmente en el análisis de la situación actual de los procesos de tecnologías de información, lo cual brinda una manera fácil de reconocer la situación actual del área de sistemas e informática de las organizaciones del sector público.

Shameli-Sendi, Aghababaei-Barzegar y Cheriet (2016), afirman que la mejor manera de abordar la implementación de un gobierno de tecnologías de información es mediante un enfoque basado en la seguridad de la información, bajo un proceso de mejora continuo ya que los factores de riesgo tecnológicos cambian constantemente.

Mayadunne y Park (2016), también sostienen que la seguridad de la información ha ido creciendo a nivel exponencial, cambiando la manera de pensar de las organizaciones y tomar una orientación cada vez más preocupada por la seguridad de su información, tal y como lo muestra un estudio realizado donde más del 90% de las instituciones que tomaron parte de la encuesta, esperaban aumentar o mantener por lo menos sus inversiones en seguridad de la información en el futuro.

Ahmad, Maynard y Shanks (2015), presentan en su investigación que el manejo a fallas y ataques de seguridad de la información, son la oportunidad para poder obtener lecciones acerca de seguridad, así como, la mejora de procesos administrativos, sin embargo, también explican que las dos grandes causantes de éstas fallas y ataques, son la falta de comunicación y colaboración entre las distintas áreas de la organización, es por esto que la mejora de procesos de tecnologías de información basada en COBIT y la seguridad de la información, apoyaría en la construcción y mantenimiento de una buena cultura de seguridad, siendo una pieza fundamental en los tiempos actuales, tal como lo explican Dhillon, Syed y Pedron (2015), poniendo énfasis en la protección de la información de la organización.

Safa, y Von Solms (2016), plantean que el intercambio de conocimiento, la colaboración, la intervención de todos los miembros de la organización y la experiencia son elementos importantes en el buen uso de las tecnologías de información, ya que tienen un efecto significativo en los procesos de tecnologías de información.

Shameli-Sendi, Aghababaei-Barzegar y Cheriet (2015), definen a la información como un activo comercial que tiene un valor significativo en todas las organizaciones, es por esto que, debe ser protegido como cualquier otro activo que tenga gran valor para la organización.

Yan y Zavala (2013) explican que una buena práctica en las organizaciones para el área de tecnologías de información, es realizar periódicamente evaluaciones de riesgos con el objeto de minimizar los mismos y priorizar aquellos catalogados como altos. Así como también considerar evaluaciones periódicas de auditoría de sistemas que permitan identificar procesos a mejorar.

También Yan y Zavala (2013) sostienen que en la planificación de una auditoría de sistemas es necesario identificar correctamente los elementos que intervienen, de modo que se tenga una visión global y concreta de los objetivos de la evaluación del proceso.

Beingolea (2015) fundamenta que, en el Perú, lamentablemente, en muchos casos se carece de una adecuada gestión de las tecnologías de información, y de esta manera se impide que éstas proporcionen valor agregado al negocio, por el contrario, pueden llegar a ocasionar mayores complicaciones a la empresa, tales como el incumplimiento de los objetivos del negocio, alta pérdida de dinero en las inversiones en tecnologías de soporte, retrasos en la operatividad, entre otros.

2.2. BASES TEÓRICAS DEL PROYECTO

2.2.1. COBIT

COBIT 5 es la guía para la gestión eficiente de las tecnologías de información en la empresa, según ISACA (2012), la implantación de las prácticas establecidas por COBIT nacen a partir de la necesidad de:

- Analizar los riesgos y su costo.

- Considerar la relación existente entre las compañías externas y los grupos externos que brindan servicios de tecnologías de información.
- Tratar la información relevante y fidedigna para la toma de decisiones empresariales eficaces y eficientes.
- Integrar las tecnologías de información al negocio.
- Proporcionar orientacion en la innovación y las tecnologías emergentes.
- Cubrir las responsabilidades funcionales de las tecnologías de información con el negocio.
- Adquirir control sobre las soluciones de tecnologías de información adquiridas.

Sánchez, Fernández y Ocaña (2013) fundamentan que COBIT puede medir o evaluar los niveles de calidad de las entidades de manera específica, lo que permite que puede ser aplicado en cualquier empresa y su efectividad no va a cambiar, no por el hecho de ser estricto y rígido sino por el hecho que cada una de sus funciones están pre adaptadas a las necesidades del negocio que lo piensa aplicarlo.

También Sánchez, Fernández y Ocaña (2013) indican que COBIT puede ser colocado con otros marcos de gestión para darle valor agregado y de esta manera poder tener una mejor herramienta a la cual poder aplicar buenas prácticas de las tecnologías de información.

Sobre los dominios de COBIT, Sánchez, Fernández y Ocaña (2013) explican que existen dominios como la planificación y organización que son los más utilizados dentro de la gestión de las tecnologías de información como cliente, así como los dominios de adquisición e implementación, entrega y soporte y evaluación y monitoreo que son más desarrollados para la parte del servidor.

Luciano (2011) establece que COBIT da a comprender y tiene en cuenta atributos comunes como sería el diseño de una metodología madura para mostrarla de manera sencilla, lo que brinda una escala de madurez poco

compleja, además indica que los treinta y cuatro procesos pueden poseer un nivel de madurez especifico.

Vieira y Souza (2016) exponen según su experiencia que los objetivos tienen que tener una vinculación entre los procesos de organización y los procesos de las tecnologías de información, si no se llega a una vinculación entre éstas, es posible que la implantación de COBIT falle.

También exponen Vieira y Souza (2016) que conocer el camino de cada proceso es de vital importancia para mantener la vinculación y de esta manera no perder el camino en común de los fines de los *stakeholders* de la organización.

Colomo (2012) expone que COBIT se muestra como un marco de gestión de las tecnologías de información, además de poder mostrarlo como un conjunto de herramientas de apoyo para permitir cerrar las brechas entre las necesidades, las técnicas y los riesgos de negocio de tecnologías de información.

Por lo tanto, COBIT es un modelo de gobierno de tecnologías de información muy robusto, como lo define Poggio (2013), puesto que ayuda a intensificar los controles sobre los procesos de la cadena de suministro de los cuales podrían definirse la gestión de servicio y la gestión de cambios, teniendo éstos controles la función de eliminar o mitigar los riesgos dependiendo del impacto dentro de la gestión de las tecnologías de información.

De esta manera Poggio (2013) explica que, COBIT es la mejor opción para realizar un control real sobre los diferentes procesos dentro de la gestión de las tecnologías de información, sin dejar de lado que es el mejor para reducir riesgos y solucionar problemas.

2.2.1.1. Versiones de COBIT.

COBIT presenta cinco versiones mayores, como se muestran en la siguiente tabla:

*Tabla 1.*Versiones de COBIT

Versión	**Año de publicación**	**Descripción**
1	1996	Colección y análisis de fuentes internacionales de equipos auditores, ésta versión poseía Objetivos de Control y Guías de Auditorías.
2	1998	Se modificaron las guías de gestión, ya que se agregaron las guías de autoevaluación, referencias y material de apoyo adicional.
3	2000	Se mejoró el marco de referencia para el soporte del control gerencial e introdujo el manejo del desempeño y desarrollo del gobierno de tecnologías de información.
4.1	2005	COBIT define 34 procesos que cubren 210 objetivos de control en 4 dominios: Planificación y Organización, Adquisición e Implementación, Entrega y Soporte y Supervisión y Evaluación.
5	2012	Amplía a la versión 4.1 mediante la integración de las normas *Val IT* y *Risk IT*, ITIL y las normas ISO.

Fuente: Elaboración propia

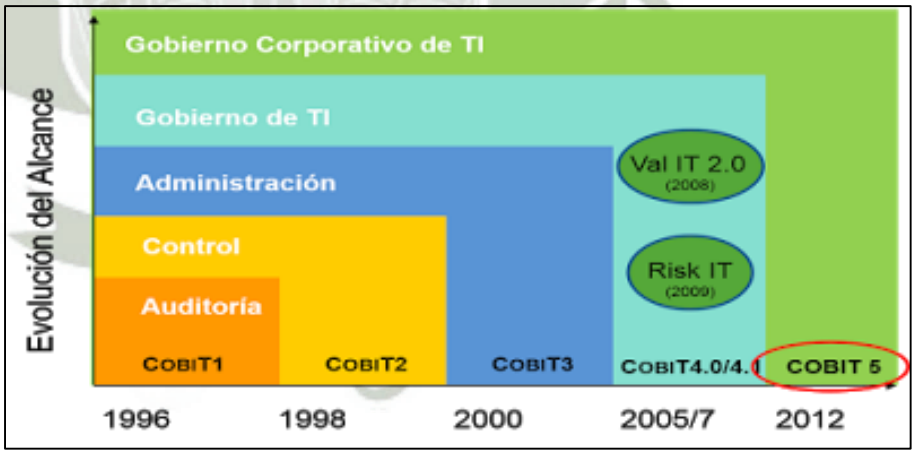


Figura 1. Versiones de COBIT
Fuente: De los Ríos, F. (2013). *Un marco de referencia de negocio para el gobierno y la gestión de las TI de la empresa*. Presentación.

2.2.1.2.Cubrir la Organización de Extremo a Extremo.

ISACA (2012) establece que el objetivo de la gestión de las tecnologías de información debe ser cubierta de extremos a extremo, es decir:

- Integración del gobierno corporativo y las tecnologías de información.
- Cubrir todas las funciones y procesos necesarios para gestionar la información y las tecnologías relacionadas donde quiera que éstas sean utilizadas.

2.2.1.3.Roles, Actividades y Relaciones

ISACA (2012), también expone que COBIT 5 define quiénes están involucrados en los procesos de tecnologías de información, como lo hacen y cómo interactúan, dentro del alcance, como se muestra en la figura 2:

Figura 2. Roles, Actividades y Relaciones Clave
Fuente: ISACA. (2012). Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa - COBIT 5.

2.2.1.4.Modelo de Referencia de Procesos de COBIT.

ISACA (2012), define que las empresas pueden organizar los procesos de tecnologías de información como lo crean por conveniente, pero que las metas establecidas queden cubiertas.

El modelo de referencia de procesos de COBIT 5 según ISACA (2012), divide a los procesos de tecnologías de información en:

- *Gobierno*

Contiene cinco procesos, dentro de cada uno se definen las prácticas de evaluación, orientación y supervisión.

- *Gestión*

  Contiene los cuatro dominios base para la estructura de los procesos:

  - Alinear, Planificar y Organizar (APO).
  - Construir, Adquirir e Implementar (BAI).
  - Entregar, dar Servicio y Soporte (DSS).
  - Supervisar, Evaluar y Valorar (MEA).

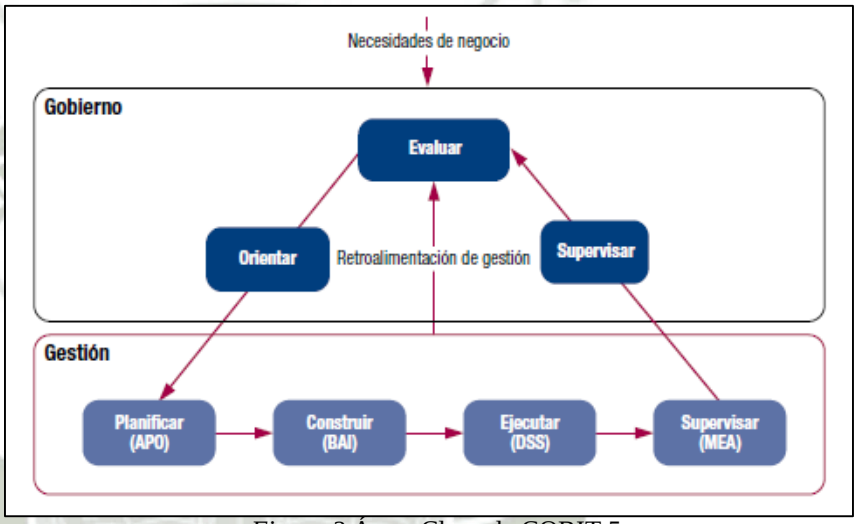


*Figura 3.*Áreas Clave de COBIT 5
Fuente: ISACA. (2012). Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa - COBIT 5.

Para el presente trabajo se tomará el dominio de Alinear, Planificar y Organizar, según ISACA (2012) éste se encuentra compuesto por los siguientes procesos:

- APO01: Gestionar el marco de gestión de tecnologías de información.
- APO02: Gestionar la estrategia.
- APO03: Gestionar la arquitectura empresarial.
- APO04: Gestionar la innovación.
- APO05: Gestionar portafolio.

- APO06: Gestionar el presupuesto y los costos.
- 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.

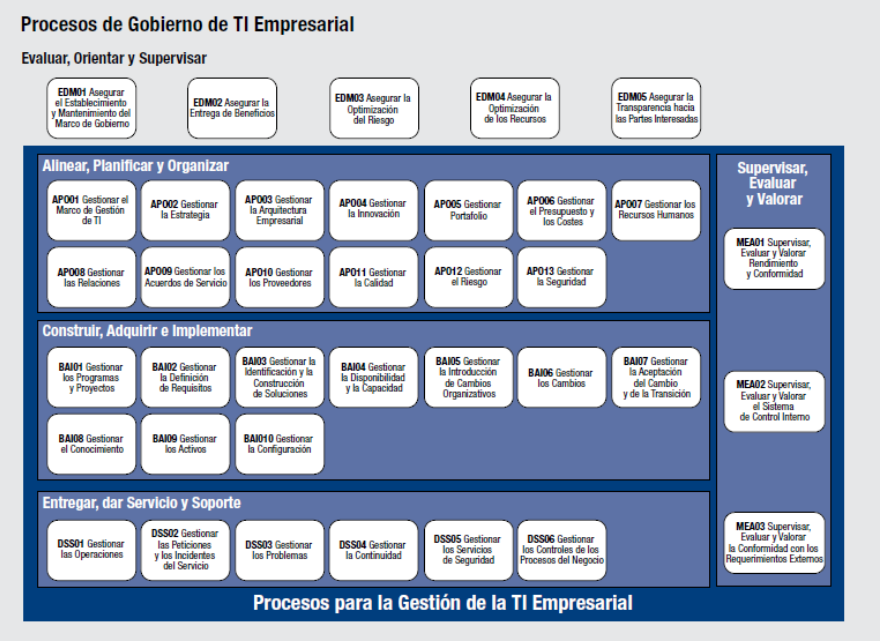


Figura 4. Modelo de Referencia de Procesos de COBIT 5
Fuente: ISACA. (2012). Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa - COBIT 5.

2.2.2. Seguridad de la Información (NTP-ISO 27001)

Delgado (s.f.) define a la seguridad de la información como el conjunto de medidas preventivas y reactivas de las organizaciones que permiten resguardar y proteger la información buscando mantener la:

- Confidencialidad

"Propiedad de la información para ser accesible únicamente por los individuos, entidades o procesos que poseen los privilegios y la autorización" (Mendoza, 2015, p. 5).

- Disponibilidad

  "Propiedad de la información para ser accesible y utilizable cuando una entidad lo requiera" (Mendoza, 2015, p. 5).

- Integridad

  "Propiedad de la información para mantener su exactitud y completitud" (Mendoza, 2015, p. 5).

Mendoza (2015) explica que un activo es cualquier cosa que tiene valor para la organización, existen varios tipos de activos como la información, software, infraestructura tecnológica, servicios, las personas junto con sus conocimientos, habilidades y experiencia o intangibles como la reputación o imagen de la empresa.

Según Delgado (s.f.) los tipos de activos de la información, son los siguientes:

- Servicios.
- Datos/información.
- Aplicaciones (Software).
- Equipo informático (Hardware).
- Personal.
- Redes de comunicación.
- Soporte de información.
- Equipamiento auxiliar.
- Instalaciones.
- Intangibles.

La norma técnica peruana NTP-ISO/IEC 27001:2014 según INDECOPI (2014), ha sido preparada para proporcionar los requisitos para establecer,

implementar, mantener y mejorar continuamente los procesos de tecnologías de información de la organización.

INDECOPI (2014) también define que la NTP-ISO/IEC 27001:2014 aplica una estructura de alto nivel, lo cual permite la compatibilidad con otras normas de sistemas de gestión como COBIT.

Horna (2016) enfatiza que la norma NTP-ISO/IEC 27001:2014 aborda los siguientes controles para la gestión de la organización:

- Políticas de seguridad de la información.
- Organización de la seguridad de la información
- Seguridad de los recursos humanos.
- Gestión de activos.
- Control de acceso.
- Criptografía.
- Seguridad física y ambiental.
- Seguridad de las operaciones.
- Seguridad de las comunicaciones.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Relaciones con los proveedores.
- Gestión de incidentes de seguridad de la información.
- Aspectos de los sistemas de información en la gestión de continuidad del negocio.
- Cumplimiento.

Horna (2016), también afirma que la norma NTP-ISO/IEC 27001:2014 puede dar los siguientes beneficios en su aplicación a las entidades públicas:

- Ayuda en el cumplimiento normativo y legal.
- Incrementa la confianza de los ciudadanos en la institución.
- Permite un apropiado flujo de información necesaria para la toma de decisiones tanto de forma local como sectorial.

- Permite abordar un enfoque integrado entre seguridad de la información y protección de datos personales (Ley 29733).
- Permite fortalecer y asegurar mecanismos apropiados de transparencia y gobierno abierto, etc.

CAPÍTULO III:

MEJORA DE PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN

3.1. DESCRIPCIÓN DE LA ORGANIZACIÓN

La Autoridad Autónoma de Majes es el organismo del Gobierno Regional de Arequipa encargado de la gestión del Proyecto Especial Majes-Siguas, cuyo objetivo es el de garantizar la disponibilidad del recurso hídrico a la población y a las actividades económicas que se desarrollen en la región.

El Proyecto Especial Majes-Siguas se inició el 03 de octubre de 1971 como un "Proyecto Regional Integral de Desarrollo Agrícola y Energético", constituyéndose como la única alternativa viable para reducir los niveles de pobreza, incrementar la producción de alimentos, generar divisas y lograr desarrollo agroindustrial sostenido. Éste proyecto ocupa un territorio de 471,576 hectáreas, de propiedad de la Autoridad Autónoma de Majes, involucrando a las provincias de Arequipa, Castilla, Camaná y Caylloma.

3.2. MISIÓN Y VISIÓN DE LA ORGANIZACIÓN

3.2.1. Misión

Somos el organismo del Gobierno Regional de Arequipa que gestiona el Proyecto Especial Majes – Siguas, garantizando la disponibilidad de los recursos hídricos a la población y a las actividades económicas, promoviendo una cultura de uso racional del agua, la reconversión productiva hacia la agro exportación, la inversión privada y la colaboración empresarial para el desarrollo de la región.

3.2.2. Visión

Acreditarse como Institución eficiente y líder en ejecución y gestión de proyectos hidráulicos y energéticos, brindando seguridad hídrica para el desarrollo humano sostenible de la región.

3.2.3. Funciones Generales

Las funciones de la Autoridad Autónoma de Majes son las siguientes:

- Gestionar el Proyecto Especial Majes – Siguas.
- Garantizar la disponibilidad del recurso hídrico a la población y actividades económicas.
- Promover una cultura del uso racional del agua.
- Promover la reconversión productiva hacia la agro exportación.
- Promover la inversión privada nacional e internacional y a la colaboración empresarial.
- Gestionar concertadamente el Plan de Ordenamiento Territorial.
- Promover y propiciar el manejo racional e integral de los recursos hídricos de las cuencas de su ámbito, en armonía con la preservación y conservación del ambiente.
- Garantizar la operación y mantenimiento de la infraestructura mayor del sistema y la seguridad de la infraestructura hidráulica.

3.3. ESTADO ACTUAL DE LA ORGANIZACIÓN (AS – IS)

3.3.1. Organigrama de la Organización

La estructura orgánica de la Autoridad Autónoma de Majes según la Ordenanza Regional N°270 – Arequipa (2014) es la siguiente:

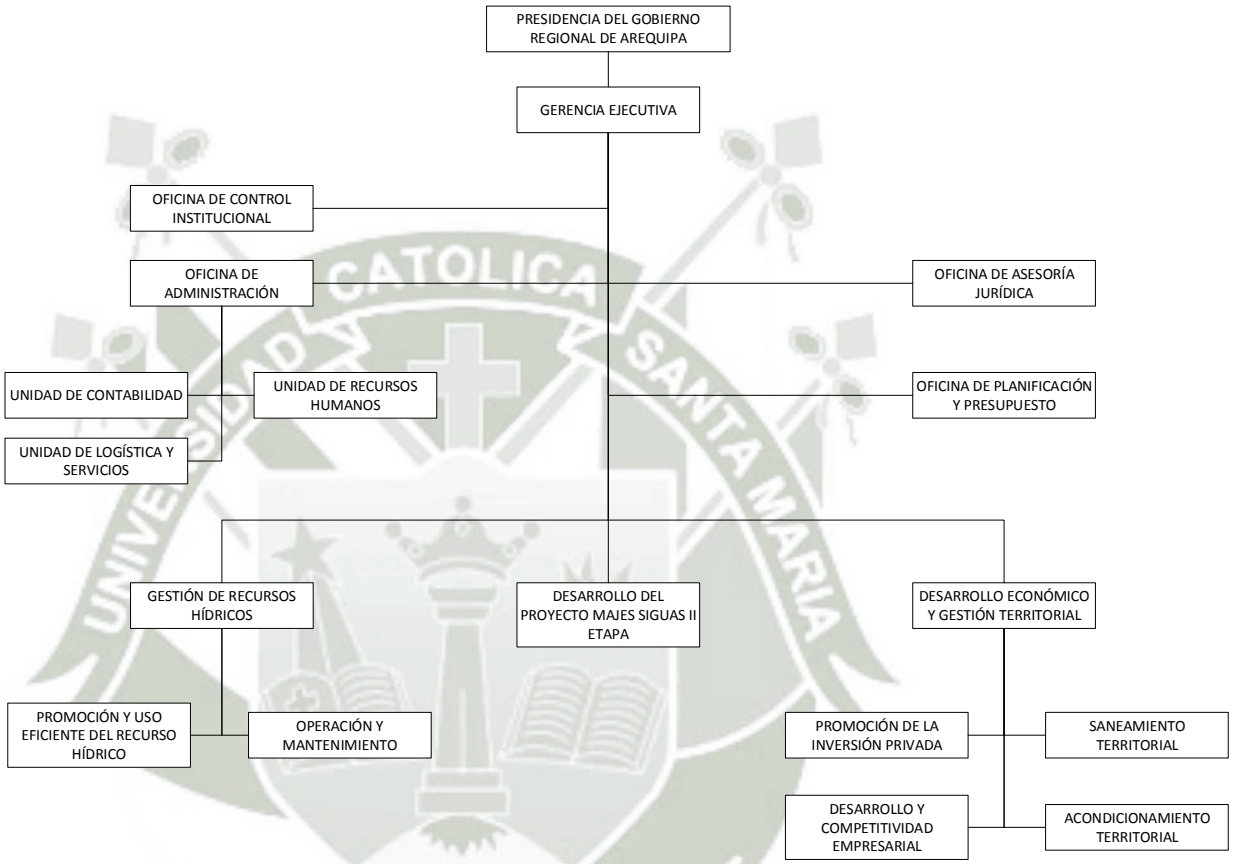


Figura 5. Estructura Orgánica de la Autoridad Autónoma de Majes
Fuente: Elaboración Propia

3.3.2. Cuadro Orgánico de la Oficina de Administración

Según la Resolución Gerencial Ejecutiva N°386-2015-GRA/PEMS-GE, los cargos de la Oficina de Administración de la Autoridad Autónoma de Majes es la siguiente:

Tabla 2. Cuadro Orgánico de Cargos de la Oficina de Administración de la AUTODEMA

N° Orden	**Unidades orgánicas y cargos estructurales**	**Nivel**	**Observaciones**
1	Gerencia Ejecutiva		
	Gerente Ejecutivo del PEMS – AUTODEMA	D-3	Cargo de confianza
2	Órgano de Control		
	Órgano de Control Institucional		
	Jefe de Control Institucional	D-2	Cargo de confianza
3	Órgano de Asesoramiento		
	Oficina de Asesoría Jurídica		
	Jefe de Oficina de Asesoría Jurídica	D-2	Cargo de confianza
	Oficina de Planificación		
	Jefe de Oficina de Planificación y Presupuesto	D-2	Cargo de confianza
4	Órgano de Apoyo		
	Oficina de Administración		
	Jefe de Oficina de Administración	D-2	Cargo de confianza
	Jefe de Unidad de Logística y Servicios	D-1	Cargo de confianza
	Jefe de Unidad de Contabilidad	D-1	Cargo de confianza
	Jefe de Unidad de Recursos Humanos	D-1	Cargo de confianza
4	Órgano de Línea		
	Gerencia de Gestión de Recursos Hídricos		

	Gerente de Gestión de Recursos Hídricos	D-2	Cargo de confianza
	Sub Gerente de Operación y Mantenimiento	D-1	Cargo de confianza
	Sub Gerente de Promoción y Uso Eficiente del Recurso Hídrico	D-1	Cargo de confianza
	Gerencia de Desarrollo del Proyecto Majes – Siguas II Etapa		
	Gerente de Desarrollo del Proyecto Majes Siguas II Etapa	D-2	Cargo de confianza
	Gerencia de Desarrollo Económico y Gestión Territorial		
	Gerente de Desarrollo Económico y Gestión Territorial	D-2	Cargo de confianza
	Sub Gerente de Desarrollo y Competitividad Empresarial	D-1	Cargo de confianza
	Sub Gerente de Promoción de la Inversión Privada	D-1	Cargo de confianza
	Sub Gerente de Saneamiento Territorial	D-1	Cargo de confianza
	Sub Gerente de Acondicionamiento Territorial	D-1	Cargo de confianza

Fuente: Elaboración propia

3.3.3. Clasificación de Puestos

Según el Manual Normativo de Clasificación de Cargos de la Administración Pública (1995) la clasificación de puestos en la Autoridad Autónoma de Majes, es la siguiente:

Directivo

Tabla 3. Clasificador de Puesto Directivo

Clasificación	Directivo
Codificación	D
Formación	Estudios profesionales de educación superior
Experiencia	Orientada al cargo
Habilidades especiales	Habilidad de liderazgo y/o vocación por la asesoría técnico-científica, talento individual

Fuente: Elaboración propia

Profesional

Tabla 4. Clasificador de Puesto Profesional

Clasificación	Profesional
Codificación	P
Formación	Estudios profesionales de educación superior o Estudios técnicos de 6 o más semestres
Experiencia	Orientada al cargo
Habilidades especiales	Habilidad por la asesoría técnico-científica, capacidad creativa

Fuente: Elaboración propia

Técnico

Tabla 5. Clasificador de Puesto Técnico

Clasificación	Técnico
Codificación	T
Formación	Estudios acorde al cargo
Experiencia	Orientada al cargo
Habilidades especiales	Trabajo en equipo, criterio y capacidad analítica para la aplicación de instrucciones y normas

Fuente: Elaboración propia

Auxiliar

Tabla 6. Clasificador de Puesto Auxiliar

Clasificación	Auxiliar
Codificación	A
Formación	Secundaria completa
Experiencia	Desempeño en trabajos similares
Habilidades especiales	Interpretación y aplicación de instrucciones y normas

Fuente: Elaboración propia

3.3.4. Denominación de Puesto

Responsable de Servicios Informáticos

El Responsable de Servicios Informáticos debe realizar la correcta administración, monitoreo, soporte y mantenimiento de los sistemas de información de la organización.

Los requisitos para la designación al puesto son:

Tabla 7. Requisitos de Puesto Responsable de Servicios Informáticos

Nombre del puesto	Responsable de Servicios Informáticos
Formación	Título Profesional de Ingeniero de Sistemas
Experiencia	3 años
Especialidad	Gestión de Redes, Sistemas Integrados y *Datawarehouse*.

Fuente: Elaboración propia

3.3.5. Procesos de Servicios Informáticos

Los procesos de Servicios Informáticos en la Autoridad Autónoma de Majes se encuentran detallados en el Manual Optimizado de Procedimientos de AUTODEMA (2009), dentro de la Unidad de Logística, siendo los siguientes:

Tabla 8. Procesos de Servicios Informáticos

Proceso	**Código**
Copias de seguridad - backup	LM-013

Soporte informático	LM-014
Seguridad, accesibilidad a usuarios, reporte mensual	LM-015
Administrador de sistemas S.I.G.A. y S.I.A.F.	LM-016
Supervisión de servicios de sistemas tercerizado	LM-017
Supervisión de cumplimiento de directiva de seguridad informática	LM-018

Fuente: Elaboración propia

– **Copias de Seguridad – *Backup*.**

AUTODEMA Manejo Sostenible	**PEMS – Oficina de Administración**	Código Proceso	**LM-013**
		Responsable Sección	**Informática**
	UNIDAD Logística	Revisado	**Jefe Unidad Logística**
		Aprobado	**Administrador**
	SECCION Informática	Fecha	**28-08-2009**
		Pagina	**1 de 1**
Alcance	* Todos los usuarios del PEMS		**Tiempo Aproximado 5 horas**
Responsabilidad	* Gerencias / Oficinas * Jefe de Unidad / Sub Gerencia * Jefe de Sección		

Área Responsabilidad	Actividades del Procedimiento	Cargo del Responsable	Días Horas
Sección Informática	**1. GENERAR COPIA DE SEGURIDAD DIARIA** a) Entrar a los sistemas informáticos S.I.G.A. y S.I.A.F. y sistemas específicos de los usuarios. b) Generar copia de seguridad de todos los sistemas informáticos c) Guardar copia de seguridad codificando nombre del sistema y fecha.	Responsable Informática	1 hora
	2. GENERAR COPIA DE SEGURIDAD SEMANAL a) Realizar último día hábil de la semana copia de seguridad b) Recopilar información de sistemas informáticos de la semana c) Guardar copia de seguridad codificada de cada sistema de la semana d) Grabar DVD copia de seguridad de cada sistema de la semana e) Etiquetar DVD consignando la fecha del periodo correspondiente a cada sistema, almacenar DVD en archivo de oficina informática f) Custodiar Información de los sistemas informáticos en caja fuerte.	Responsable Informática	1 hora
	3. GENERAR COPIA DE SEGURIDAD MENSUAL a) Realizar último día hábil del mes copia de seguridad b) Conectar servidor revisar sistemas informáticos del PEMS c) Realizar copia código fuente de sistemas informáticos de todos los usuarios PEMS d) Guardar copia de seguridad -código fuente e) Etiquetar e indicar fecha de copia de seguridad, grabar DVD copia de seguridad código fuente y consignar fecha del periodo correspondiente f) Almacenar DVD en archivo de oficina informática. g) Custodiar información de copia de seguridad código fuente en caja fuerte.	Responsable Informática	1 hora
Usuarios PEMS	**4. GENERAR SOLICITUD DIRIGIDA A OFICINA DE ADMINISTRACION INDICANDO COPIA DE BASE DATOS**	Usuario PEMS	30´
Oficina de Administración	**5. RECEPCIONAR VISAR Y DERIVAR A UNIDAD DE LOGISTICA**	Secretaria Administrador	30´
Unidad de Logística	**6. RECEPCIONAR VISAR Y DERIVAR A SECCION INFORMATICA**	Secretaria Jefe de Logística	30´
Sección Informática	**7. BRINDAR SOPORTE NECESARIO PARA ACCEDER A BASE DE DATOS SOLICITADA POR USUARIO PEMS**	Responsable Informática	30´

Figura 6. Detalle del Proceso Copias de Seguridad - Backup
Fuente: Manual Optimizado de Procedimientos de AUTODEMA. (2009). *Autoridad Autónoma de Majes Proyecto Especial Majes Siguas*

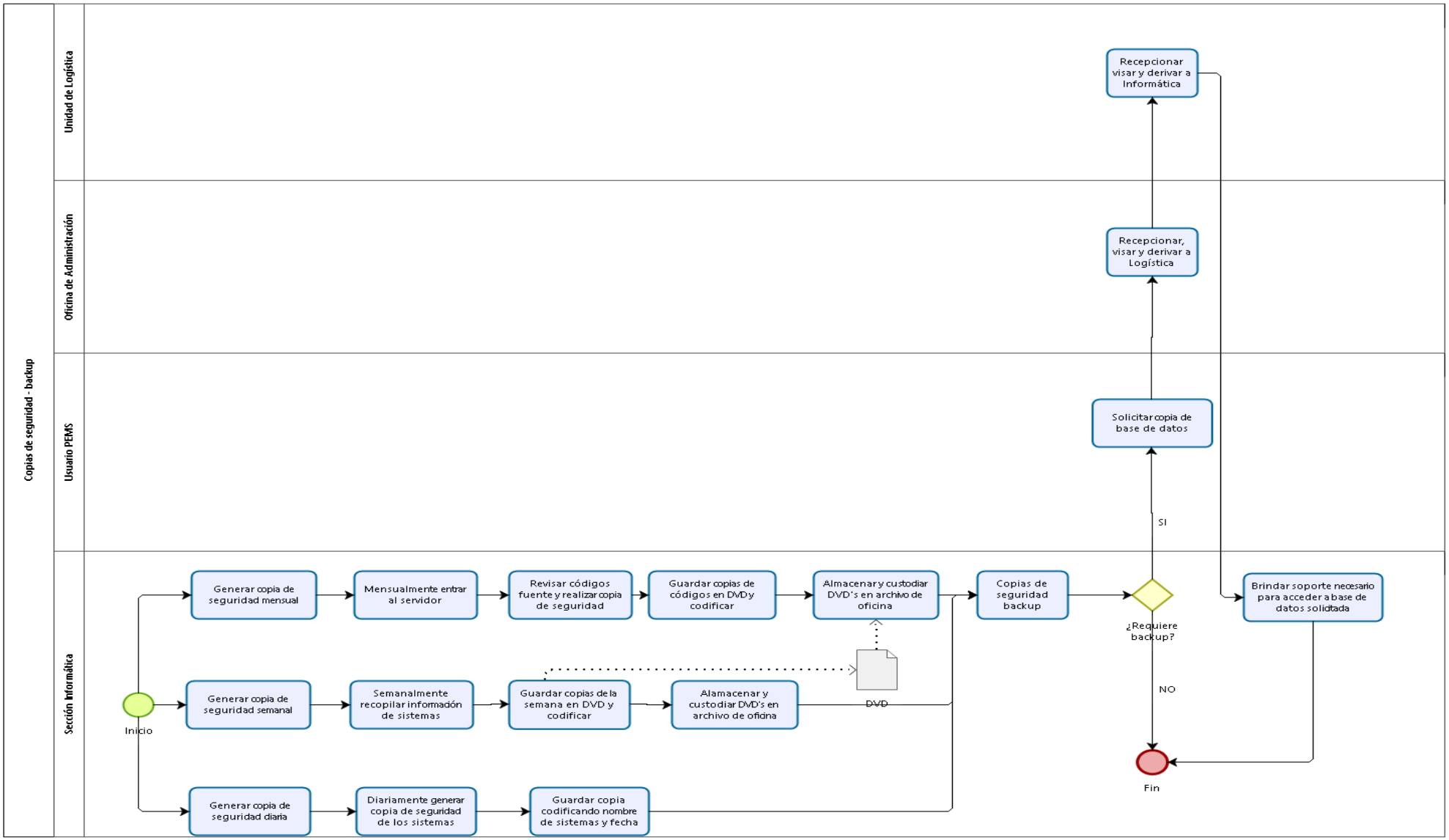


Figura 7. Diagrama de Procesos de Copias de Seguridad - Backup

Fuente: Elaboración propia

– Soporte Informático.

AUTODEMA Manejo Sostenible	**PEMS – Oficina de Administración**	Código Proceso	**LM-014**
		Responsable Sección	**Informática**
	UNIDAD Logística	Revisado	**Jefe Unidad Logística**
		Aprobado	**Administrador**
	SECCION Informática	Fecha	**28-08-2009**
		Pagina	**1 de 1**
Alcance	* Todos los usuarios del PEMS		**Tiempo Aproximado 4 horaas**
Responsabilidad	* Gerencias / Oficinas * Jefe de Unidad / Sub Gerencia * Jefe de Sección		

Área Responsabilidad	Actividades del Procedimiento	Cargo del Responsable	Días Horas
Usuario PEMS	**1. COMUNICAR NECESIDAD DE SOPORTE INFORMÁTICO - MANTENIMIENTO EN FORMA VERBAL, ESCRITA O TELÉFONO** a) Especificar naturaleza del requerimiento informático - mantenimiento b) Especificar urgencia del requerimiento	Usuario PEMS	15´
Sección Informática	**2. BRINDAR SOPORTE INFORMÁTICO** a) Analizar naturaleza del requerimiento mantenimiento, modificación, implementación de aplicativos en sistemas informáticos b) Priorizar requerimiento según nivel de importancia alto, medio bajo determinando la prioridad c) Realizar requerimiento solicitado de acuerdo a la orden de llegada a excepción los de alta importancia que serán atendidos prioritariamente. d) Generar ficha de soporte informático - mantenimiento de usuario, consignar el servicio realizado, Unidad/Subgerencia, Usuario, Hora de inicio, Hora de termino, V°B° de jefe inmediato de usuario, sistemas y satisfacción del usuario por servicio e) Elaborar informe técnico a jefe inmediato de usuario, detallando la necesidad de comprar un repuesto, o contratar un servicio especializado para el mantenimiento de equipo. f) Enviar informe técnico a jefe inmediato del usuario	Responsable Informática	2 hora
Usuario PEMS	**3. RECEPCIONAR INFORME TECNICO Y GENERAR PEDIDO DE COMPRA O SERVICIO INDICADO LA ENTREGA A RESPONSABLE DE SECCIÓN INFORMATICA** a) Indicar en el pedido que se debe entregar al encargado de soporte técnico b) Enviar requerimiento a unidad de logística adjunto a informe	Usuario PEMS	1 hora
Unidad de Logística	**4. RECEPCIONAR VISAR Y ENVIAR A SECCIÓN COMPRAS O SERVICIO**	Secretaria Jefe de Logística	30´
Sección Compras / Servicio	**5. RECEPCIONAR REQUERIMIENTO SOLICITANDO COMPRA O SERVICIO** a) Generar orden de compra o servicio b) Va procedimiento de servicios **(LM-023 o LM-024)**	Responsable de Compras/Servicios	15´

Figura 8. Detalle del Proceso Soporte Informático
Fuente: Manual Optimizado de Procedimientos de AUTODEMA. (2009). *Autoridad Autónoma de Majes Proyecto Especial Majes Siguas*

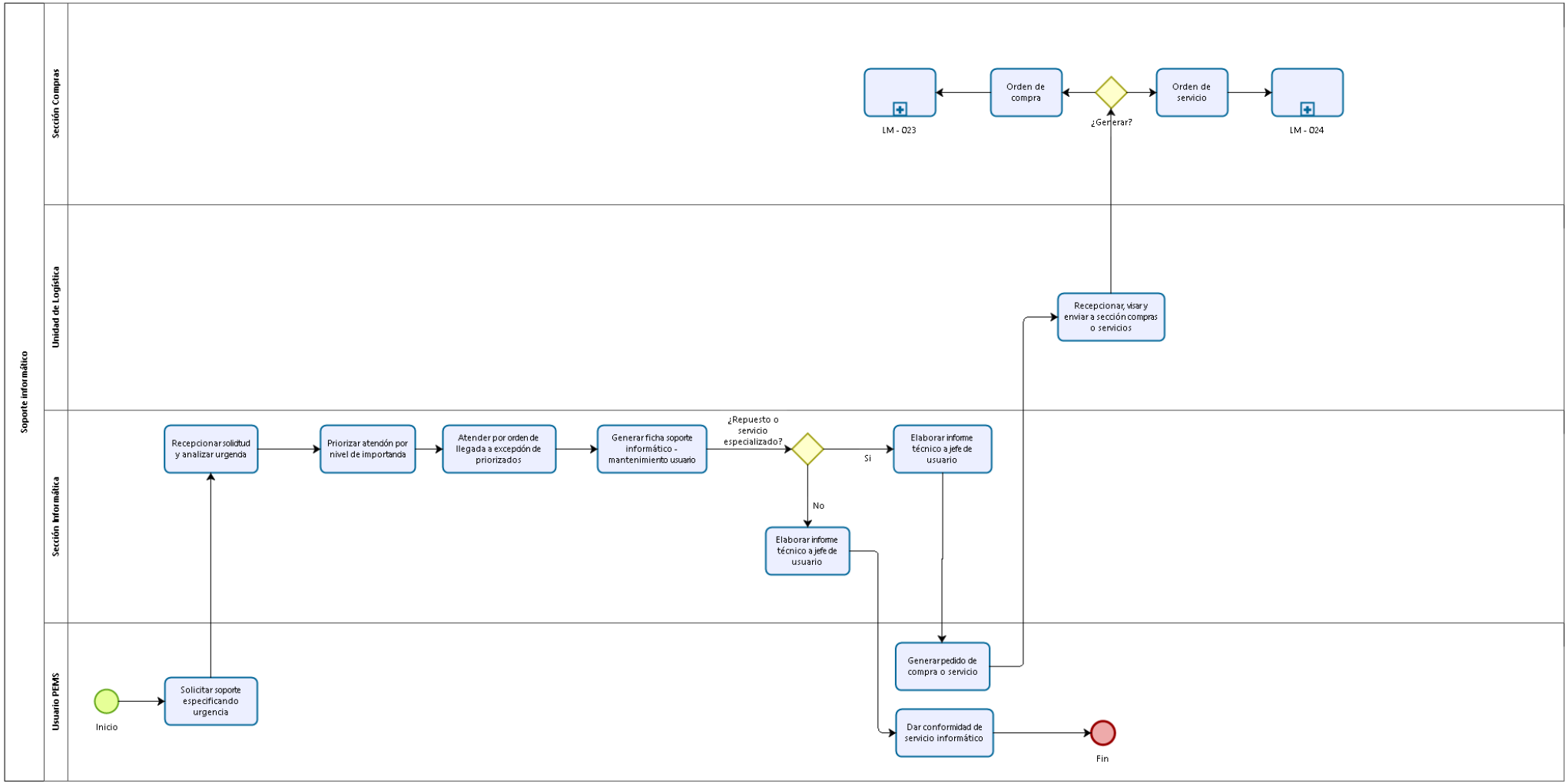


Figura 9. Diagrama de Procesos de Soporte Informático

Fuente:Elaboración propia

– Seguridad, Accesibilidad a Usuarios, Reporte Mensual.

AUTODEMA Manejo Sostenible	PEMS – Oficina de Administración	Código Proceso	LM-015
		Responsable Sección	Informática
	UNIDAD Logística	Revisado	Jefe Unidad Logística
		Aprobado	Administrador
	SECCION Informática	Fecha	28-08-2009
		Pagina	1 de 1
Alcance	* Todos los usuarios del PEMS		Tiempo Aproximado 1 dia
Responsabilidad	* Gerencias / Oficinas * Jefe de Unidad / Sub Gerencia * Jefe de Sección		

Área Responsabilidad	Actividades del Procedimiento	Cargo del Responsable	Días Horas
Sección Informática	**1. DESARROLLAR ACTIVIDADES INFORMÁTICAS**	Responsable Informática	4 hora
Sección Informática	**2. ADMINISTRAR SEGURIDAD INFORMÁTICA** a) Realizar último día hábil de cada semana verificación informática de: antivirus actualizados, histórico de accesibilidad de usuarios PEMS, modificaciones de aplicativos, acceso al servidor de usuarios PEMS b) Proporcionar niveles de seguridad a los usuarios PEMS; Administrador, Usuario tipo soporte, Usuario	Responsable Informática	4 hora
Sección Informática	**3. ADMINISTRAR ACCESO INFORMÁTICOS** a) Crear usuario para acceso informático, habilitar correo electrónico corporativo a usuarios, limitar acceso a internet o uso de acuerdo al requerimiento	Responsable Informática	30´
Sección Informática	**4. REALIZAR INFORME MENSUAL DE LAS ACTIVIDADES REALIZADAS EN EL MES** a) Identificar tareas desarrolladas tipificando la actividad b) Enviar informe a unidad logística	Responsable Informática	2 hora
Unidad Logística	**5. RECEPCIONAR INFORME**	Secretaria Jefe logística	15´

Figura 10. Detalle del Proceso Seguridad, Accesibilidad a Usuarios, Reporte Mensual
Fuente: Manual Optimizado de Procedimientos de AUTODEMA. (2009). *Autoridad Autónoma de Majes Proyecto Especial Majes Siguas*

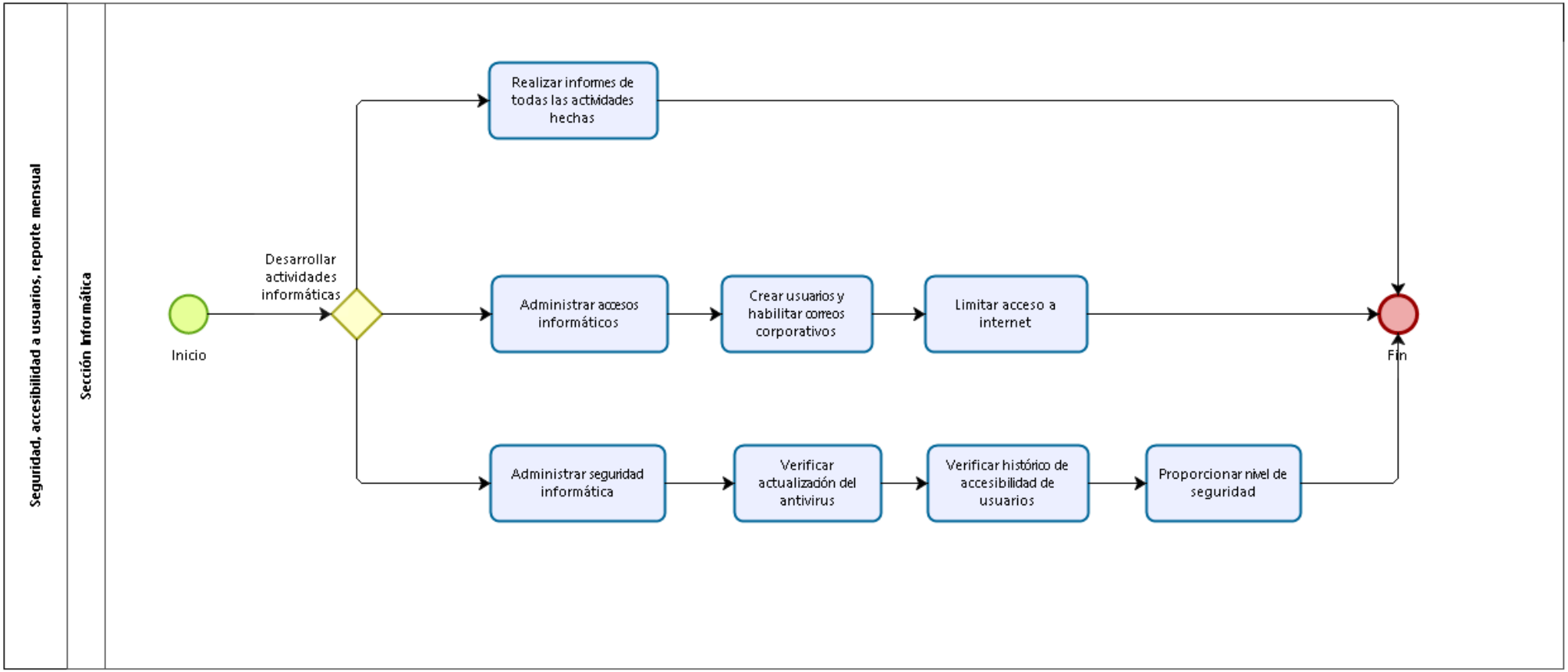


Figura 11. Diagrama de Procesos de Seguridad, Accesibilidad a Usuarios, Reporte Mensual

Fuente: Elaboración propia

– Administrador Sistemas S.I.G.A. y S.I.A.F.

AUTODEMA Manejo Sostenible	**PEMS – Oficina de Administración**	Código Proceso	**LM-016**
		Responsable Sección	**Informática**
	UNIDAD Logística	Revisado	**Jefe Unidad Logística**
		Aprobado	**Administrador**
	SECCION Informática	Fecha	**28-08-2009**
		Pagina	**1 de 1**
Alcance	* Todos los usuarios del PEMS		**Tiempo Aproximado 5 dias**
Responsabilidad	* Gerencias / Oficinas * Jefe de Unidad / Sub Gerencia * Jefe de Sección		

Área Responsabilidad	Actividades del Procedimiento	Cargo del Responsable	Días Horas
Sección Informática	**1. HABILITAR O DESHABILITAR USUARIOS EN EL SISTEMA S.I.G.A. Y/O S.I.A.F.** a) Verificar datos de usuarios: Apellidos y nombres, Código otorgado por RR.HH. Estado Civil, Hijos, Profesión, Colegiatura, Teléfono, E-mail, Denominación de Cargo, Dependencia a la que pertenece b) Habilitar acceso al sistema de acuerdo a la función que desempeñara el nuevo usuario y otorgar clave de acceso previa autorización de jefe inmediato	Responsable Informática	2 hora
Usuarios PEMS	**2. SOLICITAR A COOORDINADOR SIGA, CODIFICAR ITEM.**	Usuario PEMS	2 hora
Coordinador SIGA	**3. SOLICITAR A MEF CREAR CÓDIGO PARA ITEMS NUEVOS EN EL S.IG.A.** a) Enviar e-mail a catalogación del MEF lima solicitando creación ítems	Responsable Informática	30´
Agente Externo MEF	**4. RECEPCIONAR SOLICITUD VIA E-MAIL Y CREAR ITEMS NUEVOS EN S.I.G.A SEGÚN ORDEN DE LLEGADA** a) Enviar archivo Zip a sección informática	Responsable MEF LIMA	3,dias
Coordinador SIGA	5. **RECEPCIONAR E-MAIL CON ARCHIVO COMPRIMIDO ZIP Y HABILITAR ITEMS SOLICITADOS.** a) Ejecutar archivo en sistema S.I.G.A.	Responsable Informática	1 hora
Usuario PEMS	**6. SOLICITAR SERVICIO INFORMÁTICO DE ERRORES EN SISTEMA S.I.G.A. Y/O S.I.A.F.**	Usuario PEMS	30´
Sección Informática	**7. RECEPCIONAR SOLICITUD DE ERRORES INFORMÁTICO EN SISTEMAS S.I.G.A. Y/O S.I.A.F.** a) Recepcionar, analizar error de sistema y solucionar, en caso persiste error, derivar sectorista regional para que solucione error. Si persiste error, derivar a sectorista lima para que solucione error	Responsable Informática	2 hora
Sección Informática	**8. CAPACITAR NUEVOS USUARIOS SOBRE EL SISTEMA S.I.G.A. y/o S.I.A.F.** a) Realizar cronograma de capacitación sobre aplicativos de los sistemas SIGA o SIAF a los usuarios PEMS, dicha capacitación deberá coordinarse con el área de Recursos Humanos y deberá realizarse con los usuario nuevos **9. CAPACITACION EXTERNA DESARROLLADA CON COORDINADORA SIGA - MEF PRIMER TRIMESTRE DEL AÑO**	Responsable Informática	1,dia

Figura 12. Detalle del Proceso Administrador Sistemas S.I.G.A. y S.I.A.F.
Fuente: Manual Optimizado de Procedimientos de AUTODEMA. (2009). *Autoridad Autónoma de Majes Proyecto Especial Majes Siguas*

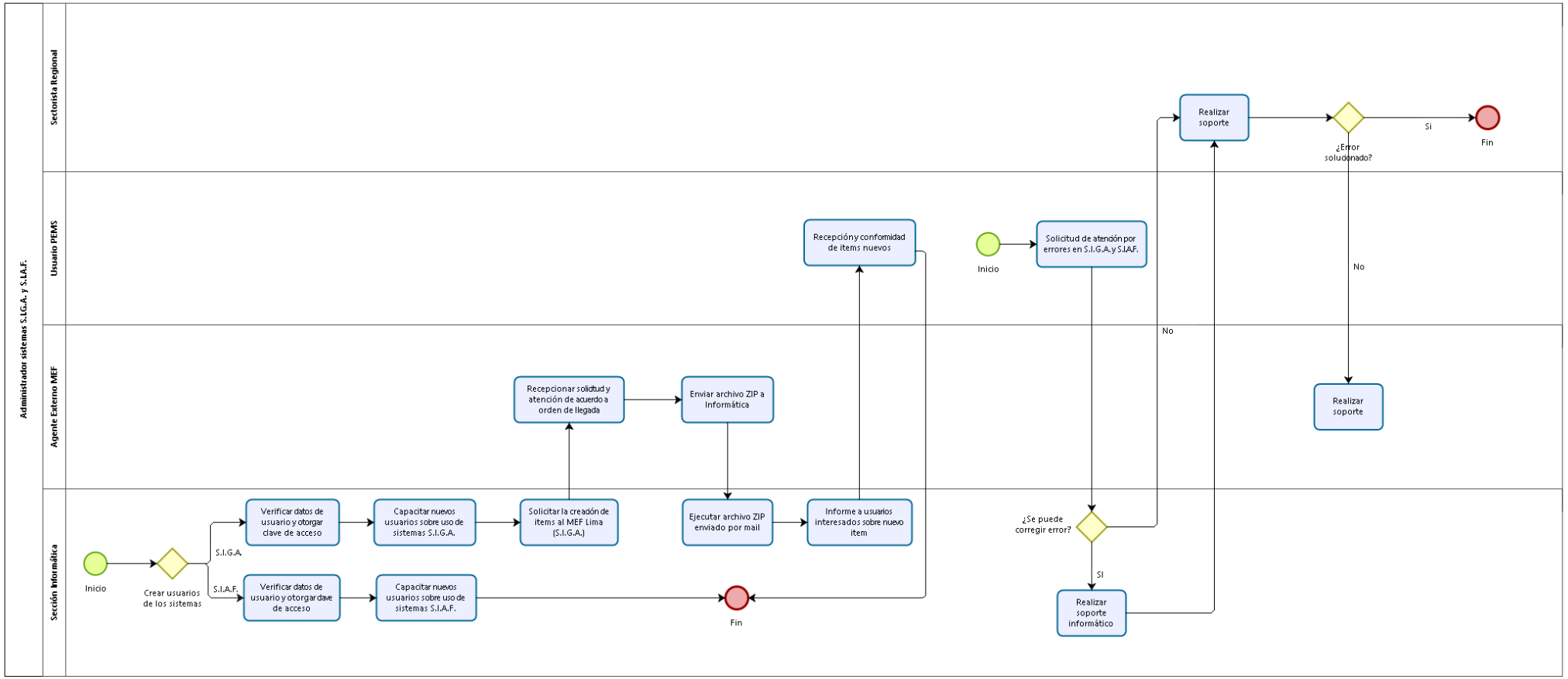


Figura 13. Diagrama de Procesos de Administrador Sistemas S.I.G.A. y S.I.A.F.

Fuente: Elaboración propia

– Servicios de Sistemas Tercerizado.

AUTODEMA Manejo Sostenible	PEMS – Oficina de Administración	Código Proceso	LM-017
		Responsable Sección	Informática
	UNIDAD Logística	Revisado	Jefe Unidad Logística
		Aprobado	Administrador
	SECCION Informática	Fecha	28-08-2009
		Pagina	1 de 1
Alcance	* Todos los usuarios del PEMS		Tiempo Aproximado 1 dia
Responsabilidad	* Gerencias / Oficinas * Jefe de Unidad / Sub Gerencia * Jefe de Sección		

Área Responsabilidad	Actividades del Procedimiento	Cargo del Responsable	Días Horas
Sección Informática	**1. SUPERVISAR SERVICIO DESARROLLADO POR TERCEROS** a) En coordinación con usuario PEMS proporcionar términos de referencia para el desarrollo de servicios de sistemas tercerizado b) Evaluar y analizar tipo de requerimiento diseño e implementación de bases de datos de sistemas desarrollados por provecedores externos c) Elaborar informe para hacer de conocimiento de oficina de administración para su aprobación d) Realizar requerimiento de servicio e) Va a procedimiento de servicios **LM 024** f) Controlar y monitorizar servicio e implantación del requerimiento g) Recibir capacitación del programador para reparar, adicionar, o extraer reportes informáticos h) Solicitar capacitación a agente externo	Responsable Informática Responsable Informática Responsable Informática	4 hora
Agente Externo	**2. BRINDAR CAPACITACION E INSTRUCCIÓN A USUARIOS**	Proveedor Externo	1 dia
Sección Informática	**3. EMITIR CONFORMIDAD DE SERVICIO Y ENVIAR CONFORMIDAD A USUARIO**	Responsable Informática	15´
Usuario PEMS	**4. RECEPCIONAR CONFORMIDAD VISAR Y ENVIAR A OFICINA DE ADMINISTRACIÓN**	Usuario PEMS	15´
Oficina de Administración	**5. RECEPCIONAR CONFORMIDAD VISAR Y ENVIAR A UNIDAD DE LOGÍSTICA**	Secretaria Administrador	30
Unidad de Logística	**6. RECEPCIONAR CONFORMIDAD Y DERIVAR A SECCIÓN SERVICIOS PARA CONTINUAR CON EL PROCEDIMIENTO DE PAGO A PROVEEDOR**	Secretaria Jefe de Logística	15´

Figura 14. Detalle del Proceso Servicios de Sistemas Tercerizado
Fuente: Manual Optimizado de Procedimientos de AUTODEMA. (2009). *Autoridad Autónoma de Majes Proyecto Especial Majes Siguas*

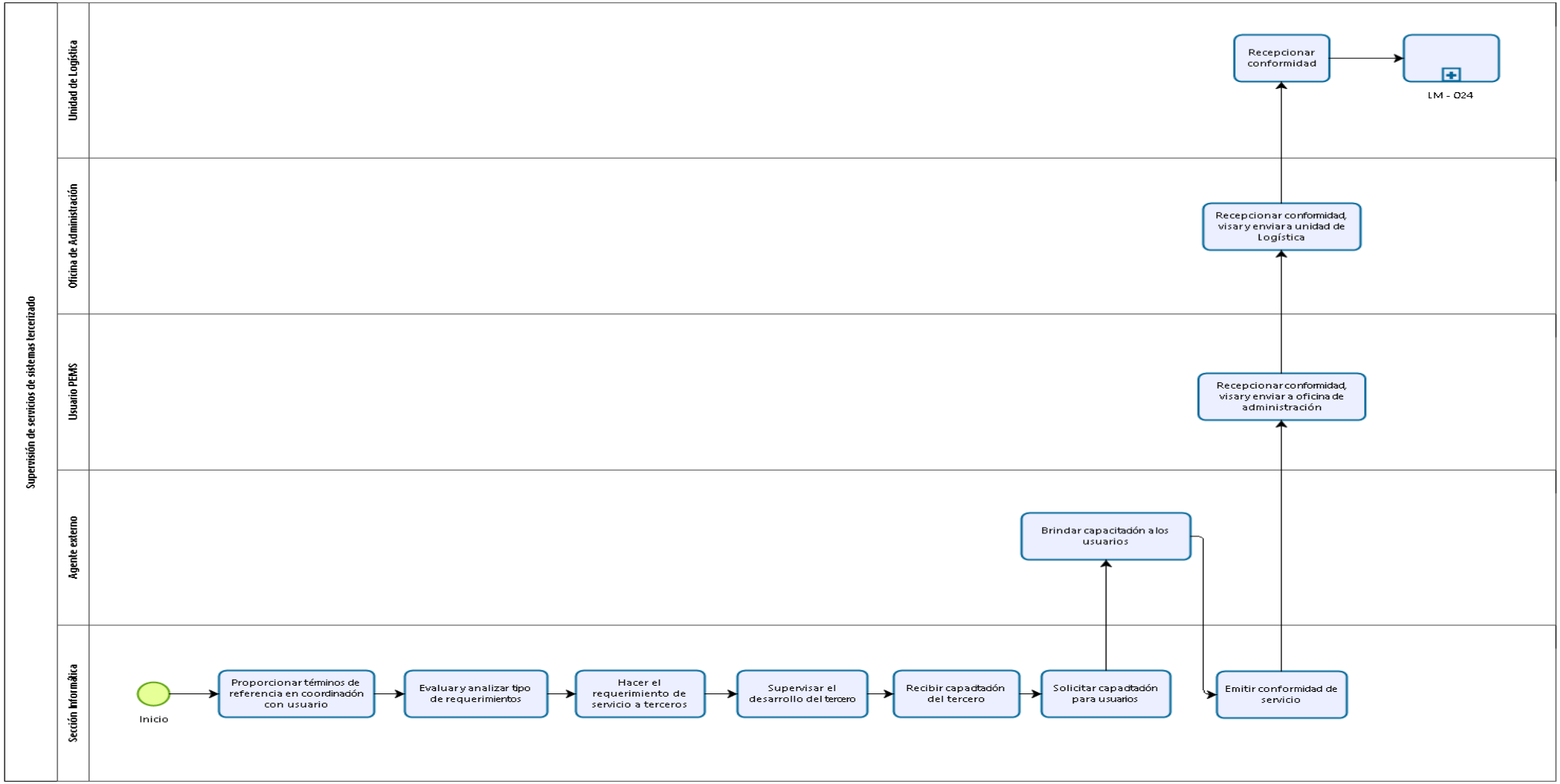


Figura 15. Diagrama de Procesos de Servicios de Sistemas Tercerizado

Fuente: Elaboración propia

– Supervisión de Cumplimiento de Directiva de Seguridad Informática

AUTODEMA Manejo Sostenible	**PEMS – Oficina de Administración**	Código Proceso	**LM-018**
		Responsable Sección	**Informática**
	UNIDAD Logística	Revisado	**Jefe Unidad Logística**
		Aprobado	**Administrador**
	SECCION Informática	Fecha	**28-08-2009**
		Pagina	**1 de 1**
Alcance	* Todos los usuarios del PEMS		**Tiempo Aproximado 6 horas**
Responsabilidad	* Gerencias / Oficinas * Jefe de Unidad / Sub Gerencia * Jefe de Sección		

Área Responsabilidad	Actividades del Procedimiento	Cargo del Responsable	Días Horas
Sección Informática	**1. ACTUALIZAR DIRECTIVA DE SEGURIDAD INFORMATICA CADA PRIMER TRIMESTRE DEL AÑO** a) Presentar actualización mediante informe a unidad de logística	Responsable Informatica	4 hora
Unidad Logística Oficina Administración	**2. RECEPCIONAR VISAR Y ENVIAR A OFICINA DE ADMINISTRACION**	Secretaria Jefe Logística	30´
	3. RECEPCIONAR VISAR Y DIFUNDIR DIRECTIVA DE SEGURIDAD INFORMATICA MEDIANTE RESOLUCION ADMINISTRATIVA	Secretaria Administrador	30´
Sección Informática	**4. SUPERVISAR CUMPLIMIENTO DE DIRECTIVA DE SEGURIDAD INFORMATICA**	Responsable de Informatica	1 hora

Figura 16. Detalle del Proceso Supervisión de Cumplimiento de Directiva de Seguridad Informática

Fuente: Manual Optimizado de Procedimientos de AUTODEMA. (2009). *Autoridad Autónoma de Majes Proyecto Especial Majes Siguas*

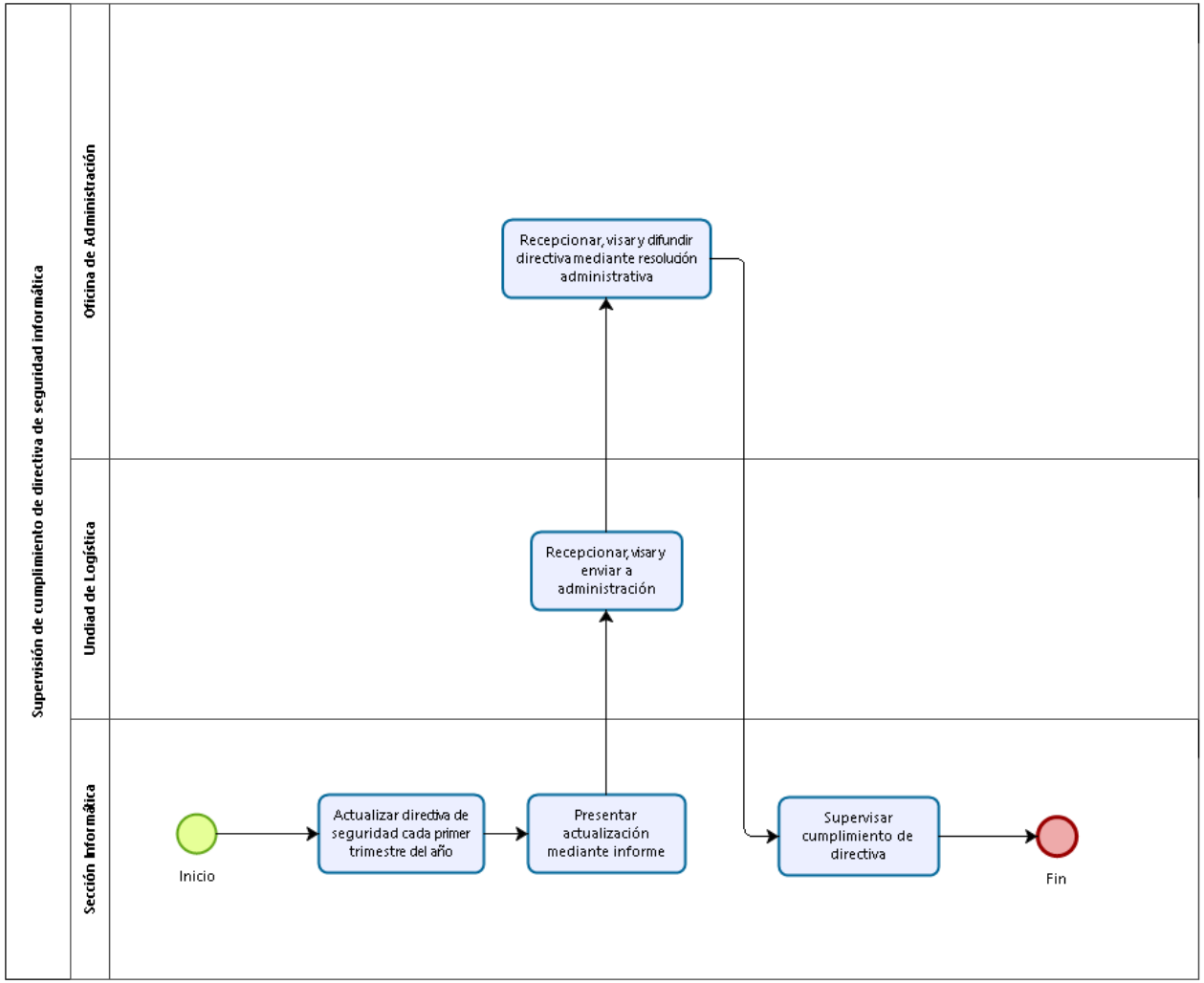


Figura 17. Diagrama de Procesos de Supervisión de Cumplimiento de Directiva de Seguridad Informática
Fuente: Elaboración propia

3.3.6. Cumplimiento de Procesos de COBIT 5 y Controles de la NTP-ISO 27001:2014

Para el cumplimiento de procesos de COBIT 5 y controles de la NTP-ISO 27001:2014 se utilizaron los procesos del dominio Alinear, Planificar y Organizar:

- APO 01 Gestionar el marco de gestión de TI.
- APO 02 Gestionar la estrategia.
- APO 04 Gestionar la innovación.
- APO 05 Gestionar el portafolio.
- APO 07 Gestionar los recursos humanos.
- APO 08 Gestionar las relaciones.
- APO 09 Gestionar los contratos de servicio.
- APO 10 Gestionar los proveedores.
- APO 12 Gestionar el riesgo.
- APO 13 Gestionar la seguridad.

Así como los requerimientos de la NTP-ISO 27001:2014:

- 4. Contexto de la organización.
  - 4.1 Entender la organización y su contexto.
  - 4.2 Comprender las necesidades y expectativas de las partes interesadas.
- 5. Liderazgo.
  - 5.1 Liderazgo y compromiso.
  - 5.3 Roles organizacionales, responsabilidades y autoridades.
- 6. Planificación.
  - 6.1 Acciones para dirigir los riesgos y oportunidades.
  - 6.2 Objetivos de seguridad de la información y planes para alcanzarlos.
- 7. Soporte.
  - 7.2 Competencias.

- 7.4 Comunicaciones.
- 7.5 Documentar información.

- 8. Operación.
  - 8.3 Tratamiento de riesgos de seguridad de la información.
- 9. Evaluación del desempeño.
  - 9.1 Monitoreo, medición, análisis y evaluación.
  - 9.2 Auditoría interna.
  - 9.3 Revisión de la gestión.
- 10. Mejora.
  - 10.2 Mejora continua.
- 15. Relaciones con proveedores.
  - 15.2 Gestión de cambios de los servicios del proveedor.

La cobertura de cada uno de los procesos de tecnologías de información según la NTP-ISO 27001:2014 está definida a partir de siguiente tabla:

Tabla 9. Cobertura de Procesos Según la NTP-ISO 27001-2014

Cobertura	**Descripción**
A	El requerimiento cubre completamente al proceso.
B	El requerimiento cubre medianamente el proceso.
C	El requerimiento cubre insuficientemente al proceso.

Fuente: Elaboración propia

- **APO 01 Gestionar el Marco de Gestión de TI.**

CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014												
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**							
APO 01	***Gestionar el marco de gestión de TI***	***Requerimientos***	***Cobertura***	***Justificación***	***LM-013***	***LM-014***	***LM-015***	***LM-016***	***LM-017***	***LM-018***	***Documentación***
APO 01.02	Establecer roles y responsabilidades	5.3 Roles organizacionales, responsabilidades y autoridades	C	Los roles y responsabilidades deben estar correctamente definidos				X			No presenta
APO 01.04	Comunicar objetivos y dirección de la administración	5.1 Liderazgo y compromiso	Inexistente	Se debe comunicar la importancia de la administración de la seguridad de la información							No presenta
		6.2 Objetivos de seguridad de la información y planes para alcanzarlos	C	Se indica que los objetivos deben ser comunicados						X	Directiva de seguridad
		7.4 Comunicaciones	Inexistente	Se determinan los protocolos de comunicación y lo que debe ser comunicado							No presenta
APO 01.06	Definir información(datos) y propietarios del sistema	7.5 Documentar información	C	Se debe tener registro de la información y los dueños de la misma	X						Copia de seguridad(DVD)
APO 01.07	Administrar la mejora continua de procesos	10.2 Mejora continua	Inexistente	El ciclo de calidad implica una mejora continua en el proceso							No presenta
APO 01.08	Mantener la conformidad con políticas y procedimientos	5 Liderazgo	Inexistente	Se debe mantener la conformidad de las políticas y procedimientos como fueron definidos							No presenta

Figura 18. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 01

Fuente: Elaboración propia

– **APO 02 Gestionar la Estrategia.**

CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014												
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**							
APO 02	***Gestionar la estrategia***	***Requerimientos***	***Cobertura***	***Justificación***	***LM-013***	***LM-014***	***LM-015***	***LM-016***	***LM-017***	***LM-018***	***Documentación***
APO 02.01	Entender la dirección de la empresa	4.2 Comprender las necesidades y expectativas de las partes interesadas	C	La norma técnica indica que se tiene que comprender las necesidades de las partes interesadas y éstas deberán tener acceso a la información pertinente			X				No presenta
APO 02.02	Evaluar el entorno actual, las capacidades y el rendimiento	5.3 Roles organizacionales, responsabilidades y autoridades	Inexistente	La norma técnica indica que cada persona deberá tener la capacidad de asignar roles y responsabilidades de acuerdo a su capacidad							No presenta
APO 02.03	Definir las capacidades de TI y sus objetivos	6.1 Acciones para dirigir los riesgos y oportunidades	Inexistente	La norma técnica indica que se deben evaluar los riesgos y oportunidades para guiar el direccionamiento del negocio							No presenta
APO 02.06	Comunicar la estrategia y la dirección de TI	7.4 Comunicaciones	C	La norma técnica indica que se debe comunicar la entre todas las partes interesadas		X					Ficha soporte informático - mantenimiento usuario

Figura 19. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 02

Fuente: Elaboración propia

- **APO 04 Gestionar la Innovación.**

CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014												
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**						
APO 04	***Gestionar la innovación***	***Requerimientos***	***Cobertura***	***Justificación***	***LM-013***	***LM-014***	***LM-015***	***LM-016***	***LM-017***	***LM-018***	***Documentación***
APO 04.02	Mantener un entendimiento del ambiente de la empresa	4.2 Comprender las necesidades y expectativas de las partes interesadas	C	La norma técnica indica que se tiene que comprender las necesidades de las partes interesadas y éstas deberán tener acceso a la información pertinente, significando que debe entender el ambiente de la empresa.			X				No presenta
APO 04.03	Monitorear y observar el abiente tecnológico	9.1 Monitoreo, medición, análisis y evaluación	C	Según la norma técnica se debe monitorear los procesos de seguridad de la información y los controles que se realizan, se debe saber quien monitorea los servicios y saber los resultados de dicho monitoreo.						X	No presenta

Figura 20. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 04

Fuente: Elaboración propia

- **APO 05 Gestionar el Portafolio.**

AUTODEMA Autoridad Autónoma de Majes	CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014										
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**						
APO 05	***Gestionar el portafolio***	***Requerimientos***	***Cobertura***	***Justificación***	***LM-013***	***LM-014***	***LM-015***	***LM-016***	***LM-017***	***LM-018***	***Documentación***
APO 05.03	Evaluar y elegir programa a financiar	7.4 Comunicaciones	Inexistente	Refiere al manejo de la información en todos los procesos de una organización, así como los recursos a utilizarse en los mismos.							No presenta

Figura 21. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 05

Fuente: Elaboración propia

– **APO 07 Gestionar los Recursos Humanos.**

CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014												
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**							
APO 07	***Gestionar los recursos humanos***	***Requerimientos***	***Cobertura***	***Justificación***	***LM-013***	***LM-014***	***LM-015***	***LM-016***	***LM-017***	***LM-018***	***Documentación***
APO 07.01	Mantener una asignación de tareas adecuada y apropiada	7.2 Competencias	Inexistene	Aprovecha las habilidades del personal para su correcta asignación de tareas							No presenta
APO 07.03	Mantener las habilidades y competencias del personal	7.2 Competencias	Inexistene	Mantiene la capacidad de recursos humanos frente al negocio en el tiempo							No presenta
APO 07.04	Evaluar el desempeño laboral del personal	9.1 Monitoreo, medición, análisis y evaluación 9.2 Auditoría interna	C	Consideración de evaluación del desempeño del personal correspondiente		X					Informe de actividades realizadas
APO 07.06	Administrar personal de contrato	7.2 Competencias	Inexistene	Requerimiento de competencias de personal							No presenta

Figura 22. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 07

Fuente: Elaboración propia

- **APO 08 Gestionar las Relaciones.**

CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014												
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**							
APO 08	***Gestionar las relaciones***	***Requerimientos***	***Cobertura***	***Justificación***	***LM-013***	***LM-014***	***LM-015***	***LM-016***	***LM-017***	***LM-018***	***Documentación***
APO 08.01	Entender las expectativas del negocio	4.2 Comprender las necesidades y expectativas de las partes interesadas	C	La norma técnica indica que se deben comprender las necesidades de las partes interesadas			X				No presenta
APO 08.02	Identificar las oportunidades, riesgos y limitaciones de TI para mejorar el negocio	6.1 Acciones para dirigir los riesgos y oportunidades	C	La norma técnica indica que se deben planear y dirigir los riesgos y las oportunidades para guiar el direccionamiento del negocio						X	Informe
APO 08.04	Coordinar y comunicar	7.4 Comunicaciones	C	Se debe comunicar necesariamente los cambios realizados en la gestión de la información para mantener íntegra la seguridad		X					Informe técnico
APO 08.05	Aportar a la mejora continua de los servicios	10.2 Mejora continua	Inexistente	Realiza siempre mejoras en la gestión de sistemas de seguridad de la información y mantener los documentos ordenados y bien documentados al alcance de todas las partes interesadas							No presenta

Figura 23. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 08

Fuente: Elaboración propia

– **APO 09 Gestionar los Contratos de Servicio.**

CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014												
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**						
APO 09	***Gestionar los contratos de servicio***	***Requerimientos***	***Cobertura***	***Justificación***	***LM-013***	***LM-014***	***LM-015***	***LM-016***	***LM-017***	***LM-018***	***Documentación***
APO 09.01	Identidficar los servicios de TI	6.1 Acciones para dirigir los riesgos y oportunidades	Inexistente	Se debe analizar la demanda de los servicios de TI, identificando los riesgos y planeando los posibles efectos de los mismos							No presenta
APO 09.02	Catálogo de servicios permitidos por TI	7.5. Documentar información	Inexistente	Según la norma técnica se debe tener documentada la información de la que se dispone, estando adecuada y disponible, además de estar siempre protegida contra pérdida.							No presenta
APO 09.04	Monitorear y reportar los niveles de servicio	9.1 Monitoreo, medición, análisis y evaluación	Inexistente	Según la norma técnica se deben monitorear los procesos de seguridad de la información y los controles que se realizan, además de monitorear los servicios y sus resultados							No presenta

Figura 24. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 09

Fuente: Elaboración propia

- **APO 10 Gestionar los Proveedores.**

CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014												
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**							
APO 10	***Gestionar el marco de gestión de TI***	***Requerimientos***	***Cobertura***	***Justificación***	***LM-013***	***LM-014***	***LM-015***	***LM-016***	***LM-017***	***LM-018***	***Documentación***
APO 10.03	Gestionar las relaciones y contratos con el proveedor	15.2 Gestión de cambios de los servicios del proveedor	C	Se debe gestionar permanentemente la información del proveedor, manteniendo y mejorando la misma, cada vez que sea necesario		X					Pedido de compra o servicio
APO 10.05	Monitorear el desempeño y cumplimiento del proveedor	15.2 Gestión de cambios de los servicios del proveedor	C	Se debe monitorear y auditar regularmente los servicios brindados por el proveedor					X		Conformidad de servicio

Figura 25. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 10

Fuente: Elaboración propia

- **APO 12 Gestionar el Riesgo.**

CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014												
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**						
APO 12	***Gestionar el riesgo***	***Requerimientos***	***Cobertura***	***Justificación***	***LM-013***	***LM-014***	***LM-015***	***LM-016***	***LM-017***	***LM-018***	***Documentación***
APO 12.02	Analizar el riesgo	6.1 Acciones para dirigir los riesgos y oportunidades	C	Evaluación de los riesgos en un determinado intervalo para determinar como se ven afectados ante algún cambio u ocurrencia		X				X	Informe
APO 12.03	Mantener el portafolio de riesgo	9.3 Revisión de la gestión	Inexistente	Considera el resultado de la evaluación de riesgos y el estado del riesgo luego del plan de tratamiento							No presenta
APO 12.04	Articular el riesgo	9.3 Revisión de la gestión	C	Considera el resultado de la evaluación de riesgos y el estado del riesgo luego del plan de tratamiento	X					X	Copia de seguridad, Directiva de seguridad
APO 12.05	Definir un portafolio de gestión de riesgos	6.1 Acciones para dirigir los riesgos y oportunidades	Inexistente	Planifica acciones para abordar los riesgos y oportunidades y como integrarlos en los procesos de gestión de seguridad de la información							No presenta
APO 12.06	Respuesta al riesgo	8.3 Tratamiento de riesgos de seguridad de la información	C	Considera la implementación del plan de tratamiento de riesgos de seguridad de la información		X					No presenta

Figura 26. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 12

Fuente: Elaboración propia

- **APO 13 Gestionar la Seguridad.**

CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014												
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**						
APO 13	***Gestionar la seguridad***	***Requerimientos***	***Cobertura***	***Justificación***	***LM-013***	***LM-014***	***LM-015***	***LM-016***	***LM-017***	***LM-018***	***Documentación***
APO 13.02	Definir y administrar un plan de tratamiento de riesgos de seguridad de la información	6 Planificación	C	Como se van a manejar los riesgos en la empresa, proporcionando información para el correcto desarrollo de los mismos						X	Directiva de seguridad

Figura 27. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 13

Fuente: Elaboración propia

3.4. ESTADO DESEADO DE LA ORGANIZACIÓN (TO – BE)

3.4.1. Mapa de Procesos de la Organización

A partir del organigrama señalado en la Resolución Gerencial Ejecutiva N°386-2015-GRA/PEMS-GE, se propone la separación del Responsable de Servicios Informáticos a un área independiente de soporte, tal como explica Santana(2011), donde explica que el primer paso de una organización, es la creación de una Jefatura de Tecnologías de Información que reporte al área de Administración o al área de Operaciones, de ésta manera comenzando a tener participación operativa en la organización y con posterioridad, una participación más estratégica, a partir de la importancia que tendrá la información para la organización.

Santana (2011), también da una mirada al sector público, donde observa un retraso en el uso estratégico de las tecnologías de información, ya que no existe una visión estratégica en la tecnología, claros ejemplos en nuestro medio son SUNAT y Registros Públicos, donde éstas instituciones alcanzaron una mejora en sus procesos de negocio gracias a las tecnologías de información y son consideradas por la población como instituciones que realizan un buen trabajo.

Con el establecimiento del proceso de soporte de Gestión de Tecnologías de Información en la Autoridad Autónoma de Majes, el Jefe de Unidad tendrá la capacidad de participación en las juntas directivas y tener la capacidad de proponer soluciones tecnológicas que vayan de la mano a los requerimientos del negocio.

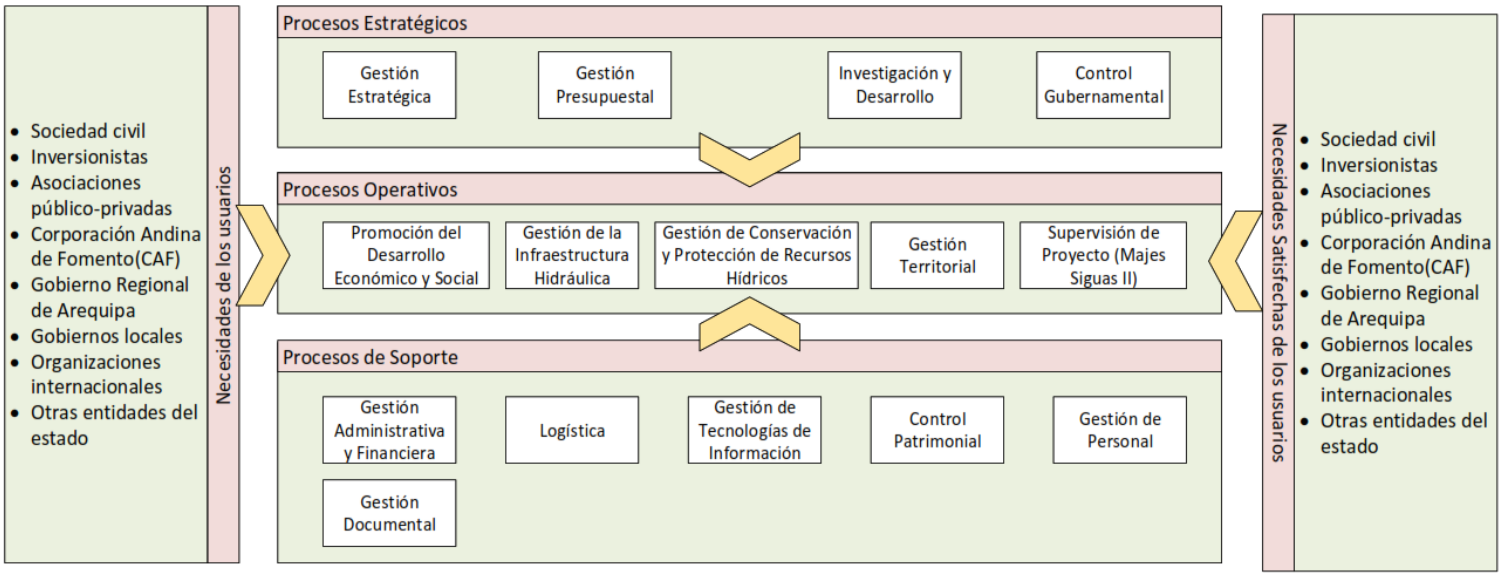


Figura 28. Mapa de Procesos de la Autoridad Autónoma de Majes Propuesto
Fuente: Elaboración propia

3.4.2. Denominación de Puestos

Jefe de Unidad de Tecnologías de Información

Es el encargado de la planificación, administración, evaluación y control de todos los procesos de tecnologías de información.

Los requisitos para la designación al puesto son:

Tabla 10. Requisitos de Puesto Jefe de Unidad de Tecnologías de Información

Nombre del puesto	Jefe de Unidad de Tecnologías de Información
Formación	Título Profesional de Ingeniero de Sistemas o Informática
Experiencia	5 años
Especialidad	Gestión de Redes, Sistemas Integrados y Datawarehouse.

Fuente: Elaboración propia

Encargado de Infraestructura de Tecnologías de Información

El Encargado de Infraestructura de Tecnologías de Información es aquel que gestiona y supervisa la arquitectura de red y las aplicaciones para asegurar el

desarrollo de los procesos de tecnologías de información de la Autoridad Autónoma de Majes.

Los requisitos para la designación al puesto son:

Tabla 11. Requisitos de Puesto Encargado de Infraestructura de Tecnologías de Información

Nombre del puesto	Encargado de Infraestructura de Tecnologías de Información
Formación	Bachiller en Ingeniería de Sistemas o Estudios Técnicos en Redes de Tecnologías de Información.
Experiencia	1 año
Especialidad	Redes, Cableado Estructurado, Sistemas Integrados de Gestión.

Fuente: Elaboración propia

Encargado de Seguridad de la Información

El Encargado de Seguridad de la Información es el responsable de la alineación de las políticas de seguridad de la Autoridad Autónoma de Majes a los procesos de tecnologías de información, garantizando la protección de los activos y de la información.

Los requisitos para la designación al puesto son:

Tabla 12. Requisitos de Puesto Encargado de Seguridad de la Información

Nombre del puesto	Encargado de Seguridad de la Información
Formación	Bachiller en Ingeniería de Sistemas o Estudios Técnicos en Administración de Sistemas.
Experiencia	2 años
Especialidad	Informática forense, *Ethical Hacking*, Seguridad de la Información, Sistemas Integrados de Gestión.

Fuente: Elaboración propia

Mesa de Servicio

La Mesa de Servicio planea, estructura y provee la entrega de servicios de soporte de tecnologías de información a los usuarios de la Autoridad Autónoma de Majes, posee más experiencia que la Mesa de Ayuda.

Los requisitos para la designación al puesto son:

Tabla 13. Requisitos de Puesto Mesa de Servicio

Nombre del puesto	Mesa de Servicio
Formación	Bachiller en Ingeniería de Sistemas o Estudios Técnicos en Tecnologías de Información
Experiencia	1 año
Especialidad	Redes, Cableado Estructurado, Reparación y Mantenimiento de Equipos de Cómputo.

Fuente: Elaboración propia

Mesa de Ayuda

La Mesa de Ayuda es la encargada de responder a los incidentes que se dan dentro de la infraestructura de tecnologías de información, con capacidad de respuesta rápida, es el primer punto de contacto entre la Unidad de Tecnologías de Información y el usuario de la Autoridad Autónoma de Majes.

Los requisitos para la designación al puesto son:

Tabla 14. Requisitos de Puesto Mesa de Ayuda

Nombre del puesto	Mesa de Ayuda
Formación	Estudios Técnicos en Reparación y Mantenimiento de Equipos de Cómputo
Experiencia	6 meses
Especialidad	Ninguno

Fuente: Elaboración propia

3.4.3. Procesos de Tecnologías de Información

Los procesos de tecnologías de información propuestos para la Autoridad Autónoma de Majes son los siguientes:

*Tabla 15.*Procesos de Tecnologías de Información Propuestos

Proceso	**Código**
Realizar copias de seguridad – Backup	GTI-01
Realizar soporte informático	GTI-02
Realizar informe mensual	GTI-03
Administrar sistemas S.I.G.A. y S.I.A.F.	GTI-04
Supervisar servicios tercerizados	GTI-05
Supervisar cumplimiento de directivas de seguridad de la información	GTI-06
Gestionar la recepción de bienes o servicios de tecnologías de información	GTI-07
Licenciamiento de software	GTI-08
Administrar portal web	GTI-09
Asignar equipo y accesos a nuevo colaborador	GTI-10

Fuente: Elabroación propia

– **Realizar copias de seguridad – Backup**

Objetivo

Normar el proceso a seguir para la realización de copias de seguridad de toda la información de los sistemas de información a cargo de la Unidad de Tecnologías de la Información.

Alcance

Comprende desde la clasificación del periodo de realización de la copia de seguridad, hasta su almacenamiento.

Tabla 16. Resumen del Proceso Realizar Copias de Seguridad - Backup

Responsable	**Actividades**
Encargado de Seguridad de la Información /Jefe de Unidad de Tecnologías de Información / Jefe de Unidad de Administración	1. Planificación de copias de seguridad - BACKUP

Encargado de Seguridad de la Información /Jefe de Unidad de Tecnologías de Información	2. Desarrollo de cronograma de copias de seguridad - BACKUP
Encargado de Seguridad de la Información /Jefe de Unidad de Tecnologías de Información	3. Almacenamiento de copias de seguridad - BACKUP

Fuente: Elaboración propia

Tabla 17. Proceso al Detalle de Realizar Copias de Seguridad - Backup

Responsable	**Actividades**
1. Planificación de copias de seguridad - BACKUP	
Encargado de Seguridad de la Información	1.1. Realiza la evaluación de los mantenimientos correctivos realizados en el año anterior, a fin de presentar las incidencias ocurridas y atenciones realizadas.
Encargado de Seguridad de la Información	1.2. Prepara el Plan Anual de Copias de Seguridad considerando: – Sistemas de Información en uso. – Criticidad de la información.
Jefe de Unidad de Tecnologías de Información	1.3. Recibe el Plan Anual de Copias de Seguridad, para su revisión y conformidad. De existir observaciones devuelve el mismo para su corrección; caso contrario, continúa con el siguiente punto.
Jefe de Oficina de Administración	1.4. Recibe el Plan Anual de Copias de Seguridad, aprobado por el Jefe de Unidad de Tecnologías de Información, para su revisión y conformidad. De existir observaciones devuelve el mismo para su
Encargado de Seguridad de la Información	

	corrección; caso contrario, continúa con el siguiente punto. 1.5. Recibe el Plan Anual de Copias de Seguridad con la conformidad del Jefe de Unidad de Tecnologías de Información y el Jefe de Oficina de Administración.
2. Desarrollo de cronograma de copias de seguridad - BACKUP	
Encargado de Seguridad de la Información Jefe de Unidad de Tecnologías de Información Encargado de Seguridad de la Información Encargado de Seguridad de la Información Encargado de Seguridad de la Información Jefe de Unidad de Tecnologías de Información Jefe de Unidad de Tecnologías de Información.	2.1. Comunica a Jefe de Unidad de Tecnologías de Información realización de copia de seguridad. 2.2. Informa al área usuaria que deben salir del sistema de información por mantenimiento. 2.3. Realiza copia de seguridad de la base de datos de los sistemas de información. 2.4. Realiza almacenamiento de copia de seguridad en disco duro externo y/o en un CD. 2.5. Entrega CD a Jefe de la Unidad de Tecnologías de Información. 2.6. Recibe CD de copia de seguridad, para su revisión y conformidad. De existir observaciones devuelve el mismo para su corrección; caso contrario, continúa con el siguiente punto.

	2.7. Registra ficha de copia de seguridad.
3. Almacenamiento de copias de seguridad - BACKUP	
Jefe de la Unidad de Tecnologías de Información.	3.1 Guarda CD de copia de seguridad en histórico de copias de seguridad.

Fuente: Elaboración propia

AUTODEMA Autoridad Autónoma de Majes	**FORMATO DE PLAN ANUAL DE COPIAS DE SEGURIDAD**			**FORMATO N°01**
				SEGURIDAD DE LA INFORMACIÓN
Encargado:				**N°:**
Sistemas:	**S.I.G.A.:** S.G.	**S.I.A.F.: S.F.**	**S.I.A.T.D.: S.T.**	**Inventarios:** IN
PROGRAMACIÓN DE COPIA DE SEGURIDAD				
Mes: Enero				
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31				
Observaciones:				

Figura 29. Formato de Plan Anual de Copias de Seguridad

Fuente: Elaboración propia

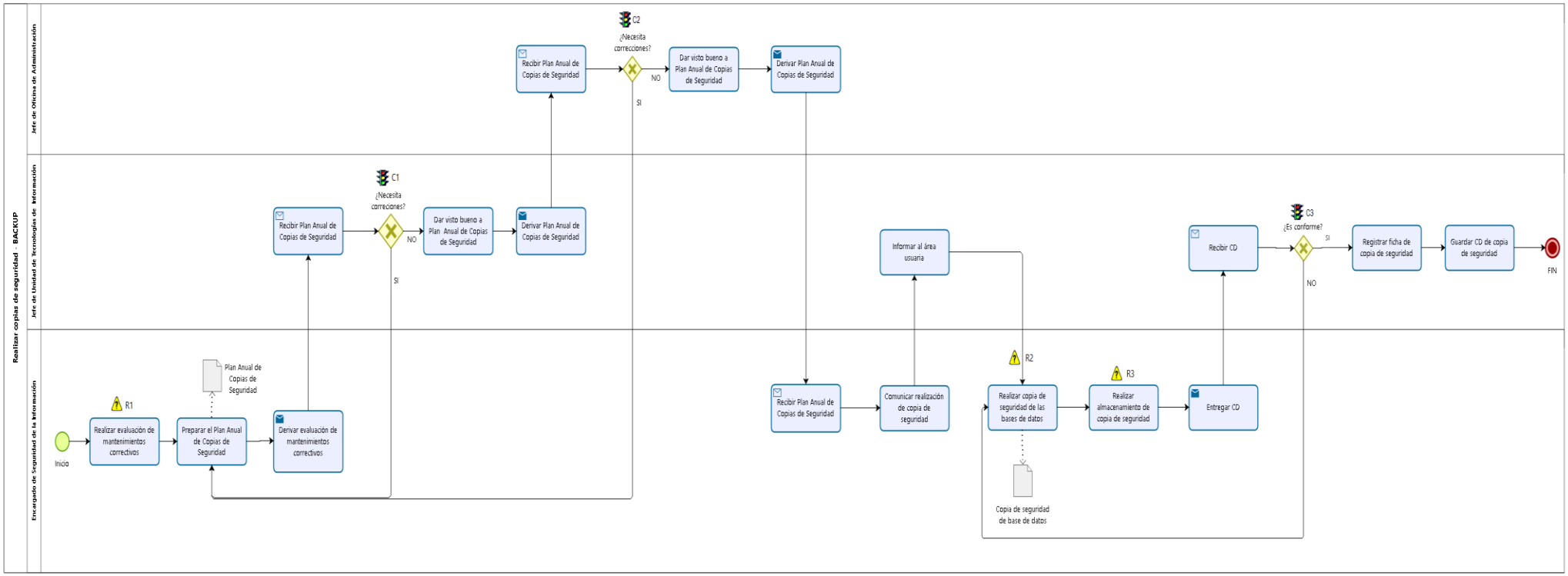


Figura 30. Diagrama de Procesos de Realizar Copias de Seguridad - Backup

Fuente: Elaboración propia

– **Realizar Soporte Informático**

Objetivo

Normar el proceso a seguir para la realización de soporte informático al área usuaria de la AUTODEMA, garantizando el buen funcionamiento de los equipos, red y programas.

Alcance

Comprende desde la recepción de solicitud de soporte informático por parte del usuario, hasta su conformidad de solución.

Tabla 18. Resumen del Proceso de Realizar Soporte Informático

Responsable	Actividades
Usuario PEMS / Mesa de Ayuda	1. Recepción de requerimiento de servicio informático
Mesa de ayuda / Mesa de Servicio / Encargado de Infraestructura de Tecnologías de Información / Jefe de Unidad de Tecnologías de Información	2. Brindar soporte informático
Mesa de Ayuda / Mesa de Servicio / Encargado de Infraestructura de Tecnologías de Información	3. Registro de solución en base de conocimiento

Fuente: Elaboración propia

Tabla 19. Proceso al Detalle de Realizar Soporte Informático

Responsable	Actividades
1. Recepción de requerimiento de servicio informático	
Usuario PEMS	1.1. Realiza requerimiento de manera verbal, escrita o telefónica de soporte informático.
Mesa de Ayuda	1.2. Recibe y analiza requerimiento del usuario PEMS y prioriza requerimiento según nivel de importancia:

	– Alto: Compromete continuidad del negocio. – Medio: Compromete tiempo de ejecución del negocio. – Bajo: No compromete la continuidad del negocio.
2. Brindar soporte informático	
Mesa de Ayuda	2.1. Realiza requerimiento solicitado. De no satisfacer requerimiento, deriva requerimiento a Mesa de Servicio.
Mesa de Servicio	2.2. Recibe requerimiento de Mesa de Ayuda y realiza soporte informático. De no satisfacer requerimiento, deriva requerimiento al Encargado de Infraestructura de Tecnologías de Información.
Encargado de Infraestructura de Tecnologías de Información	2.3. Recibe requerimiento de Mesa de Servicio y realiza soporte informático. De ser necesaria la compra de un repuesto o contratar un servicio especializado, elabora un informe técnico y lo envía al Jefe de Unidad de Tecnologías de Información
Jefe de Unidad de Tecnologías de Información	2.4. Recibe informe técnico, pasa revisión y conformidad y lo envía a usuario PEMS.
3. Registro de solución en base de conocimiento	
Mesa de Ayuda.	3.2 Registra ficha de soporte informático, de haber sido derivado el requerimiento a la Mesa de Servicio, recibe ficha de soporte informático.
Mesa de Servicio.	3.3 Registra ficha de soporte informático, de haber sido derivado el requerimiento al Encargado de

	Infraestructura de Tecnologías de Información, recibe ficha de soporte informático.
Encargado de Infraestructura de Tecnologías de Información	3.4 Registra ficha de soporte informático, de haber un informe técnico, adjuntarlo a la ficha.

Fuente: Elaboración propia

AUTODEMA Autoridad Autónoma de Majes	**FORMATO DE SOPORTE INFORMÁTICO**	**FORMATO N°02**	
		MESA DE SERVICIOS INFRAESTRUCTURA DE T. I.	
Área Solicitante:		**N°:**	
Usuario Solicitante:		**FECHA:**	
Encargado de requerimiento:			
Prioridad:		**Adjunta:**	
Requerimiento:	_____ _____ _____ _____ _____		
Solución:	_____ _____ _____ _____ _____ _____		
_____ Jefe de Unidad de Tecnologías de Información		_____ Encargado	

Figura 31. Formato de Soporte Informático

Fuente: Elaboración propia

AUTORIDAD AUTÓNOMA DE MAJES

"AÑO DEL BUEN SERVICIO AL CIUDADANO"

INFORME Nº XXX–XXXX–GRA–PEMS/TECNOLOGÍAS DE INFORMACIÓN

PARA :

ASUNTO :

REFERENCIA:

FECHA :

Campamento Central
Majes
www.autodema.gob.pe
Teléfono 837117 – Fax: 837117

"Apoya los Censos 2017: Tú cuentas para el Perú"

Urb. La
Marina E-8 Cayma
Arequipa
majessiguas@regionarequipa.gob.pe

Figura 32. Formato de Informe

Fuente: Elaboración propia

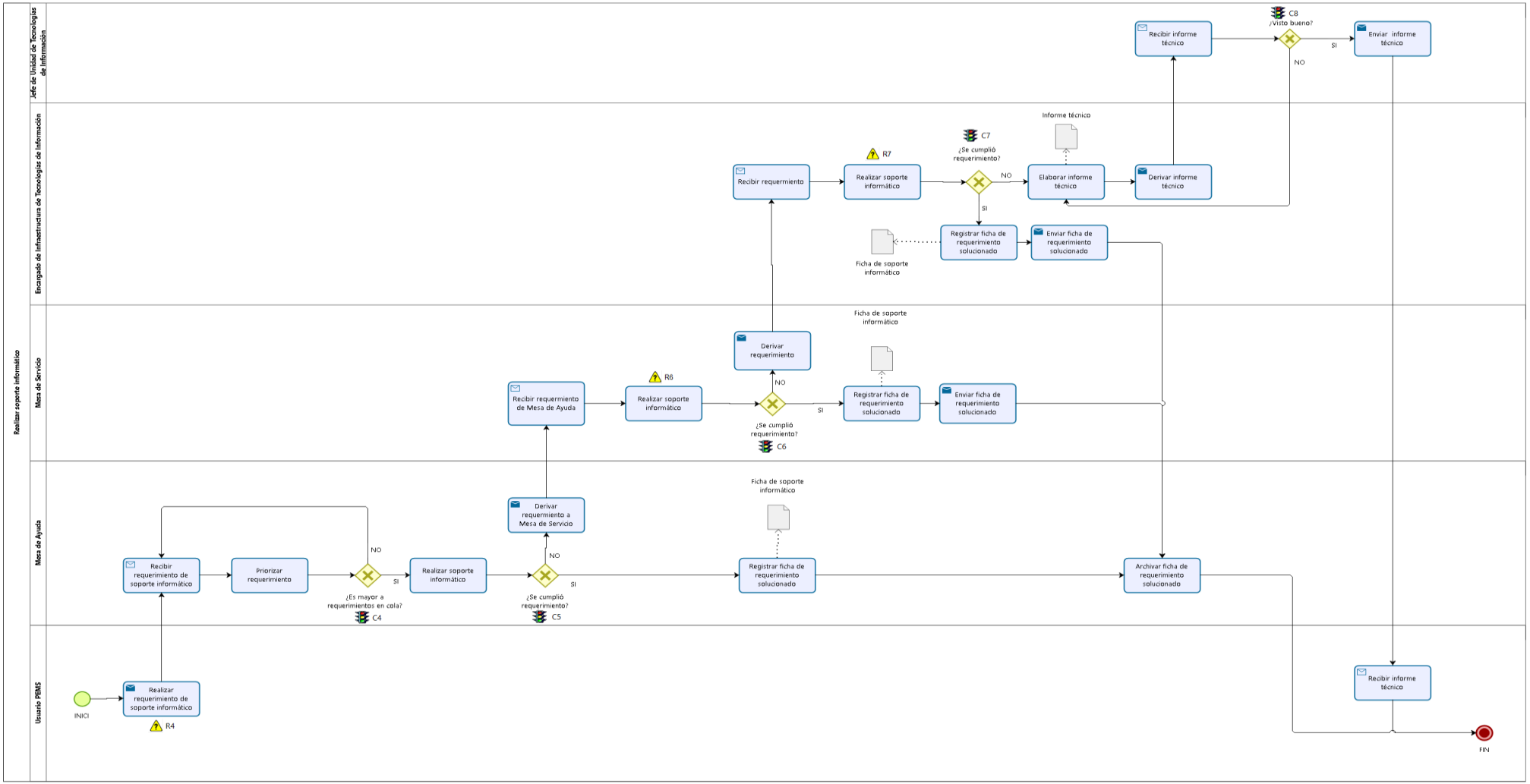


Figura 33. Diagrama de Procesos de Realizar Soporte Informático

Fuente: Elaboración propia

– **Realizar Informe Mensual.**

Objetivo

Normar el proceso a seguir para la elaboración del reporte mensual de trabajo de la Unidad de Tecnologías de Información.

Alcance

Comprende desde la solicitud de informe de actividades hasta la comunicación a la Gerencia Ejecutiva y al Jefe de Oficina de Administración acerca de las actividades realizadas en el mes.

Tabla 20. Resumen del Proceso de Realizar Informe Mensual

Responsable	Actividades
Jefe de Unidad de Tecnologías de Información / Encargado de Infraestructura de Tecnologías de Información / Encargado de Seguridad de la Información / Mesa de Servicio	1. Elaboración de informe mensual

Fuente: Elaboración propia

Tabla 21. Proceso al Detalle de Realizar Informe Mensual

Responsable	Actividades
1. Elaboración de reporte mensual	
Jefe de Unidad de Tecnologías de Información	1.1. Solicita a Mesa de Servicio, Encargado de Infraestructura de Tecnologías de Información y a Encargado de Seguridad de la Información informe mensual de las actividades realizadas en el mes.
Mesa de Servicio	1.2. Realiza informe mensual con las actividades realizadas en el mes y lo entrega a Jefe de Unidad de Tecnologías de Información.

Encargado de Infraestructura de Tecnologías de Información	1.3. Realiza informe mensual con las actividades realizadas en el mes y lo entrega a Jefe de Unidad de Tecnologías de Información.
Encargado de Seguridad de la Información	1.4. Realiza informe mensual con las actividades realizadas en el mes y lo entrega a Jefe de Unidad de Tecnologías de Información.
Jefe de Unidad de Tecnologías de Información	1.5. Recibe, evalúa y compara si las actividades realizadas por los Encargados de Unidad de Tecnologías de Información están alineadas a las metas mensuales.
Jefe de Unidad de Tecnologías de Información	1.6. Convoca a reunión para establecer metas de mes que apoyen a los objetivos anuales de la Unidad.
Jefe de Unidad de Tecnologías de Información	1.7. Elabora informe consolidado.
Jefe de Unidad de Tecnologías de Información	1.8. Envía copia de informe consolidado a Gerencia Ejecutiva y a Jefe de Oficina de Administración.

Fuente: Elaboración propia

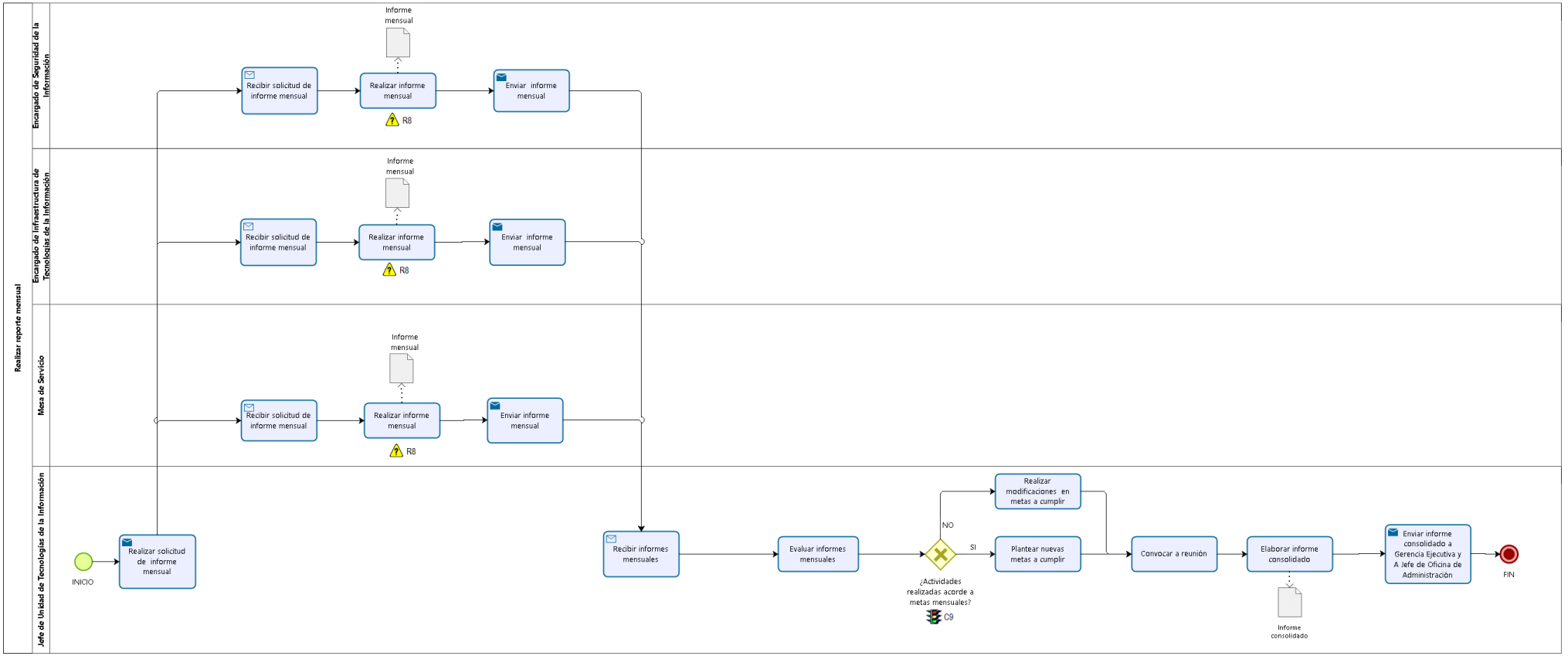


Figura 34. Diagrama de Procesos de Realizar Reporte Mensual

Fuente: Elaboración propia

– **Administrar Sistemas S.I.G.A. y S.I.A.F.**

Objetivo

Normar el proceso a seguir para la administración de los sistemas de información S.I.G.A. y S.I.A.F.

Alcance

El proceso comienza en el requerimiento del usuario PEMS y termina en la notificación de la solución al requerimiento.

Tabla 22. Resumen del Proceso de Administrar Sistemas S.I.G.A. y S.I.A.F.

Responsable	Actividades
Usuario PEMS / Jefe de Unidad / Jefe de Unidad de Tecnologías de Información	1. Gestión de usuarios en el sistema de información S.I.G.A. y/o S.I.A.F.
Mesa de Ayuda / Encargado de Seguridad de la Información / Jefe de Unidad de Tecnologías de Información / Secretaria de Recursos Humanos	2. Gestión de requerimiento interna.
Sectorista regional	3. Gestión de requerimiento externa.

Fuente: Elaboración propia

Tabla 23. Proceso al Detalle de Administrar Sistemas S.I.G.A. y S.I.A.F.

Responsable	Actividades
1. Recepción de requerimiento del sistema de información S.I.G.A. y/o S.I.A.F.	
Usuario PEMS	1.1. Realiza requerimiento del sistema S.I.G.A. o S.I.A.F. a Jefe de Unidad
Jefe de Unidad	1.2. Recibe requerimiento, da conformidad y deriva solicitud a Jefe de Unidad de Tecnologías de Información, en caso la rechace termina el proceso.
Jefe de Unidad de Tecnologías de Información	1.3. Recibe requerimiento y analiza si puede solucionarse en el área o es necesario el soporte externo del

	Ministerio de Economía y Finanzas, en caso sea interno, lo deriva a Mesa de Ayuda, en caso sea externo, lo deriva a Sectorista Regional.
2. Gestión de requerimiento interna	
Mesa de Ayuda	2.5. Recibe requerimiento, lo analiza y realiza soporte técnico. En caso de ser necesaria la creación de credenciales de acceso o ítems lo deriva al Encargado de Seguridad de la Información.
Encargado de Seguridad de la Información	2.6. Recibe el requerimiento, en caso sea necesaria la creación de usuario, solicita datos a Jefe de Unidad de Tecnologías de Información: – Apellidos y nombres – Código – Profesión – Teléfono – Email – Denominación de cargo – Dependencia En caso sea necesaria la creación de ítem, solicita datos a Jefe de Unidad de Tecnologías de Información: – Descripción del producto. – Link de referencia. – Imagen del producto.
Jefe de Unidad de Tecnologías de Información	2.7. Recibe solicitud y la deriva a Secretaria de Recursos Humanos.
Secretaria de Recursos Humanos	2.8. Recibe solicitud y envía datos requeridos a Jefe de Unidad de Tecnologías de Información.

Jefe de Unidad de Tecnologías de Información Encargado de Seguridad de la Información	2.9. Recibe datos y los envía a Encargado de Seguridad de la Información. 2.10. Recibe los datos, realiza la creación de usuario/ítem y la notifica.
3. Gestión de requerimiento externa	
Sectorista regional	3.1 Recibe requerimiento, realiza la solución del mismo y notifica su solución, en caso no haya satisfecho el requerimiento lo deriva al Sectorista Nacional.

Fuente: Elaboración propia

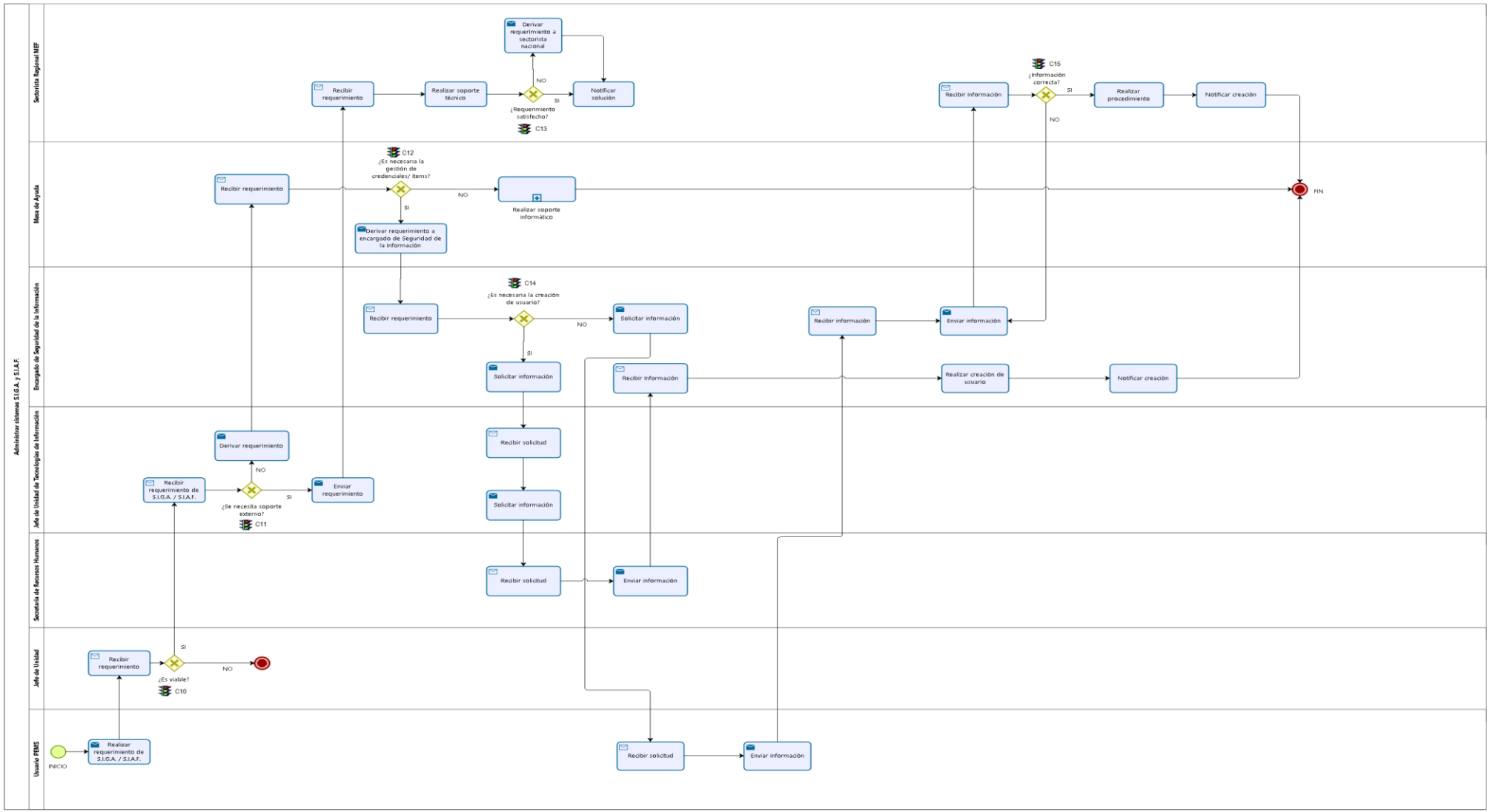


Figura 35. Diagrama de Procesos de Administrar Sistemas S.I.G.A. y S.I.A.F.

Fuente: Elaboración propia

– **Supervisar Servicios Tercerizados.**

Objetivo

Normar el proceso a seguir para la supervisión de los servicios tercerizados de la Unidad de Tecnologías de Información.

Alcance

Comprende desde la elaboración del requerimiento del servicio, hasta la emisión de conformidad del servicio.

Tabla 24. Resumen del Proceso de Supervisar Servicios Tercerizados

Responsable	Actividades
Usuario PEMS / Jefe de Unidad de Tecnologías de Información / Jefe de Oficina de Administración / Encargado de Infraestructura de Tecnologías de Información	4.11 Supervisión de servicios tercerizados

Fuente: Elaboración propia

Tabla 25. Proceso al Detalle de Supervisar Servicios Tercerizados

Responsable	Actividades
1. Supervisión de servicios tercerizados	
Usuario PEMS	1.1. Realiza requerimiento de manera escrita de términos de referencia para el desarrollo de sistema de información.
Jefe de Unidad de Tecnologías de Información	1.2. Recibe y analiza requerimiento del usuario PEMS, en caso de dar visto bueno, realiza términos de referencia y los devuelve a área usuaria.
Usuario PEMS	1.3. Elabora informe y lo envía para su aprobación a Oficina de Administración con copia a Unidad de Tecnologías de Información.

Jefe de Oficina de Administración	1.4. Recibe y analiza informe, en caso de dar conformidad, envía a Logística requerimiento de Servicio.
Encargado de Infraestructura de Tecnologías de Información	1.5. Controla y monitorea implementación del servicio.
Jefe de Unidad de Tecnologías de Información	1.6. Recibe y deriva documentación del servicio al área usuaria.
Jefe de Unidad de Tecnologías de Información	1.7. Emite conformidad de servicio y la envía a usuario PEMS.

Fuente: Elaboración propia

AUTORIDAD AUTÓNOMA DE MAJES

"AÑO DEL BUEN SERVICIO AL CIUDADANO"

TERMINOS DE REFERENCIA

SERVICIO PARA XXXXXXXxxxxxxx

I. OBJETO DE LA CONTRATACION.

Seleccionar al proveedor sea persona natural o jurídica que realice el **"SERVICIO XXXXXXXXxxxxxxx"**

II. FINALIDAD

III. ENTIDAD CONVOCANTE

Autoridad Autónoma de majes

IV. BASE LEGAL

- Ley Nº 04764/2016-PE de Presupuesto del Sector público para el año Fiscal 2016.
- Código Civil libro VII- Titulo IX, Capitulo 11 Art.1764
- Ley de Contrataciones del estado, Aprobada mediante D.L. Nº 1017, su Reglamento, aprobado por D.S. Nº 184-2008 y demás normas modificatorias (de aplicación supletoria por disposición del art. 3 del RLCE).

V. CARACTERISTICAS Y ALCANCES DEL SERVICIO.

VI. PERFIL DE LA PERSONA NATURAL O JURIDICA QUE DEBERA PRESTAR EL SERVICO SEGÚN LA NATURALEZA DE LA CONTRATACION.

VII. LUGAR Y PLAZO DE EJECUCION.

VIII. VALOR REFERENCIAL.

IX. PERIODO DE CONTRATACION O PLAZO.

X. FORMA DE PAGO

XI. INICIO DEL SERVICIO

XII. OBLIGACIONES Y RESPONSABILIDADES DEL PROVEEDOR

XIII. SUPERVISION Y CONFORMIDAD DE SERVICIO.

Figura 36. Temario de Términos de Referencia
Fuente: Elaboración propia

AUTORIDAD AUTÓNOMA DE MAJES

"AÑO DEL BUEN SERVICIO AL CIUDADANO"

INFORME N° XXX–XXXX–GRA–PEMS/TECNOLOGÍAS DE INFORMACIÓN

PARA : Jefe de la Oficina de Administración

ASUNTO : Conformidad de Servicio

REFERENCIA :

FECHA :

Tipo de Servicios

Periodo

Monto Total a Pagar

Responsable

Se otorga conformidad al presente servicio.
Fecha:.....

.....

Jefe de Unidad de Tecnologías de Información

Reg. Doc.:	
Reg. Exp.:	

Figura 37. Conformidad de Servicio

Fuente: Elaboración propia

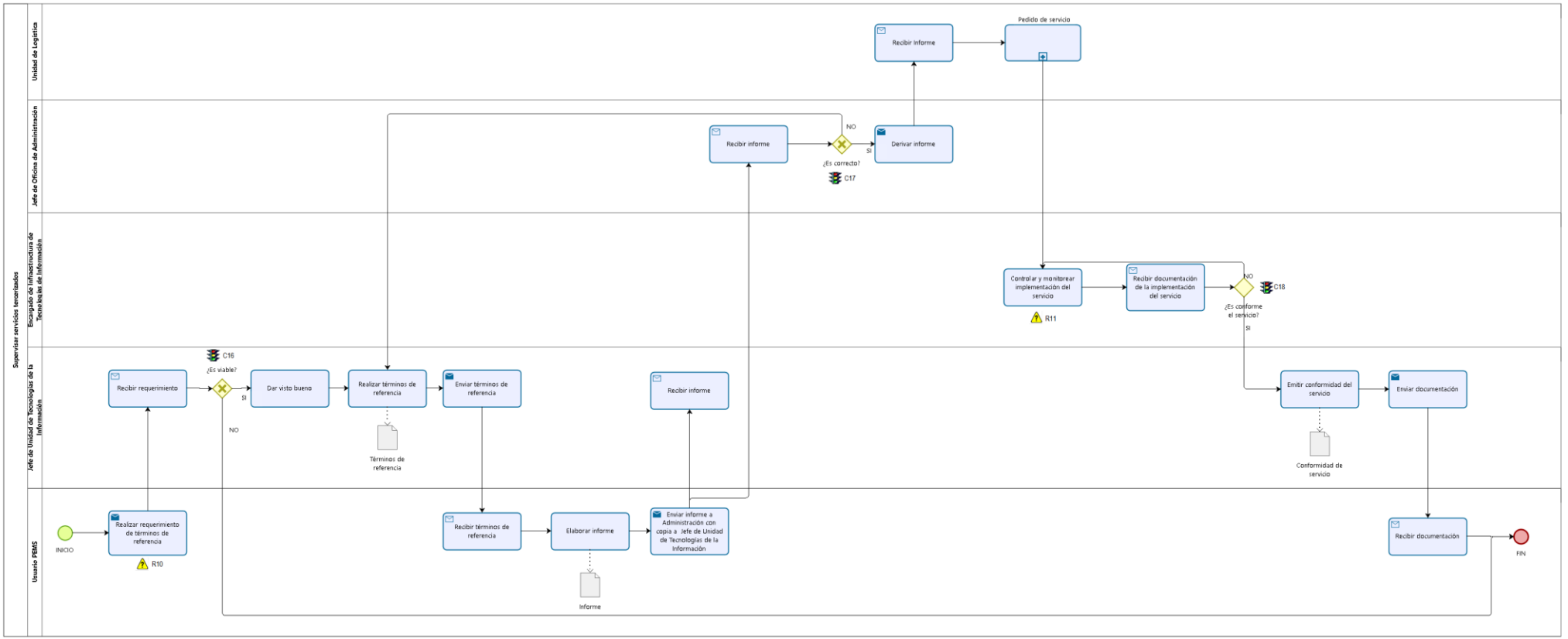


Figura 38. Diagrama de Procesos de Supervisar Servicios Tercerizados

Fuente: Elaboración propia

– **Supervisar Cumplimiento de Directivas de Seguridad de la Información.**

Objetivo

Normar el proceso a seguir para la elaboración y supervisión del cumplimiento de directivas de seguridad de la información.

Alcance

Comprende desde el análisis del cumplimiento de las directivas de seguridad de la información hasta su difusión al área usuaria.

Tabla 26. Resumen del Proceso de Supervisar Cumplimiento de Directivas de Seguridad de la Información

Responsable	Actividades
Encargado de Seguridad de la Información / Jefe de Unidad de Tecnologías de Información / Jefe de Oficina de Administración	1. Elaboración de directivas de seguridad de la información.
Encargado de Seguridad de la Información	2. Supervisión de directivas de seguridad de la información.

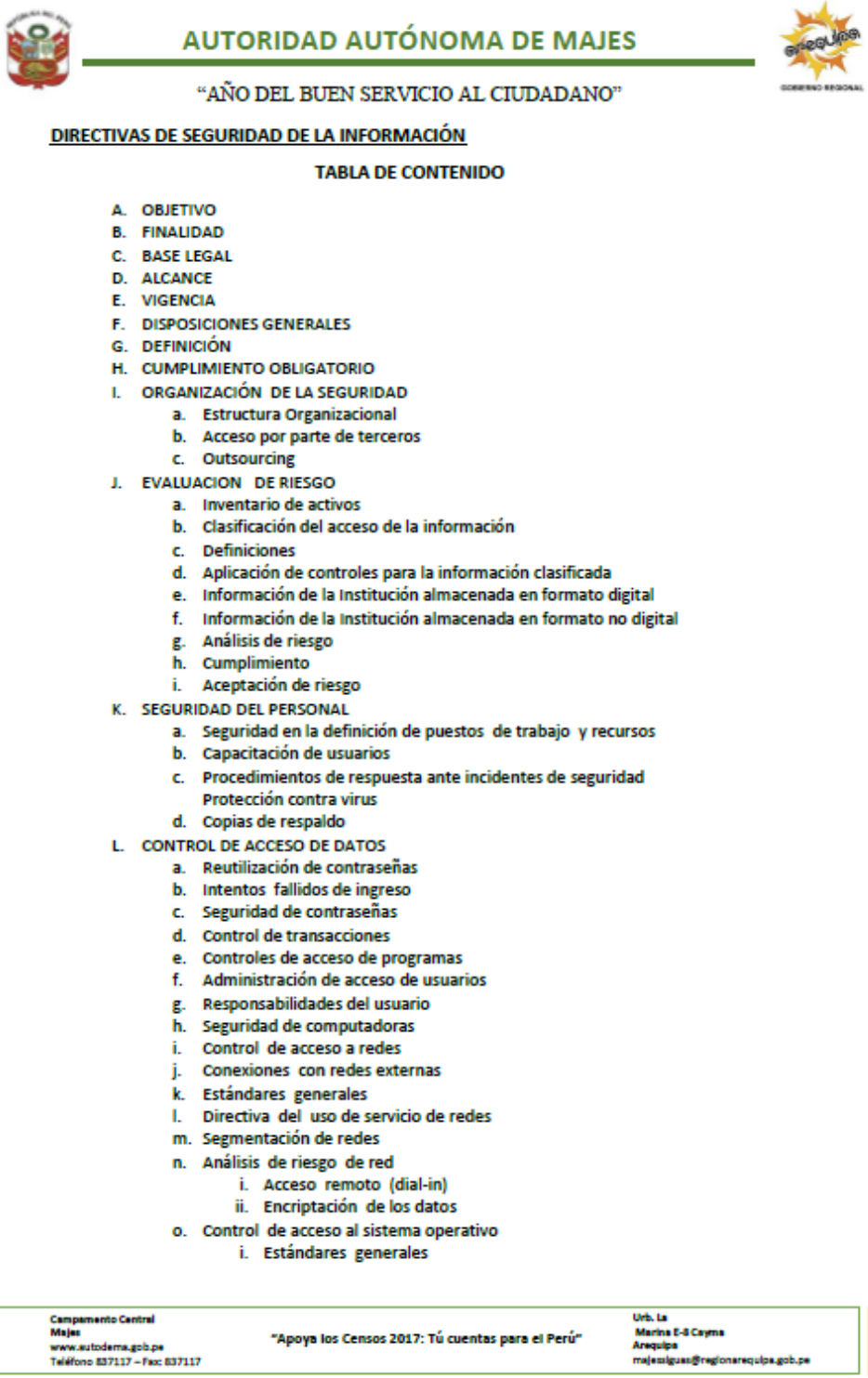
Fuente: Elaboración propia

Tabla 27. Proceso al Detalle de Supervisar Cumplimiento de Directivas de Seguridad de la Información

Responsable	Actividades
1. Elaboración de directivas de seguridad de la información	
Encargado de Seguridad de la Información	1.1. Analiza situación actual de la seguridad de la información de la AUTODEMA.
Encargado de Seguridad de la Información	1.2. Realiza actualización de directivas de seguridad de la información y las deriva al Jefe de Unidad de Tecnologías de Información para su aprobación.
Jefe de Unidad de Tecnologías de Información	1.3. Recibe las directivas de seguridad de la información para su revisión y conformidad. De existir

Jefe de Oficina de Administración	observaciones devuelve el mismo para su corrección; caso contrario, lo deriva al Jefe de Oficina de Administración para su aprobación. 1.4. Recibe las directivas de seguridad de la información para su revisión y conformidad. De existir observaciones devuelve el mismo para su corrección; caso contrario, lo visa y envía a Gerencia para su difusión mediante resolución administrativa.
2. Supervisión de directivas de seguridad de la información	
Encargado de Seguridad de la Información	2.1. Realiza monitoreo continuo del uso de la información de la AUTODEMA.

Fuente: Elaboración propia



AUTORIDAD AUTÓNOMA DE MAJES

"AÑO DEL BUEN SERVICIO AL CIUDADANO"

DIRECTIVAS DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

Campamento Central
Majes
www.autodema.gob.pe
Teléfono 837117 – Fax 837117

"Apoya los Censos 2017: Tú cuentas para el Perú"

Urb. La
Marina E-8 Cayma
Arequipa
majesiguas@regionarequipa.gob.pe

Figura 39. Índice de Directivas de Seguridad de la Información
Fuente: Elaboración propia

ii. Limitaciones de horario
iii. Administración de contraseñas
iv. Inactividad del sistema
v. Estándares de autenticación en los sistemas

p. Control de acceso de aplicación
q. Restricciones de acceso a información
r. Aislamiento de sistemas críticos
s. Monitoreo del acceso y uso de los sistemas
   i. Sincronización del reloj
   ii. Responsabilidades generales
   iii. Registro de eventos del sistema
t. CUMPLIMIENTO NORMATIVO
   i. Registros
   ii. Revisión de la directiva de seguridad y cumplimiento técnico
   iii. Propiedad de los programas
u. INFORMACIÓN ALMACENADA EN MEDIOS DIGITALES Y FÍSICOS
   i. Etiquetado de la información
   ii. Copiado de la información
   iii. Distribución de la información
   iv. Almacenamiento de la información
   v. Eliminación de la información

Figura 40. Índice de Directivas de Seguridad de la Información
Fuente: Elaboración propia

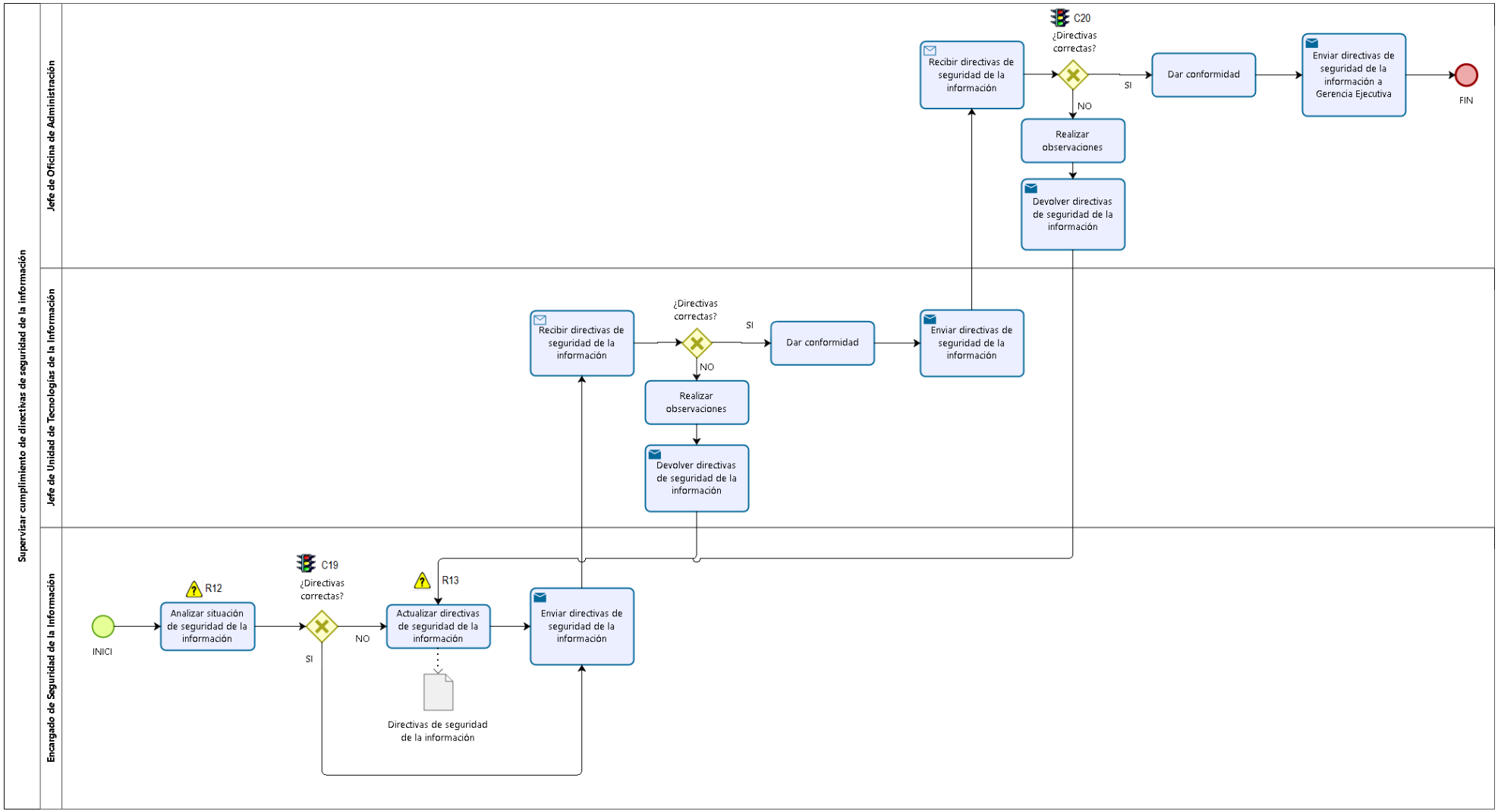


Figura 41. Diagrama de Procesos de Supervisar Cumplimiento de Directivas de Seguridad de la Información

Fuente: Elaboración propia

– **Gestionar la Recepción de Bienes o Servicios de Tecnologías de la Información.**

Objetivo

Normar el proceso a seguir para la gestión de recepción de bienes o servicios relacionados a las tecnologías de información.

Alcance

Comprende desde la recepción del bien o servicio, hasta su conformidad.

Tabla 28. Resumen del Proceso de Gestionar la Recepción de Bienes o Servicios de Tecnologías de Información

Responsable	Actividades
Jefe de Unidad de Tecnologías de Información / Encargado de Infraestructura de Tecnologías de Información / Encargado de Compras	1. Recepción de bien
Encargado de servicios / Jefe de Unidad de Tecnologías de Información / Agente Externo de Servicios	2. Recepción de servicio

Fuente: Elaboración propia

Tabla 29. Proceso al Detalle de Gestionar la Recepción de Bienes o Servicios de Tecnologías de Información

Responsable	Actividades
1. Recepción de bien	
Jefe de Unidad de Tecnologías de Información	1.1. Recibe bien y lo entrega al Encargado de Infraestructura de las Tecnologías de la Información para su revisión.
Encargado de Infraestructura de Tecnologías de Información	1.2. Recibe bien y solicita especificaciones técnicas a Encargado de Compras.

Encargado de Compras	1.3. Envía especificaciones técnicas a Encargado de Infraestructura de Tecnologías de la Información.
Encargado de Infraestructura de Tecnologías de Información	1.4. Recibe especificaciones técnicas y corrobora que el bien adquirido las cumpla, da visto bueno y entrega equipo a usuario PEMS. De haber alguna observación o desperfecto, elabora informe y lo deriva a Jefe de Unidad de Tecnologías de Información.
Jefe de Unidad de Tecnologías de Información	1.5. Recibe informe, da conformidad y lo deriva a Encargado de Compras para su solución.
Encargado de Infraestructura de Tecnologías de Información	1.6. Envía bien a almacén.
2. Recepción de servicio	
Encargado de servicios	2.1. Notifica a Jefe de Unidad de Tecnologías de Información del inicio del servicio.
Jefe de Unidad de Tecnologías de Información	2.2. Informa a Encargado de servicios comienzo de servicio. En caso de que no se cumpla en el periodo establecido, notifica a Encargado de servicios.
Agente externo de servicios	2.3. Realiza servicio, elabora informe de trabajo y lo entrega a Jefe de Unidad de Tecnologías de Información para su aprobación.

Jefe de Unidad de Tecnologías de Información	2.4. Recibe informe de trabajo, para su revisión y conformidad y lo entrega a Encargado de Servicios. En caso de que no se cumpla con lo solicitado en los términos de referencia, se lo comunica al Agente Externo de Servicios para su regularización.
Agente Externo de Servicios	2.5. Realiza servicio, actualiza informe de trabajo y lo entrega a Jefe de Unidad de Tecnologías de Información para su aprobación.
Jefe de la Unidad de Tecnologías de Información	2.6. Recibe informe de trabajo, para su revisión y conformidad y lo entrega a Encargado de Servicios. En caso de que no se cumpla, notifica a Encargado de Servicios.

Fuente: Elaboración propia

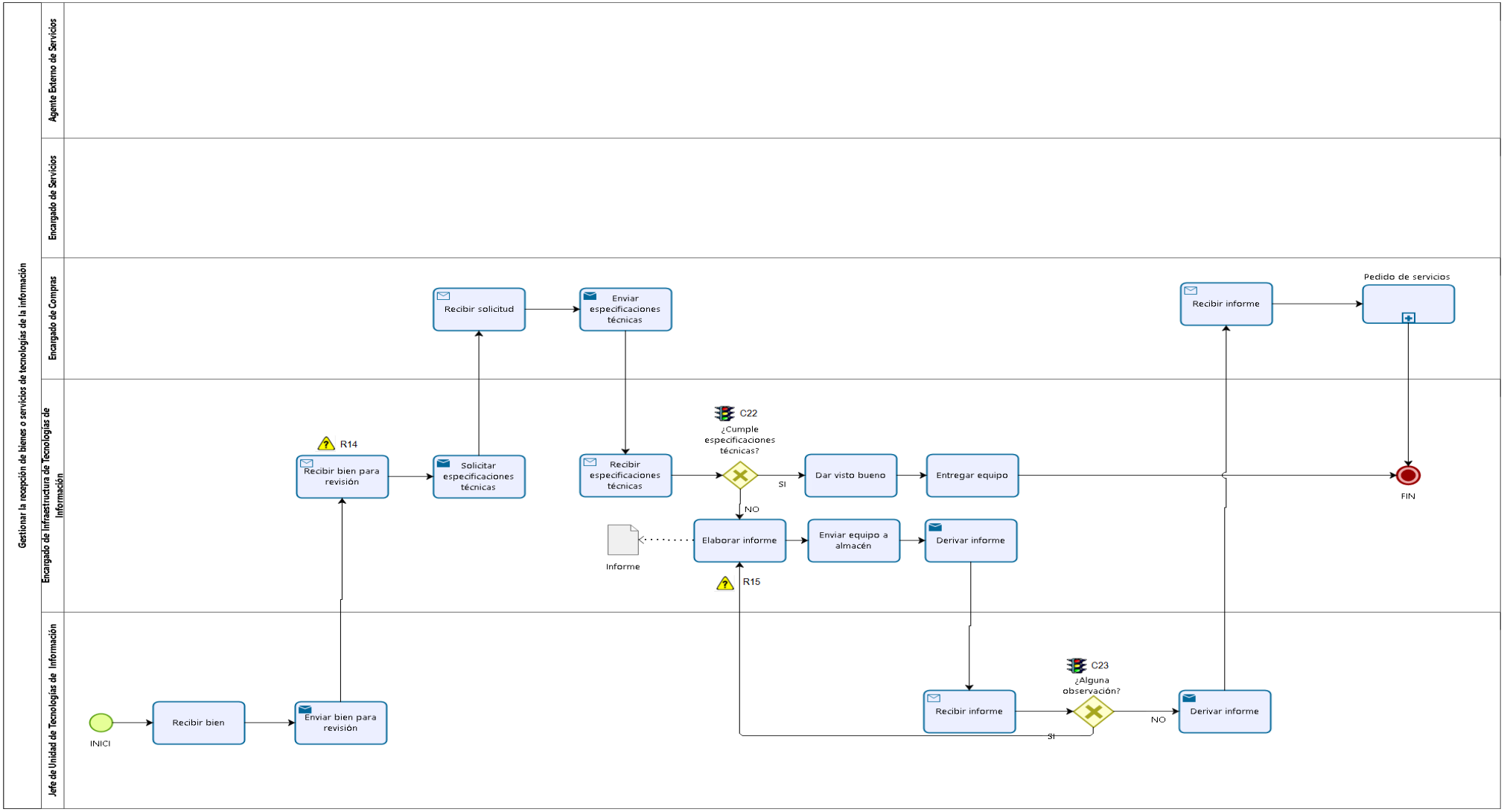


Figura 42. Diagrama de Procesos de Gestionar la Recepción de Bienes o Servicios de Tecnologías de Información

Fuente: Elaboración propia

– **Licenciamiento de Software.**

Objetivo

Normar el proceso a seguir para el licenciamiento de software para su posterior instalación en los equipos de cómputo.

Alcance

Comprende desde la solicitud del Usuario PEMS hasta la instalación de *software* licenciado por parte de Mesa de Ayuda.

Tabla 30. Resumen del Proceso de Licenciamiento de Software

Responsable	Actividades
Usuario PEMS / Jefe de Unidad de Tecnologías de Información / Encargado de Infraestructura de Tecnologías de Información / Mesa de Ayuda	1. Instalación de *software* licenciado

Fuente: Elaboración propia

Tabla 31. Proceso al Detalle de Licenciamiento de Software

Responsable	Actividades
1. Instalación de *software* licenciado	
Usuario PEMS	1.1. Solicita instalación de *software* en su equipo de cómputo al Jefe de Unidad de Tecnologías de Información.
Jefe de Unidad de Tecnologías de Información	1.2. Recibe solicitud de instalación de *software*, para su revisión y conformidad y la deriva a Encargado de Infraestructura de Tecnologías de Información. De no dar conformidad, se deniega solicitud; caso contrario, continúa con el siguiente punto.
Encargado de Infraestructura de Tecnologías de Información	1.3. Recibe solicitud de instalación de *software*, da conformidad, asigna

	licencia a equipo de cómputo, actualiza formato de asignación de equipo y entrega licencia a Mesa de Ayuda para su instalación. De no haber licencia, solicita adquisición a Jefe de Unidad de Tecnologías de Información.
Jefe de Unidad de Tecnologías de Información	1.4. Realiza requerimiento de compra.
Mesa de Ayuda	1.5. Recibe licencia de *software* y realiza instalación de *software* en equipo de cómputo

Fuente: Elaboración propia

AUTODEMA Autoridad Autónoma de Majes	FORMATO DE ASIGNACIÓN DE EQUIPO	FORMATO N°01
		INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN

Asignado:				FECHA:			
Unidad:				SBN:			
Sistema Operativo			SBN:				
Windows XP		Windows 8		Windows Server 2008		Linux	
Windows Vista		Windows 8.1		Windows Server 2012		Otro	
Windows 7		Windows 10		Windows Server 2016			
Ofimática			SBN:				
Office 2007		Office 2013		Visio 2013		Otro	
Office 2010		Office 2016		Project 2013			
Desarrollo e Ingeniería							
Visual Studio		SQL Server 2000		SQL Server 2012		S10	
Visual Fox Pro		SQL Server 2005		SQL Server 2016		Autocad	
Crystal Reports		SQL Server 2008		Arcgis		Otro	
Utilitarios							
Winrar		Nitro PDF		Google Chrome		Antivirus	
Google Earth		Nero		Power DVD		Vencimiento:	
Adobe Reader		Mozilla Firefox		VLC Player		Otro	
Sistemas y aplicaciones							
S.I.A.F.		S.I.A.T.D.		Retenciones		PDT / PLE	
S.I.G.A.		LORD-PRO		Planillas		Otro	
Diseño							
Adobe Photoshop		Adobe After Effects		Adobe Fireworks		Otros	
Adobe Dreamweaver		Adobe Illustrator		Corel Draw			

Toda reproducción o utilización de software sin tener la licencia correspondiente otorgada por el titular del derecho de autor o su representante se considera ilícita y posible de sanción administrativa y/o judicial, conforme a la R.M. N°073-2004-PCM "Administración eficiente del software legal en la administración pública".

Jefe de Unidad de Tecnologías de Información	Encargado de Infraestructura de Tecnologías de Información

Figura 43. Formato de Asignación de Equipo

Fuente: Elaboración propia

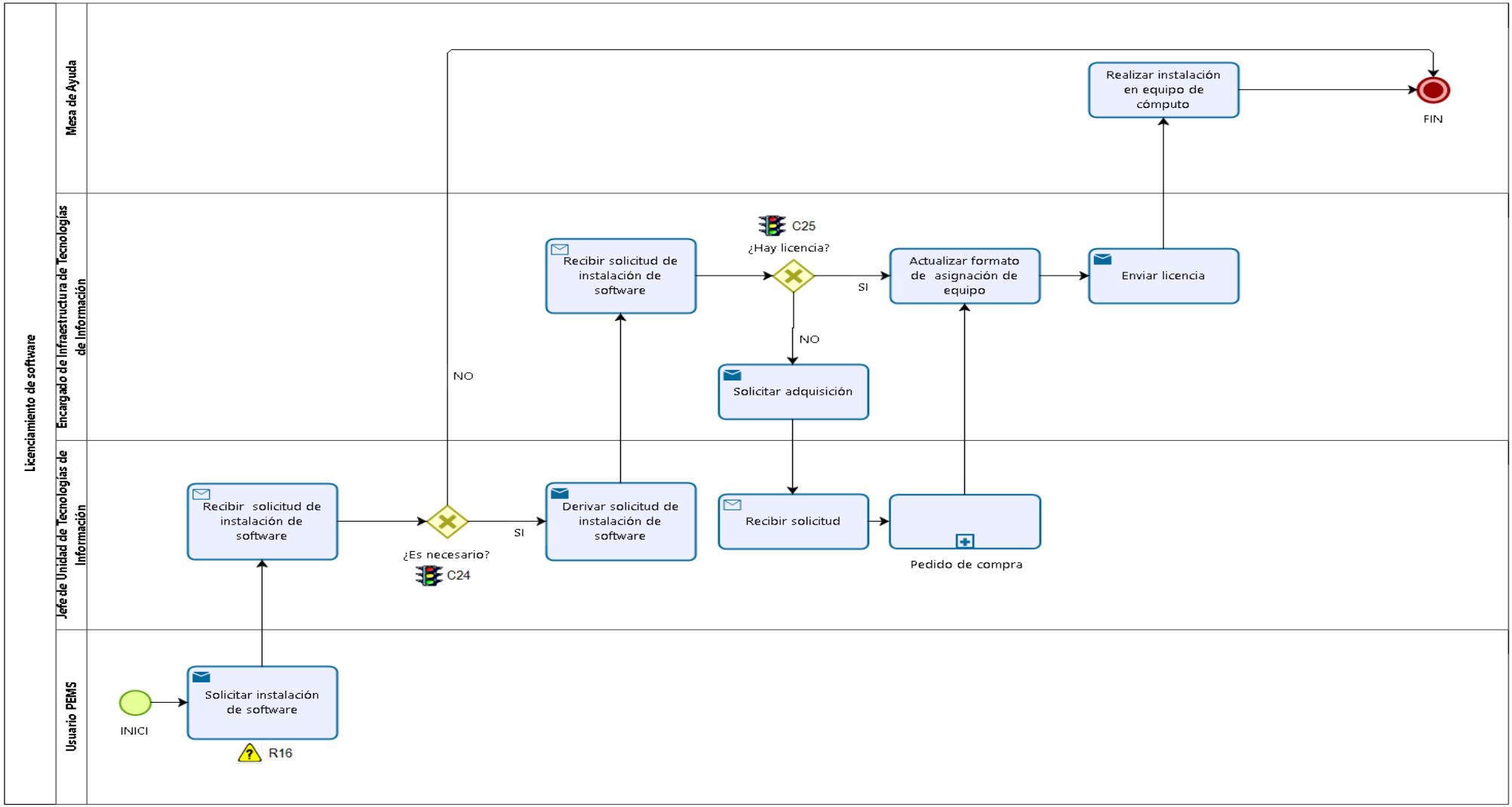


Figura 44. Diagrama de Procesos de Licenciamiento de Software

Fuente: Elaboración propia

– **Administrar Portal Web.**

Objetivo

Normar el proceso a seguir para la administración del portal web de la AUTODEMA.

Alcance

Comprende desde la solicitud de actualización de la información, hasta la notificación al Jefe de Unidad de Tecnologías de la Información.

Tabla 32. Resumen del Proceso de Administrar Portal Web

Responsable	Actividades
Encargado de Seguridad de la Información /Jefe de Unidad de Tecnologías de Información / Jefe de Oficina de Administración	1. Actualizar información de portal web
Trámite Documentario / Jefe de Unidad de Tecnologías de Información / Encargado de Infraestructura de Tecnologías de la Información	2. Subir resoluciones ejecutivas a portal web

Fuente: Elaboración propia

Tabla 33. Proceso al Detalle de Administrar Portal Web

Responsable	Actividades
1. Actualizar información de portal web	
Jefe de Unidad Jefe de Unidad de Tecnologías de Información	1.1. Solicita a Jefe de Unidad de Tecnologías de Información la actualización de información de portal web. 1.2. Recibe la solicitud de actualización de información, para su revisión y conformidad y la deriva a Encargado de Infraestructura de Tecnologías de Información. De no proceder,

Encargado de Infraestructura de Tecnologías de Información	deniega solicitud; caso contrario, continúa con el siguiente punto. 1.3. Recibe la solicitud de actualización de información realiza las modificaciones solicitadas, elabora y envía informe a Jefe de Unidad con copia a Jefe de Unidad de Tecnologías de Información.
2. Subir resoluciones ejecutivas a portal web	
Trámite Documentario Jefe de Unidad de Tecnologías de Información Encargado de Infraestructura de Tecnologías de Información Encargado de Infraestructura de Tecnologías de Información	2.1. Envía resolución ejecutiva a Jefe de Unidad de Tecnologías de Información. 2.2. Recibe y deriva resolución ejecutiva a Encargado de Infraestructura de Tecnologías de Información. 2.3. Recibe, digitaliza y sube archivo .pdf a portal web. 2.4. Archiva resolución ejecutiva y notifica a Jefe de Unidad de Tecnologías de Información.

Fuente: Elaboración propia

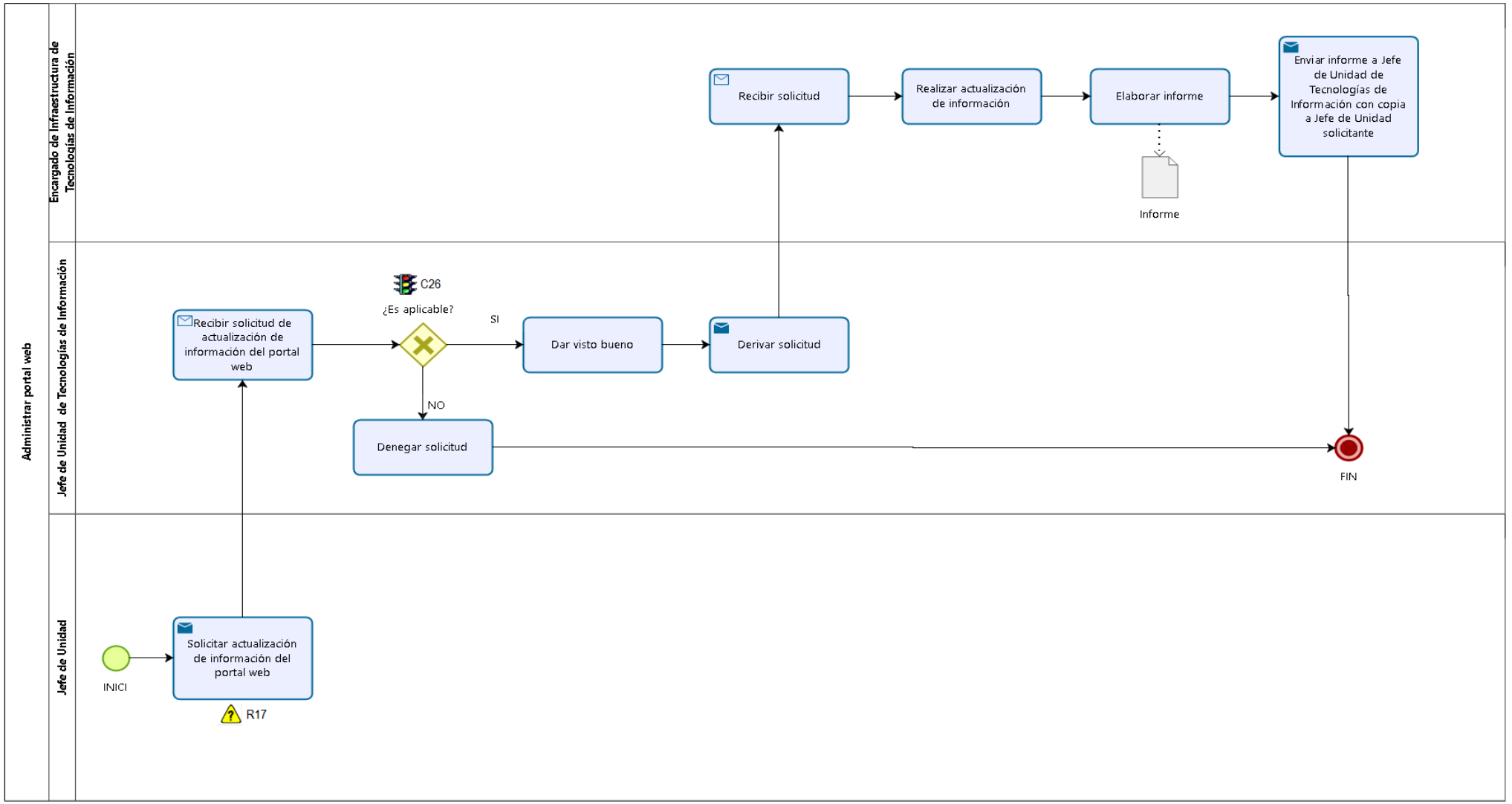


Figura 45. Diagrama de Procesos de Administrar Portal Web

Fuente: Elaboración propia

– **Asignar Equipo y Accesos a Nuevo Colaborador.**

Objetivo

Normar el proceso a seguir para la asignación de equipo de cómputo o impresora, *software,* así como los accesos a la red de la AUTODEMA y correo corporativo al nuevo colaborador.

Alcance

Comprende desde la solicitud de equipo de cómputo hasta la configuración y entrega de accesos a usuario PEMS.

*Tabla 34.*Resumen de Proceso de Asignar Equipo y Accesos a Nuevo Colaborador

Responsable	Actividades
Jefe de Unidad / Encargado de Patrimonio / Jefe de Unidad de Tecnologías de Información / Encargado de Infraestructura de Tecnologías de Información / Encargado de Patrimonio / Secretaria de Recursos Humanos /Mesa de Ayuda	1. Asignación de equipo
Secretaria de Recursos Humanos / Jefe de Unidad de Tecnologías de Información / Encargado de Seguridad de la Información / Mesa de Ayuda	2. Asignación de accesos

Fuente: Elaboración propia

Tabla 35. Proceso al Detalle de Asignar Equipo y Accesos a Nuevo Colaborador

Responsable	Actividades
1. Asignación de equipo	
Jefe de Unidad	1.1. Solicita equipo de cómputo u impresora a Encargado de Patrimonio.
Encargado de Patrimonio	1.2. Revisa inventario de activos y deriva la solicitud a Jefe de Tecnologías de Información. De no tener en inventario equipo de cómputo u impresora disponible, informa a Jefe

	de Unidad que haga un pedido de compra.
Jefe de Unidad de Tecnologías de Información	1.3. Deriva solicitud a Encargado de Infraestructura de Tecnologías de Información.
Encargado de Infraestructura de Tecnologías de Información	1.4. Realiza la verificación del estado del equipo, formatea equipo de cómputo e instala *software* solicitado por Jefe de Unidad
Encargado de Infraestructura de Tecnologías de Información	1.5. Registra formato de asignación de equipo y envía una copia a Recursos Humanos y a Patrimonio.
Encargado de Patrimonio	1.6. Recibe ficha de asignación de equipo y hace descargo de equipo de cómputo u impresora.
Secretaria de Recursos Humanos	1.7. Recibe ficha de asignación de equipo y adjunta a *file* personal de trabajador.
Mesa de Ayuda	1.8. Realiza instalación de equipo de cómputo u impresora en estación de trabajo.
2. Asignación de accesos	
Encargado de Seguridad de la Información	2.1. Solicita a Jefe de Unidad de Tecnologías de Información, la creación de usuario en *Active Directory* con los siguientes datos:

	– Apellidos y nombres – Código – Profesión – Teléfono – Email – Denominación de cargo – Dependencia
Jefe de la Unidad de Tecnologías de Información	2.2. Recibe solicitud y la deriva a Secretaria de Recursos Humanos.
Secretaria de Recursos Humanos	2.3. Recibe solicitud y envía datos requeridos a Jefe de Unidad de Tecnologías de Información.
Jefe de Unidad de Tecnologías de Información	2.4. Recibe datos y los deriva a Encargado de Seguridad de la Información.
Encargado de Seguridad de la Información	2.5. Recibe datos, crea usuario en *Active Directory* para su acceso al dominio y crea correo electrónico corporativo.
Encargado de Seguridad de la Información	2.6. Envía información a Mesa de Ayuda.
Mesa de Ayuda	2.7. Recibe información, realiza la configuración del usuario en equipo de cómputo y accesos a equipo y correo corporativo.

Fuente: Elaboración propia

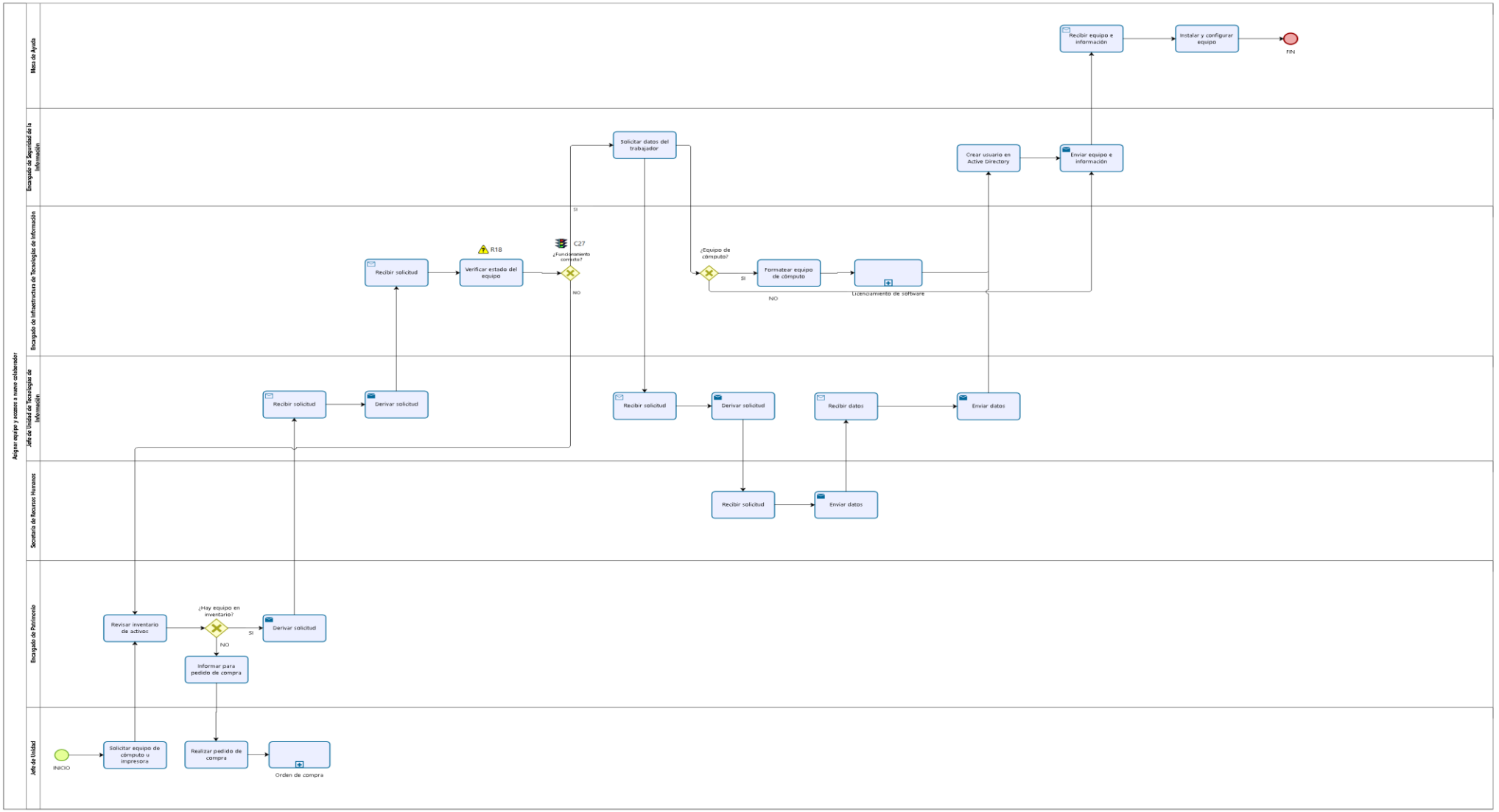


Figura 46. Diagrama de Procesos de Asignar Equipos y Accesos a Nuevo Colaborador

Fuente: Elaboración propio

3.4.4. Cumplimiento de Procesos de COBIT 5 y Controles de la NTP-ISO 27001:2014

- **APO01 Gestionar el Marco de Gestión de TI**

CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014																
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**											
APO 01	***Gestionar el marco de gestión de TI***	***Requerimientos***	***Cobertura***	***Justificación***	***GTI-01***	***GTI-02***	***GTI-03***	***GTI-04***	***GTI-05***	***GTI-06***	***GTI-07***	***GTI-08***	***GTI-09***	***GTI-10***	***Documentación***
APO 01.02	Establecer roles y responsabilidades	5.3 Roles organizacionales, responsabilidades y autoridades	C	Los roles y responsabilidades deben estar correctamente definidos.			X	X						X	Informe consolidado, Gestión de usuarios,Crear usuario en Active Directory.
APO 01.04	Comunicar objetivos y dirección de administración	5.1 Liderazgo y compromiso	A	Se debe comunicar la importancia de la administración de la seguridad de la información.			X			X		X			Informe consolidado, Directivas de seguridad de la información, Formato de asignación de equipo.
		6.2 Objetivos de Seguridad de la Información y planes para alcanzarlos	A	Se indica que los objetivos deben ser comunicados.			X			X					Informe consolidado,Directivas de seguridad de la información.
		7.4 Comunicaciones	C	Se determinan los protocolos de comunicación y lo que debe ser comunicado.						X					Directivas de seguridad de la información.
APO 01.06	Definir información(datos) y propietarios del sistema	7.5 Documentar Información	A	Se debe tener registro de la información y los dueños de la misma.	X	X									Formato de plan anual de copias de seguridad, Ficha de requerimiento solucionado, Informe técnico, Formato de copia de seguridad - backup, Formato de soporte informático, Informe mensual, Informe consolidado.
APO 01.07	Administrar la mejora continua de procesos	10.2 Mejora Continua	A	El ciclo de calidad implica una mejora continua en el proceso.		X	X		X						Ficha de requerimiento solucionado, Informe técnico, Informe mensual, Informe consolidado, Conformidad de servicio.
APO 01.08	Mantener la conformidad con políticas y procedimientos	5 Liderazgo	A	Se debe mantener la conformidad de las políticas y procedimientos como fueron definidos.	X	X	X		X	X	X	X	X		Formato de plan anual de copias de seguridad, Ficha de requerimiento solucionado, Informe técnico, Formato de copia de seguridad - backup, Formato de soporte informático, Informe mensual, Informe consolidado, Términos de referencia, Directivas de seguridad de la información, Informe, Formato de asignación de equipo, Informe.

Figura 47. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 01

Fuente: Elaboración propia

- **APO02 Gestionar la Estrategia**

CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014																
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**											
APO 02	***Gestionar la estrategia***	***Requerimientos***	***Cobertura***	***Justificación***	***GTI-01***	***GTI-02***	***GTI-03***	***GTI-04***	***GTI-05***	***GTI-06***	***GTI-07***	***GTI-08***	***GTI-09***	***GTI-10***	***Documentación***
APO 02.01	Entender la dirección de la empresa	4.2 Comprender las necesidades y expectativas de las partes interesadas	A	La norma técnica indica que se tiene que comprender las necesidades de las partes interesadas y éstas deberán tener acceso a la información pertinente.				X					X	X	Gestión de usuarios, Informe, Crear usuario en Active Directory.
APO 02.02	Evaluar el entorno actual, las capacidades y el rendimiento	5.3 Roles organizacionales, responsabilidades y autoridades	A	La norma técnica indica que cada persona deberá tener la capacidad de asignar roles y responsabilidades de acuerdo a su capacidad.										X	Crear usuario en Active Directory.
APO 02.03	Definir las capacidades de TI y sus objetivos	6.1 Acciones para dirigir los riesgos y oportunidades	A	La norma técnica indica que se deben evaluar los riesgos y oportunidades para guiar el direccionamiento del negocio.		X				X					Ficha de requerimiento solucionado, Informe técnico, Directivas de seguridad de la información.
APO 02.06	Comunicar la estrategia y la dirección de TI	7.4 Comunicaciones	A	La norma técnica indica que se debe comunicar la entre todas las partes interesadas.						X					Directivas de seguridad de la información.

Figura 48. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 02

Fuente: Elaboración propia

- **APO04 Gestionar la Innovación**

CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014															
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**										
APO 04	***Gestionar la innovación***	***Requerimientos***	***Cobertura***	***Justificación***	***GTI-01***	***GTI-02***	***GTI-03***	***GTI-04***	***GTI-05***	***GTI-06***	***GTI-07***	***GTI-08***	***GTI-09***	***GTI-10***	***Documentación***
APO 04.02	Mantener un entendimiento del ambiente de la empresa	4.2 Comprender las necesidades y expectativas de las partes interesadas	A	La norma técnica indica que se tiene que comprender las necesidades de las partes interesadas y éstas deberán tener acceso a la información pertinente, significando que debe entender el ambiente de la empresa.	X			X						X	Realizar requerimiento de soporte informático, Realizar requerimientos de S.I.G.A. o S.I.A.F., Crear usuario en Active Directory.
APO 04.03	Monitorear y observar el abiente tecnológico	9.1 Monitoreo, medición, análisis y evaluación	A	Según la norma técnica se debe monitorear los procesos de seguridad de la información y los controles que se realizan, se debe saber quien monitorea los servicios y saber los resultados de dicho monitoreo.			X			X					Informe mensual, Informe consolidado, Directivas de seguridad de la información.

Figura 49. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 04

Fuente: Elaboración propia

- **APO05 Gestionar el Portafolio**

CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014															
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**										
APO 05	***Gestionar el portafolio***	***Requerimientos***	***Cobertura***	***Justificación***	***GTI-01***	***GTI-02***	***GTI-03***	***GTI-04***	***GTI-05***	***GTI-06***	***GTI-07***	***GTI-08***	***GTI-09***	***GTI-10***	***Documentación***
APO 05.03	Evaluar y elegir programa a financiar	7.4 Comunicaciones	A	Refiere al manejo de la información en todos los procesos de una organización, así como los recursos a utilizarse en los mismos.					X		X	X			Términos de referencia,Informe, Formato de asignación de equipo

Figura 50. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 05

Fuente: Elaboración propia

– **APO07 Gestionar los Recursos Humanos**

AUTODEMA Autoridad Autónoma de Majes	CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014														
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**										
APO 07	***Gestionar los recursos humanos***	***Requerimientos***	***Cobertura***	***Justificación***	***GTI-01***	***GTI-02***	***GTI-03***	***GTI-04***	***GTI-05***	***GTI-06***	***GTI-07***	***GTI-08***	***GTI-09***	***GTI-10***	***Documentación***
APO 07.01	Mantener una asignación de tareas adecuada y apropiada	7.2 Competencias	A	Aprovecha las habilidades del personal para su correcta asignación de tareas.			X								Informe consolidado.
APO 07.03	Mantener las habilidades y competencias del personal	7.2 Competencias	A	Mantiene la capacidad de recursos humanos frente al negocio en el tiempo.					X						Términos de referencia, Conformidad de servicio.
APO 07.04	Evaluar el desempeño laboral del personal	9.1 Monitoreo, medición, análisis y evaluación 9.2 Auditoría interna	A	Consideración de evaluación del desempeño del personal correspondiente.			X								Informe mensual.
APO 07.06	Administrar personal de contrato	7.2 Competencias	A	Requerimiento de competencias de personal.					X						Términos de referencia.

Figura 51. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 07

Fuente: Elaboración propia

- **APO08 Gestionar las Relaciones**

CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014																
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**											
APO 08	***Gestionar las relaciones***	***Requerimientos***	***Cobertura***	***Justificación***	***GTI-01***	***GTI-02***	***GTI-03***	***GTI-04***	***GTI-05***	***GTI-06***	***GTI-07***	***GTI-08***	***GTI-09***	***GTI-10***	***Documentación***
APO 08.01	Entender las expectativas del negocio	4.2 Comprender las necesidades y expectativas de las partes interesadas	A	La norma técnica indica que se deben comprender las necesidades de las partes interesadas.			X			X					Informe consolidado, Directivas de Seguridad de la Información.
APO 08.02	Identificar las oportunidades, riesgos y limitaciones de TI para mejorar el negocio	6.1 Acciones para dirigir los riesgos y oportunidades	A	La norma técnica indica que se deben planear y dirigir los riesgos y las oportunidades para guiar el direccionamiento del negocio.			X			X					Informe consolidado, Directivas de Seguridad de la Información.
APO 08.04	Coordinar y comunicar	7.4 Comunicaciones	A	Se debe comunicar necesariamente los cambios realizados en la gestión de la información para mantener íntegramente la seguridad.						X					Directivas de Seguridad de la Información.
APO 08.05	Aportar a la mejora continua de los servicios	10.2 Mejora continua	A	Realiza siempre mejoras en la gestión de sistemas de seguridad de la información y mantener los documentos ordenados y bien documentados al alcance de todas las partes interesadas.	X	X				X	X				Formato de plan de copias de seguridad, Ficha de requerimiento solucionado, Informe técnico, Directivas de Seguridad de la Información, Informe.

Figura 52. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 08

Fuente: Elaboración propia

- **APO09 Gestionar los Contratos de Servicio**

CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014															
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**										
APO 09	***Gestionar los contratos de servicio***	***Requerimientos***	***Cobertura***	***Justificación***	***GTI-01***	***GTI-02***	***GTI-03***	***GTI-04***	***GTI-05***	***GTI-06***	***GTI-07***	***GTI-08***	***GTI-09***	***GTI-10***	***Documentación***
APO 09.01	Identidficar los servicios de TI	6.1 Acciones para dirigir los riesgos y oportunidades	A	Se debe analizar la demanda de los servicios de TI, identificando los riesgos y planeando los posibles efectos de los mismos.	X				X		X	X			Formato de plan anual de copias de seguridad, Informe.
APO 09.02	Catálogo de servicios permitidos por TI	7.5. Documentar información	A	Según la norma técnica se debe tener documentada la información de la que se dispone, estando adecuada y disponible, además de estar siempre protegida contra pérdida.	X					X	X	X	X	X	Formato de plan anual de copias de seguridad, Directivas de seguridad de la información, Informe, Formato de asignación de equipo.
APO 09.04	Monitorear y reportar los niveles de servicio	9.1 Monitoreo, medición, análisis y evaluación	A	Según la norma técnica se deben monitorear los procesos de seguridad de la información y los controles que se realizan, además de monitorear los servicios y sus resultados.			X			X					Informe mensual, Informe consolidado, Directivas de seguridad de la información.

Figura 53. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 09

Fuente: Elaboración propia

- **APO10 Gestionar el Marco de Gestión de TI**

CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014																
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**											
APO 10	***Gestionar el marco de gestión de TI***	***Requerimientos***	***Cobertura***	***Justificación***	***GTI-01***	***GTI-02***	***GTI-03***	***GTI-04***	***GTI-05***	***GTI-06***	***GTI-07***	***GTI-08***	***GTI-09***	***GTI-10***	***Documentación***
APO 10.03	Gestionar las relaciones y contratos con el proveedor	15.2 Gestión de cambios de los servicios del proveedor	C	Se debe gestionar permanentemente la información del proveedor, manteniendo y mejorando la misma, cada vez que sea necesario.					X			X	X		Conformidad de servicio, Formato de asignación de equipo,Informe.
APO 10.05	Monitorear el desempeño y cumplimiento del proveedor	15.2 Gestión de cambios de los servicios del proveedor	C	Se debe monitorear y auditar regularmente los servicios brindados por el proveedor.					X			X	X		Conformidad de servicio, Formato de asignación de equipo, Informe.

Figura 54. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 10

Fuente: Elaboración propia

- **APO12 Gestionar el Riesgo**

CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014																
COBIT 5.0		NTP-ISO 27001:2014			Procesos											
APO 12	*Gestionar el riesgo*	*Requerimientos*	*Cobertura*	*Justificación*	*GTI-01*	*GTI-02*	*GTI-03*	*GTI-04*	*GTI-05*	*GTI-06*	*GTI-07*	*GTI-08*	*GTI-09*	*GTI-10*	*Documentación*
APO 12.02	Analizar el riesgo	6.1 Acciones para dirigir los riesgos y oportunidades	A	Evaluación de los riesgos en un determinado intervalo para determinar como se ven afectados ante algún cambio u ocurrencia.		X				X					Ficha de requerimiento solucionado, Informe técnico, Directivas de seguridad de la información.
APO 12.03	Mantener el portafolio de riesgo	9.3 Revisión de la gestión	A	Considera el resultado de la evaluación de riesgos y el estado del riesgo luego del plan de tratamiento.		X				X					Ficha de requerimiento solucionado, Informe técnico, Directivas de seguridad de la información.
APO 12.04	Articular el riesgo	9.3 Revisión de la gestión	C	Considera el resultado de la evaluación de riesgos y el estado del riesgo luego del plan de tratamiento.	X		X			X					Formato de plan anual de copias de seguridad, Informe mensual, Informe consolidado, Directivas de seguridad de la información.
APO 12.05	Definir un portafolio de gestión de riesgos	6.1 Acciones para dirigir los riesgos y oportunidades	A	Planifica acciones para aboradar los riesgos y oportunidades y como integrarlos en los procesos de gestión de seguridad de la información.	X		X			X					Formato de plan anual de copias de seguridad, Informe mensual, Informe consolidado, Directivas de Seguridad de la Información.
APO 12.06	Respuesta al riesgo	8.3 Tratamiento de riesgos de seguridad de la información	C	Considera la implementación del plan de tratamiento de riesgos de seguridad de la información.			X			X					Informe consolidado, Directivas de seguridad de la información.

Figura 55. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 12

Fuente: Elaboración propia

- **APO13 Gestionar la Seguridad**

CUMPLIMIENTO DE PROCESOS DE COBIT 5 Y DE NTP-ISO 27001:2014															
COBIT 5.0		**NTP-ISO 27001:2014**			**Procesos**										
APO 13	***Gestionar la seguridad***	***Requerimientos***	***Cobertura***	***Justificación***	***GTI-01***	***GTI-02***	***GTI-03***	***GTI-04***	***GTI-05***	***GTI-06***	***GTI-07***	***GTI-08***	***GTI-09***	***GTI-10***	***Documentación***
APO 13.02	Definir y administrar un plan de tratamiento de riesgos de seguridad de la información	6 Planificación	A	Como se van a manejar los riesgos en la empresa, proporcionando información para el correcto desarrollo de los mismos.			X			X					Informe consolidado, Directivas de seguridad de la información.

Figura 56. Cumplimiento de Procesos de COBIT 5 y Controles de NTP-ISO 27001:2014 APO 13

Fuente: Elaboración propia

3.4.5. Evaluación de Riesgos y Controles según COBIT 5 y la NTP-ISO 27001:2014

La evaluación de riesgos y controles según COBIT 5 y la NTP- ISO 27001:2014 permitirá identificar y valorar los riesgos a los cuáles están expuestos los procesos de tecnologías de información de la Autoridad Autónoma de Majes.

3.4.5.1 Factores de Riesgo

Los factores de riesgo a evaluarse se definen en la siguiente tabla:

Tabla 36. Factores de Riesgo

Factor	**Descripción**
Personal	Personas de la organización que se encuentran relacionadas a la ejecución del proceso directa o indirectamente.
Procesos Internos	Actividades y tareas interrelacionadas que forman parte del proceso.
Tecnologías de Información	Herramientas tecnológicas que forman parte del proceso.
Eventos Externos	Condiciones incontrolables por la organización que afectan directa o indirectamente.

Fuente: Elaboración propia

3.4.5.2 Evaluación Inherente

La evaluación inherente calcula el nivel del riesgo inherente de cada uno de los riesgos de los procesos de tecnologías de información, a partir de la probabilidad de ocurrencia del mismo y su impacto sobre el desarrollo habitual del proceso.

Tabla 37. Probabilidades del Riesgo

Probabilidad	**Puntuación**
Casi certeza	5

Probable	4
Posible	3
Improbable	2
Raro	1

Fuente: Elaboración propia

Tabla 38. Impacto del Riesgo

Impacto	**Puntuación**
Catastrófico	5
Mayor	4
Moderado	3
Menor	2
Insignificante	1

Fuente: Elaboración propia

Tabla 39. Nivel del Riesgo Inherente

Probabilidad / ***Impacto***	Insignificante	Menor	Moderado	Mayor	Catastrófico
Casi certeza	(5,1)	(5,2)	(5,3)	(5,4)	(5,5)
Probable	(4,1)	(4,2)	(4,3)	(4,4)	(4,5)
Posible	(3,1)	(3,2)	(3,3)	(3,4)	(3,5)
Improbable	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)
Raro	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)

Fuente: Elaboración propia

Tabla 40. Infografía de Colores del Nivel del Riesgo

Nivel	**Color**
Extremo	Rojo
Alto	Naranja
Moderado	Amarillo
Bajo	Verde

Fuente: Elaboración propia

3.4.5.3. Tipos de Controles

Según Beingolea (2015), los controles para mitigar el riesgo, son los siguientes:

Tabla 41. Tipos de Controles

Tipo de control	Descripción
Preventivo	Tipo de control que controla las causas que ocasionan el riesgo.
Detectivo	Tipo de control que detecta y reporta la ocurrencia de los eventos que ocasionan el riesgo.
Correctivo	Tipo de control que minimiza el impacto del riesgo.

Fuente: Elaboración propia

3.4.5.4. Modalidades de Operación

Beingolea(2015), también establece las modalidades de operación por cada control:

Tabla 42. Modalidad de Operación

Modalidades de operación	Descripción
Automático	Se ejecuta por sí mismo una vez que ha sido configurado u establecido.
Combinado	Se ejecuta por sí mismo pero con intervención del responsable del control para su operatividad continua.
Manual	Se ejecuta con la intervención del responsable del control para su funcionamiento.

Fuente: Elaboración propia

3.4.5.5. Evaluación Residual

La evaluación residual calcula el nivel del riesgo residual de cada uno de los riesgos de los procesos de tecnologías de información, a partir

de la probabilidad de ocurrencia del mismo y su impacto sobre el desarrollo del proceso bajo la aplicación de controles.

Tabla 43. Evaluación Residual del Riesgo

$Probabilidad/Impacto$	Insignificante	Menor	Moderado	Mayor	Catastrófico
Casi certeza	(5,1)	(5,2)	(5,3)	(5,4)	(5,5)
Probable	(4,1)	(4,2)	(4,3)	(4,4)	(4,5)
Posible	(3,1)	(3,2)	(3,3)	(3,4)	(3,5)
Improbable	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)
Raro	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)

Fuente: Elaboración propia

Tabla 44. Infografía de Colores del Nivel del Riesgo

Nivel	**Color**
Extremo	Rojo
Alto	Naranja
Moderado	Amarillo
Bajo	Verde

Fuente: Elaboración propia

3.4.5.6. Planes de Acción

El plan de acción consiste en las actividades que realizará el responsable del mismo para tratar el riesgo.

Beingolea (2015), define cuatro opciones de tratamiento de los riesgos a aplicarse al plan de acción:

Tabla 45. Tratamiento del Riesgo

Opciones de tratamiento	**Descripción**
Aceptar	El riesgo es aceptado cuando no se puede implementar un control adecuado, el costo de la implementación del control es mayor a la

	materialización del riesgo y/o el nivel del riesgo es aceptable.
Mitigar	El riesgo es mitigado cuando se reduce la probabilidad o el impacto del riesgo a un nivel aceptable.
Transferir	El riesgo se transfiere cuando no se cuenta con los recursos necesarios para su tratamiento y se comparte con un tercero.
Eliminar	El riesgo se elimina cuando se suprime la fuente que origina el riesgo.

Fuente: Elaboración propia

RIESGOS Y CONTROLES DE LOS PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA AUTODEMA

Proceso			Riesgo				Evaluación inherente			Control												Evaluación residual			Planes de acción			
Macroproceso	Proceso	Subproceso	Código del Riesgo	Riesgo	Causa	Factor de Riesgo	Probabilidad	Impacto	Nivel de Riesgo Inherente	Código del Control	Descripción del Control	ISO 27001	COBIT 5.0	Responsable	Tipo	Ejecución	Documentación	Periodicidad	Responsabilidad	Segregación de funciones	¿Reduce la probabilidad?	¿Reduce el impacto?	Probabilidad	Impacto	Nivel de Riesgo Residual	Tratamiento	Código de Plan de Acción	Plan de Acción	Responsable
		Copias de Seguridad - BACKUP	R1	Realizar una evaluación incompleta o errónea de los mantenimientos correctivos.	Falta de juicio de expertos.	Personal	2	4	Alto	C1	Una vez que el Encargado de Seguridad de la Información desarrolla el Plan anual de copias de seguridad, el Jefe de Unidad de Tecnologías de Información lo verifica, en caso de que tenga alguna discrepancia o algo no le parezca se lo devuelve al Encargado de Seguridad de la Información para su modificación.	4.2 Comprender las necesidades y expectativas de las partes interesadas 5. Políticas, 6.1 Acciones para abordar los riesgos y oportunidades, 7.5 Documentar información 9.3 Revisión de la gestión, 10.2 Mejora continua .	APO 01.06 Definir información y propietarios del sistema, APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 04.02 Mantener un entendimiento del ambiente de la empresa, APO 06.05. Apoyo a la mejora continua APO 09.01 Identificar los servicios de TI, APO 09.02 Catálogo de servicios permitidos por TI APO 12.04 Articular el riesgo, APO12.05 Definir un portafolio de gestión de riesgos.	Jefe de Unidad de Tecnologías de Información	Preventivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	SI	No	1	4	Alto	Transferir	PA1	El Encargado de Seguridad de la Información debe hacer la modificación del Plan Anual de Seguridad de la Información según las correcciones del Jefe de Unidad de Tecnologías de Información.	Encargado de Seguridad de la Información
					Mala documentación de los mantenimientos correctivos.	Procesos internos	4	4	Extremo	C2	El Jefe de Oficina de Administración revisa el Plan Anual de Copias de Seguridad, en caso de que tenga alguna discrepancia o algo no le parezca se lo devuelve al Encargado de Seguridad de la Información para su modificación.	5. Políticas, 9.3 Revisión de la gestión, 10.2 Mejora continua.	APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 06.05. Apoyo a la mejora continua, APO 12.04 Articular el riesgo.	Jefe de Oficina de Administración	Preventivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	SI	No	1	4	Alto	Transferir	PA2	El Encargado de Seguridad de la Información debe hacer la modificación del Plan Anual de Seguridad de la información según las correcciones del Jefe de la Oficina de Administración	Encargado de Seguridad de la Información
			R2	Realizar copia de seguridad corrupta.	La copia de seguridad de la base de datos se interrumpió o se generó dañada.	Procesos internos	2	5	Extremo	C3	El Jefe de Unidad de Tecnologías de Información realiza la verificación de la copia de seguridad a almacenarse.	5. Políticas, 9.3 Revisión de la gestión, 10.2 Mejora continua.	APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 06.05. Apoyo a la mejora continua, APO 12.04 Articular el riesgo.	Jefe de Unidad de Tecnologías de Información	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	SI	No	1	5	Alto	Mitigar	PA3	El Jefe de Unidad de Tecnologías de Información debe verificar cada una de las copias de seguridad realizadas para garantizar la integridad.	Jefe de Unidad de Tecnologías de Información
			R3	Almacenar copia de seguridad corrupta.	La copia de seguridad de la base de datos se generó dañada.	Tecnología de la Información	2	5	Extremo																				

Figura 57. Evaluación de Riesgos y Controles según COBIT 5 y la NTP-ISO 27001:2014 GTI-01

Fuente: Elaboracion propia

RIESGOS Y CONTROLES DE LOS PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA AUTODEMA

Proceso			Riesgo				Evaluación inherente			Control														Evaluación residual			Planes de acción			
Macroproceso, Proceso		Subproceso	Código del Riesgo	Riesgo	Causa	Factor de Riesgo	Probabilidad	Impacto	Nivel de Riesgo Inherente	Código del Control	Descripción del Control	ISO 27001	COBIT 5.0	Responsable	Tipo	Ejecución	Documentación	Periodicidad	Responsabilidad	Segregación de funciones	¿Reduce la probabilidad?	¿Reduce el impacto?	Probabilidad	Impacto	Nivel de Riesgo Residual	Tratamiento	Código de Plan de Acción	Plan de Acción	Responsable
		Realizar Soporte Informático	R4	Solicitar atención de requerimiento de soporte informático inmediato.	El usuario PEMS piensa que su requerimiento es el más importante.	Personal	5	3	Extremo	C4	Mesa de Ayuda al hacer el primer contacto con el usuario PEMS, asigna la prioridad respectiva al requerimiento realizado a partir de los demás requerimientos que están en cola.	5. Políticas, 6.1Acciones para dirigir los riesgos y oportunidades, 7.5 Documentar Información, 9.3 Revisión de la gestión, 10.2 Mejora continua.	APO 01.06 Definir información y propietarios del sistema, APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 02.03 Definir las capacidades de TI y sus objetivos, APO 08.05 Aportar a la mejora continua de los servicios, APO 12.02 Analizar el riesgo, APO 12.03 Mantener el portafolio de riesgo.	Mesa de Ayuda	Preventivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	Si	3	2	Moderado	Mitigar	PA4	La Mesa de Ayuda prioriza cada una de las solicitudes de atención de requerimientos	Mesa de Ayuda
			R5	Realizar soporte informático que no esté en la base de conocimiento.	Requerimiento no descrito en base de conocimiento.	Procesos internos	4	3	Alto	C5	Mesa de Ayuda si realiza soporte informático, hace el llenado de una ficha de requerimiento solucionado que servirá como base de conocimiento para la solución de requerimientos similares. En caso contrario lo deriva a un nivel superior para su solución.	5. Políticas, 6.1Acciones para dirigir los riesgos y oportunidades, 7.5 Documentar Información, 9.3 Revisión de la gestión, 10.2 Mejora continua.	APO 01.06 Definir información y propietarios del sistema, APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 02.03 Definir las capacidades de TI y sus objetivos, APO 08.05 Aportar a la mejora continua de los servicios, APO 12.02 Analizar el riesgo, APO 12.03 Mantener el portafolio de riesgo.	Mesa de Ayuda	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	Si	2	2	Bajo	Aceptar	N/A	N/A	N/A
			R6	Realizar soporte informático no solucionado por Mesa de Ayuda.	Requerimiento no descrito en base de conocimiento.	Procesos internos	3	3	Alto	C6	Mesa de Servicio si realiza soporte informático, hace el llenado de una ficha de requerimiento solucionado que servirá como base de conocimiento para la solución de requerimientos similares. En caso contrario lo deriva a un nivel superior para su solución.	5. Políticas, 6.1Acciones para dirigir los riesgos y oportunidades, 7.5 Documentar Información, 9.3 Revisión de la gestión, 10.2 Mejora continua.	APO 01.06 Definir información y propietarios del sistema, APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 02.03 Definir las capacidades de TI y sus objetivos, APO 08.05 Aportar a la mejora continua de los servicios, APO 12.02 Analizar el riesgo, APO 12.03 Mantener el portafolio de riesgo.	Mesa de Servicios	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	Si	2	1	Bajo	Aceptar	N/A	N/A	N/A
			R7	Realizar soporte informático no solucionado por Mesa de Servicio.	Requerimiento no descrito en base de conocimiento.	Procesos internos	2	3	Moderado	C7	Encargado de Infraestructura de Tecnologías de Información si realiza soporte informático, hace el llenado de una ficha de requerimiento solucionado que servirá como base de conocimiento para la solución de requerimientos similares. En caso contrario elabora un Informe Técnico para su entrega al Jefe de Unidad de Tecnologías de la Información.	5. Políticas, 6.1Acciones para dirigir los riesgos y oportunidades, 7.5 Documentar Información, 9.3 Revisión de la gestión, 10.2 Mejora continua.	APO 01.06 Definir información y propietarios del sistema, APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 02.03 Definir las capacidades de TI y sus objetivos, APO 08.05 Aportar a la mejora continua de los servicios, APO 12.02 Analizar el riesgo, APO 12.03 Mantener el portafolio de riesgo.	Encargado de Infraestructura de Tecnologías de Información	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	Si	1	1	Bajo	Transferir	PA5	Se deriva el informe técnico al Jefe de Unidad de Tecnologías de Información, el cual será para la adquisición de nuevos bienes o servicios.	Jefe de Unidad de Tecnologías de Información
										C8	Revisa el Informe Técnico realizado por el Encargado de Infraestructura de Tecnologías de la Información para su posterior entrega al usuario PEMS. En caso de que necesite correcciones lo devuelve.	5. Políticas, 6.1Acciones para dirigir los riesgos y oportunidades, 7.5 Documentar Información, 9.3 Revisión de la gestión, 10.2 Mejora continua.	APO 01.06 Definir información y propietarios del sistema, APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 02.03 Definir las capacidades de TI y sus objetivos, APO 08.05 Aportar a la mejora continua de los servicios, APO 12.02 Analizar el riesgo, APO 12.03 Mantener el portafolio de riesgo.	Jefe de Unidad de Tecnologías de Información	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	No	Si	1	1	Bajo	Mitigar	PA6	Se revisa el informe técnico para dar la conformidad del mismo y entregárselo al usuario PEMS.	Jefe de Unidad de Tecnologías de Información

Figura 58. Evaluación de Riesgos y Controles según COBIT 5 y la NTP-ISO 27001:2014 GTI-02

Fuente: Elaboracion propia

RIESGOS Y CONTROLES DE LOS PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA AUTODEMA

Proceso		Riesgo				Evaluación inherente			Control											Evaluación residual			Planes de acción			
Macroproceso, Proceso	Subproceso	Código del Riesgo	Riesgo	Causa	Factor de Riesgo	Probabilidad	Impacto	Nivel de Riesgo Inherente	Código del Control	Descripción del Control	ISO 27001	COBIT 5.0	Responsable	Tipo	Ejecución	Documentación	Periodicidad	Responsabilidad	Segregación de funciones	¿Reduce la probabilidad?	¿Reduce el impacto?	Probabilidad	Impacto	Nivel de Riesgo Residual	Tratamiento	Código de Plan de Acción	Plan de Acción	Responsable
	Realizar Reporte Mensual	R8	Realizar informe mensual que no refleja a lo realizado en el mes.	El responsable de su elaboración no refleja las actividades realizadas en el mes en su Informe Mensual.	Personal	2	3	Moderado	C9	Revisa el Informe Mensual y corrobora que las actividades realizadas estén acorde a las metas planteadas para el mes, en caso éstas no hayan sido cumplidas, se analiza la razón y se reprograman. Si éstas han sido cumplidas, se asignan nuevas metas a cumplir.	4.2 Comprender las necesidades y expectativas de las partes interesadas, 5.1 Liderazgo y compromiso, 5.3 Roles organizacionales y responsabilidades, 6 Planeamiento 6.1 Acciones para dirigir los riesgos y oportunidades, 6.2 Objetivos de Seguridad de Información y planes para alcanzarlos, 7.2 Competencias, 9.1 Monitoreo, medición, análisis y evaluación, 9.3 Revisión de la gestión.	APO 01.02 Establecer roles y responsabilidades, APO 01.04 Comunicar objetivos y dirección de administración, APO01.08 Mantener la conformidad con políticas y procedimientos, APO 04.03 Monitorear y observar el ambiente tecnológico, APO 07.01 Mantener una asignación de tareas adecuada y apropiada, APO 07.04 Evaluar el desempeño laboral del personal, APO 08.01 Entender las expectativas del negocio, APO 08.02 Identificar las oportunidades, riesgos y limitaciones de TI para la mejora del negocio, APO 09.04 Monitorear y reportar los niveles de servicio, APO 12.04 Articular el riesgo, APO 12.05 Definir un portafolio de gestión de riesgos, APO 12.06 Respuesta al riesgo, , APO 13.02 Definir y administrar un plan de tratamiento de riesgos de seguridad	Jefe de Unidad de Tecnologías de Información	Correctivo	Manual	Documentado	Mensual	Asignada	Adecuada	Si	Si	1	2	Bajo	Mitigar	PA7	Se analizan las actividades realizadas con las metas del mes, si éstas van a ser actualizadas, se realizan a partir de las metas del mes vigente y anterior.	Jefe de Unidad de Tecnologías de Información

Figura 59. Evaluación de Riesgos y Controles según COBIT 5 y la NTP-ISO 27001:2014 GTI-03

Fuente: Elaboracion propia

RIESGOS Y CONTROLES DE LOS PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA AUTODEMA

Proceso		Riesgo				Evaluación inherente			Control												Evaluación residual			Planes de acción			
Macroproceso / Proceso	Subproceso	Código del Riesgo	Riesgo	Causa	Factor de Riesgo	Probabilidad	Impacto	Nivel de Riesgo Inherente	Código del Control	Descripción del Control	ISO 27001	COBIT 5.0	Responsable	Tipo	Ejecución	Documentación	Periodicidad	Responsabilidad	Segregación de funciones	¿Reduce la probabilidad?	¿Reduce el impacto?	Probabilidad	Impacto	Nivel de Riesgo Residual	Tratamiento	Código de Plan de Acción	Plan de Acción	Responsable
Información	Administrar Sistemas S.I.G.A. y S.I.A.F.	R9	Realizar un requerimiento que no amerita ser atendido.	El usuario PEMS realiza un requerimiento innecesario para el desarrollo del negocio.	Personal	4	1	Moderado	C10	El Jefe de Unidad decide si el requerimiento solicitado por el usuario PEMS amerita ser derivado a la Unidad de Tecnologías de Información.	4.2 Comprender las necesidades y expectativas de las partes interesadas.	APO 01.02 Establecer roles y responsabilidades, APO 02.01 Entender la dirección de la empresa, APO 04.02 Mantener un entendimiento del ambiente de la empresa.	Jefe de Unidad	Detectivo	Manual	Sin Documentar	Cada vez que ocurre	No Asignada	N/E	Si	No	3	1	Bajo	Transferir	PA8	Se realiza el filtrado de requerimientos.	Jefe de Unidad
									C11	Verifica si el requerimiento solicitado necesita intervención del MEF para ser cumplio o puede realizarse en la institución.	4.2 Comprender las necesidades y expectativas de las partes interesadas.	APO 01.02 Establecer roles y responsabilidades, APO 02.01 Entender la dirección de la empresa, APO 04.02 Mantener un entendimiento del ambiente de la empresa.	Jefe de Unidad de Tecnologías de Información	Detectivo	Manual	Sin Documentar	Cada vez que ocurre	No Asignada	Adecuada	Si	No	2	1	Bajo	Transferir	PA9	Se realiza el filtrado de requerimientos.	Jefe de Unidad de Tecnologías de Información
									C12	Se verifica si el requerimiento es de gestión de credenciales o de gestión de ítems para su derivación.	4.2 Comprender las necesidades y expectativas de las partes interesadas.	APO 01.02 Establecer roles y responsabilidades, APO 02.01 Entender la dirección de la empresa, APO 04.02 Mantener un entendimiento del ambiente de la empresa.	Mesa de Ayuda	Detectivo	Manual	Sin Documentar	Cada vez que ocurre	No Asignada	Adecuada	Si	No	1	1	Bajo	Aceptar	N/A	N/A	N/A
									C13	Se verifica si el requerimiento ha sido satisfecho, en caso éste no haya podido ser solucionado lo deriva a un nivel más alto del MEF.	4.2 Comprender las necesidades y expectativas de las partes interesadas.	APO 01.02 Establecer roles y responsabilidades, APO 02.01 Entender la dirección de la empresa, APO 04.02 Mantener un entendimiento del ambiente de la empresa.	Sectorista Regional MEF	Correctivo	Combinado	Sin Documentar	Cada vez que ocurre	Asignada	Adecuada	Si	No	1	1	Bajo	Transferir	PA10	Se realiza el filtrado de requerimientos.	Sesctorista Regional
									C14	Se verifica si el usuario realizó el requerimiento de creación de credenciales, para la asignación de permisos respectiva para que pueda trabajar en el sistema.	4.2 Comprender las necesidades y expectativas de las partes interesadas.	APO 01.02 Establecer roles y responsabilidades, APO 02.01 Entender la dirección de la empresa, APO 04.02 Mantener un entendimiento del ambiente de la empresa.	Encargado de Seguridad de la Información	Detectivo	Manual	Sin Documentar	Cada vez que ocurre	Asignada	Adecuada	Si	No	1	1	Bajo	Mitigar	PA11	Se realiza la creación de credenciales de acceso al sistema.	Encargado de Seguridad de la Información
									C15	Se verifica si el requerimiento cumple con brindar la información necesaria para la creación del ítem. En caso no cumpla, se realiza la devolución de la solicitud para su corrección.	4.2 Comprender las necesidades y expectativas de las partes interesadas.	APO 01.02 Establecer roles y responsabilidades, APO 02.01 Entender la dirección de la empresa, APO 04.02 Mantener un entendimiento del ambiente de la empresa.	Sectorista Regional MEF	Detectivo	Manual	Sin Documentar	Cada vez que ocurre	Asignada	Adecuada	Si	No	1	1	Bajo	Transferir	PA12	Se envía al MEF la información necesaria para la creación del ítem	Encargado de Seguridad de la Información

Figura 60. Evaluación de Riesgos y Controles según COBIT 5 y la NTP-ISO 27001:2014 GTI-04

Fuente: Elaboracion propia

RIESGOS Y CONTROLES DE LOS PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA AUTODEMA

Proceso		Riesgo				Evaluación Inherente			Control										Evaluación residual			Planes de acción			
Macroproceso / Proceso	Subproceso	Código del Riesgo	Riesgo	Causa	Factor de Riesgo	Probabilidad	Impacto	Nivel de Riesgo Inherente	Código del Control	Descripción del Control	ISO 27001	COBIT 5.0	Responsable	Tipo	Ejecución	Documentación	Periodicidad	Responsabilidad	Segregación de funciones	¿Reduce la probabilidad?	¿Reduce el impacto?	Probabilidad	Impacto	Nivel de Riesgo Residual	Tratamiento	Código de Plan de Acción	Plan de Acción	Responsable
Tecnologías de la Información / Gestión de las Tecnologías	Supervisar Servicios Tercerizados	R10	Realizar un requerimiento que no se encuentra planeado.	El usuario PEMS realiza un requerimiento innecesario para el desarrollo del negocio o no cuenta la Unidad para su ejecución.	Personal	3	3	Alto	C16	Se revisa el requerimiento realizado por el usuario PEMS. En caso de no ser viable se rechaza la solicitud.	5. Políticas, 6.1 Acciones para dirigir los riesgos y oportunidades, 7.4 Comunicaciones, 10.2 Mejora continua.	APO 01.07 Administrar la mejora continua de procesos, APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 05.03 Evaluar y elegir programa a financiar, APO 07.03 Mantener las habilidades y competencias del personal, APO 09.01 Identificar los servicios de TI.	Jefe de Unidad de Tecnologías de Información	Detectivo	Manual	Sin Documentar	Cada vez que ocurre	Asignada	Adecuada	No	Si	3	1	Bajo	Mitigar	PA13	Se realiza el filtrado de requerimientos.	Jefe de Unidad de Tecnologías de Información
									C17	Se revisa el informe con los términos de referencia. En caso esté mal elaborado, se devuelve para su corrección.	5. Políticas, 6.1 Acciones para dirigir los riesgos y oportunidades, 7.4 Comunicaciones, 10.2 Mejora continua, 15. Gestión de cambios de los servicios del proveedor.	APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 05.03 Evaluar y elegir programa a financiar, APO 07.03 Mantener las habilidades y competencias del personal, APO 07.06 Administrar personal de contrato, APO 09.01 Identificar los servicios de TI, APO 10.03 Gestionar las relaciones y contratos con el proveedor .	Jefe de Oficina de Administración	Detectivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	No	Si	3	2	Moderado	Transferir	PA14	Se revisa el Informe de Términos de Referencia según los requerimientos del negocio.	Jefe de Oficina de Administración
		R11	El servicio recibido no cumple el requerimiento.	El personal del servicio no cumple lo establecido en los Términos de Referencia.	Eventos Externos	2	4	Alto	C18	Se revisa el servicio recibido y se compara con lo requerido en los Términos de Referencia, si éste no cumple con lo especificado, el servicio tiene la obligación de corregirlo, una vez que cumpla lo establecido, se dá la conformidad de servicio.	5. Políticas, 6.1 Acciones para dirigir los riesgos y oportunidades, 7.4 Comunicaciones, 10.2 Mejora continua, 15. Gestión de cambios de los servicios del proveedor.	APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 05.03 Evaluar y elegir programa a financiar, APO 07.03 Mantener las habilidades y competencias del personal, APO 07.06 Administrar personal de contrato, APO 09.01 Identificar los servicios de TI, APO 10.03 Gestionar las relaciones y contratos con el proveedor APO 10.05 Monitorear el desempeño y cumplimiento del proveedor.	Jefe de Unidad de Tecnologías de Información	Correctivo	Combinado	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	Si	1	2	Bajo	Mitigar	PA15	Revisar y monitorear el cumplimiento del servicio tercerizado hasta que cumpla con o establecido en los Términos de Referencia y dar la Conformidad de Servicio, caso contrario hacer efectiva la cláusula de incumplimiento.	Jefe de Unidad de Tecnologías de Información

Figura 61. Evaluación de Riesgos y Controles según COBIT 5 y la NTP-ISO 27001:2014 GTI-05

Fuente: Elaboracion propia

RIESGOS Y CONTROLES DE LOS PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA AUTODEMA

Proceso		Riesgo				Evaluación inherente			Control												Evaluación residual			Planes de acción				
Macroproceso	Proceso	Subproceso	Código del Riesgo	Riesgo	Causa	Factor de Riesgo	Probabilidad	Impacto	Nivel de Riesgo Inherente	Código del Control	Descripción del Control	ISO 27001	COBIT 5.0	Responsable	Tipo	Ejecución	Documentación	Periodicidad	Responsabilidad	Segregación de funciones	¿Reduce la probabilidad?	¿Reduce el impacto?	Probabilidad	Impacto	Nivel de Riesgo Residual	Tratamiento	Código de Plan de Acción	Plan de Acción	Responsable
		Supervisar Cumplimiento de Directivas de Seguridad de la Información	R12	Realizar un análisis que no refleje la situación actual.	El encargado de Seguridad de la Información realiza un análisis de la situación de seguridad de la información sin detalle o incompleto.	Personal	3	3	Alto	C19	Se revisan las directivas de Seguridad de la Información anteriores para corroborar la situación de la Seguridad de la Información. En caso no estén correctas se realiza la actualización de las mismas	4.2 Comprender las necesidades y expectativas de las partes interesadas, 5. Políticas, 6 Planeamiento, 6.1 Acciones para dirigir los riesgos y oportunidades, 7.5 Control de la información documentada, 8.3 Tratamiento de riesgos de Seguridad de la Información, 9.1 Monitoreo, medición, análisis y evaluación, 9.3 Revisión de la gestión, 10.2 Mejora continua,	APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 02.03 Definir las capacidades de TI y sus objetivos, APO 04.03 Monitorear y observar el ambiente tecnológico, APO 08.01 Entender las expectativas del negocio, APO 08.02 Identificar las oportunidades, riesgos y limitaciones de TI para mejorar el negocio, APO 08.05 Aportar a la mejora continua de los servicios, APO 09.02 Catálogo de servicios permitidos por TI, APO 09.04 Monitorear y reportar los niveles de servicio, APO 12.02 Analizar el riesgo, APO 12.03 Mantener el portafolio de riesgo, APO 12.04 Articular el riesgo, APO 12.05 Definir un portafolio de gestión de riesgos, APO 12.06 Respuesta al riesgo, APO 13.02 Definir y administrar un plan de tratamiento de riesgos de seguridad de la información.	Encargado de Seguridad de la Información	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	Si	2	1	Bajo	Mitigar	PA16	Se realizan las correcciones realizadas por el Jefe de Unidad de Tecnologías de Información.	Encargado de Seguridad de la Información
			R13	Se definen directivas de seguridad de la información innecesarias o mal definidas.	El encargado de Seguridad de la Información define directivas que no son necesarias para mantener la disponibilidad, integridad y confidencialidad de los datos.	Personal	2	4	Alto	C20	Se revisan las Directivas de Seguridad de la Información presentada por el Encargado de Seguridad de Información. En caso no estén correctas, realiza observaciones y se las devuelve.	4.2 Comprender las necesidades y expectativas de las partes interesadas, 5. Políticas 6.1 Acciones para dirigir los riesgos y oportunidades, 6.2 Objetivos de Seguridad de Información y planes para alcanzarlos, 7.4 Comunicaciones, 7.5 Control de la información documentada, 8.3 Tratamiento de riesgos de Seguridad de la Información, 9.1 Monitoreo, medición, análisis y evaluación, 9.1 Monitoreo, medición, análisis y evaluación, 9.3 Revisión de la gestión, 10. Mejora continua.	APO 01.08 Mantener la conformidad con políticas y procedimientos. APO 02.03 Definir las capacidades de TI y sus objetivos, APO 02.06 Comunicar la estrategia y la dirección de TI, APO 04.03 Monitorear y observar el ambiente tecnológico. APO 08.01 Entender las expectativas del negocio, APO 08.02 Identificar las oportunidades, riesgos y limitaciones de TI para mejorar el negocio, APO 08.04 Coordinar y comunicar, APO 08.05 Aportar a la mejora continua de los servicios, APO 09.02 Catálogo de servicios permitidos por TI, APO 09.04 Monitorear y reportar los niveles de servicio, APO 12.02 Analizar el riesgo, APO 12.03 Mantener el portafolio de riesgo, APO 12.04 Articular el riesgo, 12.05 Definir un portafolio de gestión de riesgos, APO 12.06 Respuesta al riesgo, APO 13.02 Definir y administrar un plan de tratamiento de riesgos de seguridad de la información.	Jefe de Unidad de Tecnologías de Información	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	No	1	4	Alto	Transferir	PA17	Se realizan las correcciones solicitadas por el Jefe de Unidad de Tecnologías de Información.	Jefe de Unidad de Tecnologías de Información
										C21	Se revisan las directivas de Seguridad de la Información presentada por el Encargado de Seguridad de Información y revisadas por el Jefe de Unidad de Tecnologías de Información. En caso no estén correctas, realiza observaciones y se las devuelve.	4.2 Comprender las necesidades y expectativas de las partes interesadas, 5. Políticas 5.1 Liderazgo y compromiso, 6.1 Acciones para dirigir los riesgos y oportunidades, 6.2 Objetivos de Seguridad de información y planes para alcanzarlos, 7.4 Comunicaciones, 7.5 Control de la información documentada, 8.3 Tratamiento de riesgos de Seguridad de la Información, 9.1 Monitoreo, medición, análisis y evaluación 9.1 Monitoreo, medición, análisis y evaluación, 9.3 Revisión de la gestión, 10. Mejora continua.	APO 01.04 Comunicar objetivos y dirección de administración, APO 01.08 Mantener la conformidad con políticas y procedimientos. APO 02.03 Definir las capacidades de TI y sus objetivos, APO 02.06 Comunicar la estrategia y la dirección de TI, APO 04.03 Monitorear y observar el ambiente tecnológico. APO 08.01 Entender las expectativas del negocio, APO 08.02 Identificar las oportunidades, riesgos y limitaciones de TI para mejorar el negocio, APO 08.04 Coordinar y comunicar, APO 08.05 Aportar a la mejora continua de los servicios, APO 09.02 Catálogo de servicios permitidos por TI, APO 09.04 Monitorear y reportar los niveles de servicio, APO 12.02 Analizar el riesgo, APO 12.03 Mantener el portafolio de riesgo, APO 12.04 Articular el riesgo, 12.05 Definir un portafolio de gestión de riesgos, APO 12.06 Respuesta al riesgo, 13.02 Definir y administrar un plan de tratamiento de riesgos de seguridad de la información.	Jefe de Oficina de Administración	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	No	1	4	Alto	Mitigar	PA18	Se realizan las correcciones solicitadas por el Jefe de Unidad de Tecnologías de Información.	Encargado de Seguridad de la Información

Figura 62. Evaluación de Riesgos y Controles según COBIT 5 y la NTP-ISO 27001:2014 GTI-06

Fuente: Elaboracion propia

RIESGOS Y CONTROLES DE LOS PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA AUTODEMA

Proceso		Riesgo				Evaluación inherente			Control											Evaluación residual			Planes de acción				
Macroproceso / Proceso	Subproceso	Código del Riesgo	Riesgo	Causa	Factor de Riesgo	Probabilidad	Impacto	Nivel de Riesgo Inherente	Código del Control	Descripción del Control	ISO 27001	COBIT 5.0	Responsable	Tipo	Ejecución	Documentación	Periodicidad	Responsabilidad	Segregación de funciones	¿Reduce la probabilidad?	¿Reduce el impacto?	Probabilidad	Impacto	Nivel de Riesgo Residual	Tratamiento	Código de Plan de Acción	Plan de Acción	Responsable
	Gestionar la Recepción de Bienes o Servicios de Tecnologías de Información	R14	Revisión incompleta del bien.	Encargado de Infraestructura de Tecnologías de Información solo corrobora el funcionamiento del bien, mas no sus Especificaciones Técnicas.	Personal	2	3	Moderado	C22	Después de haber recibido el bien y las especificaciones técnicas se realiza la corroboración de cada una de las características que debería tener el equipo. En caso no sean cumplidas se elabora un informe para el proveedor.	5. Políticas, 7.4 Comunicaciones, 6.1 Acciones para dirigir los riesgos y oportunidades, 7.5 Control de la información documentada	APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 05.03 Evaluar y elegir programa a financiar, APO 09.01 Identificar los servicios de TI, APO 09.02 Catálogo de servicios permitidos por TI.	Encargado de Infraestructura de Tecnologías de Información	Detectivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	No	Si	2	2	Bajo	Transferir	PA19	Elaborar un informe con copia al proveedor y al usuario solicitante con el incumplimiento de características que presenta el bien según las Especificaciones Técnicas.	Encargado de Infraestructura de Tecnologías de Información
									C23	Se realiza la revisión del informe realizado por el Encargado de Infraestructura de Tecnologías de Información. En caso existan observaciones, lo devuelve para su corrección.	5. Políticas, 6.1 Acciones para dirigir los riesgos y oportunidades, 7.5 Control de la información documentada.	APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 09.01 Identificar los servicios de TI, APO 09.02 Catálogo de servicios permitidos por TI.	Jefe de Unidad de Tecnologías de Información	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	No	Si	2	2	Bajo	Transferir	PA20	Se realizan las correcciones solicitadas por el Jefe de Unidad de Tecnologías de Información.	Encargado de Infraestructura de Tecnologías de Información

Figura 63. Evaluación de Riesgos y Controles según COBIT 5 y la NTP-ISO 27001:2014 GTI-07

Fuente: Elaboracion propia

RIESGOS Y CONTROLES DE LOS PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA AUTODEMA

Proceso		Riesgo				Evaluación Inherente			Control												Evaluación residual			Planes de acción			
Macroproceso / Proceso	Subproceso	Código del Riesgo	Riesgo	Causa	Factor de Riesgo	Probabilidad	Impacto	Nivel de Riesgo Inherente	Código del Control	Descripción del Control	ISO 27001	COBIT 5.0	Responsable	Tipo	Ejecución	Documentación	Periodicidad	Responsabilidad	Segregación de funciones	¿Reduce la probabilidad?	¿Reduce el impacto?	Probabilidad	Impacto	Nivel de Riesgo Residual	Tratamiento	Código de Plan de Acción	Plan de Acción	Responsable
	Licenciamiento de Software	R15	El usuario solicita la instalación de software innecesario para el negocio o que perjudique el funcionamiento del negocio.	El usuario PEMS solicita instalación de software desconociendo la necesidad de licenciamiento, el contrato de licencia del mismo o su fin.	Personal	4	2	Alto	C24	Se revisa si la solicitud de instalación es necesaria para el correcto funcionamiento del negocio. En caso no lo sea, es rechazada.	5. Políticas 5.1 Liderazgo y compromiso, 7.4 Comunicaciones, 6.1 Acciones para dirigir los riesgos y oportunidades, 7.5 Control de la información documentada.	APO 01.04 Comunicar objetivos y dirección de administración, APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 09.01 Identificar los servicios de TI, APO 09.02 Catálogo de servicios permitidos por TI .	Jefe de Unidad de Tecnologías de Información	Detectivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	No	Si	4	1	Moderado	Evitar	N/A	N/A	N/A
									C25	Se revisa si el software requiere licencia de paga. En caso necesite licenciamiento se solicita la adquisición de licencia.	5.1 Liderazgo y compromiso, 7.4 Comunicaciones, 7.5 Control de la información documentada, 15.2 Gestión de cambios de los servicios del proveedor.	APO 01.04 Comunicar objetivos y dirección de administración, APO 05.03 Evaluar y elegir programa a financiar, APO 09.02 Catálogo de servicios permitidos por TI, APO 10.03 Gestionar las relaciones y contratos con el proveedor, APO 10.05 Monitorear el desempeño y cumplimiento del proveedor.	Encargado de Infraestructura de Tecnologías de Información	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	No	Si	4	1	Moderado	Aceptar	N/A	Se solicita al área que realizó el requerimiento el Pedido de Compra del software.	Área solicitante

Figura 64. Evaluación de Riesgos y Controles según COBIT 5 y la NTP-ISO 27001:2014 GTI-08

Fuente: Elaboracion propia

RIESGOS Y CONTROLES DE LOS PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA AUTODEMA																														
Proceso		Riesgo				Evaluación inherente			Control													Evaluación residual			Planes de acción					
Macroproceso / Proceso	Subproceso	Código del Riesgo	Riesgo	Causa	Factor de Riesgo	Probabilidad	Impacto	Nivel de Riesgo Inherente	Código del Control	Descripción del Control	ISO 27001	COBIT 5.0	Responsable	Tipo	Ejecución	Documentación	Periodicidad	Responsabilidad	Segregación de funciones	¿Reduce la probabilidad?	¿Reduce el impacto?	Probabilidad	Impacto	Nivel de Riesgo Residual	Tratamiento	Código de Plan de Acción	Plan de Acción	Responsable		
	Administrar Portal Web	R17	El Jefe de Unidad solicita actualizar información en el sitio web que incumpla con la Ley de Transparencia o la Ley de Protección de Datos Personales.	Desconocimiento de la Ley de Transparencia o la Ley de Protección de Datos Personales por parte del solicitante.	Personal	3	2	Moderado	C26	Se revisa la información a publicar en el sitio web. En caso transgredan la Ley de Transparencia o la Ley de Protección de Datos Personales, se rechaza.	4.2 Comprender las necesidades y expectativas de las partes interesadas, 5. Políticas, 15.2 Gestión de cambios de los servicios del proveedor.	APO 01.08 Mantener la conformidad con políticas y procedimientos APO 02.01 Entender la dirección de la empresa, APO 09.02 Catálogo de servicios permitidos por TI, APO 10.03 Gestionar las relaciones y contratos con el proveedor, APO 10.05 Monitorear el desempeño y cumplimiento del proveedor.	Jefe de Unidad de Tecnologías de Información	Detectivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	No	Si	3	1	Bajo	Evitar	N/A	N/A	N/A		

Figura 65. Evaluación de Riesgos y Controles según COBIT 5 y la NTP-ISO 27001:2014 GTI-09

Fuente: Elaboracion propia

RIESGOS Y CONTROLES DE LOS PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA AUTODEMA																																
Proceso		Riesgo				Evaluación inherente			Control														Evaluación residual			Planes de acción						
Macroproceso - Proceso	Subproceso	Código del Riesgo	Riesgo	Causa	Factor de Riesgo	Probabilidad	Impacto	Nivel de Riesgo Inherente	Código del Control	Descripción del Control	ISO 27001	COBIT 5.0	Responsable	Tipo	Ejecución	Documentación	Periodicidad	Responsabilidad	Segregación de funciones	¿Reduce la probabilidad?	¿Reduce el impacto?	Probabilidad	Impacto	Nivel de Riesgo Residual	Tratamiento	Código de Plan de Acción	Plan de Acción	Responsable				
	Asignar Equipo y Accesos a Nuevo Colaborador	R18	El equipo entregado no tiene correcto funcionamiento.	Cuando se realizó la compra del bien, no pasó por la Unidad de Tecnologías de Información para su aprobación.	Procesos internos	2	3	Moderado	C27	Encargado de Infraestructura de Tecnologías de Información hace la revisión del bien para corroborar su buen funcionamiento. En caso éste no funcione correctamente, lo devuelve a Patrimonio.	4.2 Comprendiendo las necesidades y expectativas de las partes interesadas, 5.3 Roles organizacionales, responsabilidades y autoridades, 7.5 Control de la información documentada.	APO 01.02 Establecer roles y responsabilidades, APO 02.0.1 Entender la dirección de la empresa, APO 02.02 Evaluar el entorno actual, las capacidades y el rendimiento, APO 04.02 Mantener un entendimiento del ambiente de la empresa, APO 09.02 Catálogo de servicios permitidos por TI.	Encargado de Infraestructura de Tecnologías de Información	Detectivo	Manual	Sin Documentar	Cada vez que ocurre	Asignada	Adecuada	No	Si	2	2	Bajo	Transferir	PA21	En caso el bien no funcione correctamente se devuelve a Patrimonio para que realice el procedimiento de cambio de bien con el proveedor o su entrega al Jefe de Unidad solicitante del Pedido de Compra.	Encargado de Patrimonio				

Figura 66. Evaluación de Riesgos y Controles según COBIT 5 y la NTP-ISO 27001:2014 GTI-10

Fuente: Elaboracion propia

CAPÍTULO IV:
RESULTADOS

Para validar la propuesta de mejora de procesos de tecnologías de información, se empleó una muestra no probabilística de tipo dirigida a los trabajadores de la AUTODEMA tomando en cuenta:

- Oficina o Unidad donde labora.
- Cargo desempeñado.

Como alternativas de respuesta se elaboró una escala que indique el grado de satisfacción del trabajador con el estado actual de la organización (AS – IS) y su estado deseado (TO – BE), las cuales están indicadas en la siguiente tabla:

Tabla 46. Escala de Satisfacción

Escala	**Grado de satisfacción**
0	Muy Bajo
1	Bajo
2	Medio
3	Alto
4	Muy Alto

Fuente: Elaboración propia

El total de trabajadores de la AUTODEMA encuestados según su Oficina o Unidad donde labora y su cargo desempeñado se encuentran detallados en la siguiente tabla:

Tabla 47. Trabajadores Encuestados Según Cargo y Oficina

	Directivo			Profesional				Técnico			Servicios	Total
	1	2	3	A	B	C	D	A	B	C		
Gerencia Ejecutiva	0	0	1	0	0	1	0	0	0	1	0	3
Órgano de Control Institucional	0	0	0	0	1	0	0	0	0	0	0	1

Oficina de Administración	0	1	0	0	0	1	0	0	0	0	0	2
Oficina de Asesoría Jurídica	0	1	0	0	2	0	0	0	0	1	2	6
Oficina de Planificación y Presupuesto	0	1	0	0	0	2	0	0	0	0	3	6
Gerencia de Gestión de Recursos Hídricos	0	0	0	0	0	0	0	0	0	0	0	0
Gerencia de Desarrollo del Proyecto Majes – Siguas II	0	0	0	1	0	0	0	0	0	1	0	2
Gerencia de Desarrollo Económico y Gestión Territorial	0	0	0	0	0	0	0	0	0	0	0	0
Unidad de Contabilidad	0	0	0	0	1	0	0	0	0	0	0	1
Unidad de Recursos Humanos	0	0	0	0	0	0	0	0	0	0	0	0
Unidad de Logística	0	0	0	0	0	1	0	0	0	0	2	3
Oficina de Promoción de la Inversión Privada	0	0	0	0	0	1	0	0	0	0	1	2
Total	0	3	1	1	4	6	0	0	0	3	8	26

Fuente: Elaboración propia

El modelo de las encuestas aplicadas a los trabajadores de la AUTODEMA acerca de la situación actual de la organización se encuentra en la siguiente figura:

AUTODEMA	ENCUESTA ACERCA DE LOS PROCESOS DE TECNOLOGÍAS DE INFORMACIÓN										N°:_____	
Oficina / Unidad:												
Cargo:	Directivo			Profesional				Técnico			Servicios	
	1	2	3	A	B	C	D	A	B	C		
ESTADO ACTUAL DE LA ORGANIZACIÓN AS – IS												
Responda todas las preguntas utilizando la escala propuesta de manera descendente, donde cuatro(4) indica el mayor puntaje y cero(0) el menor puntaje.												
ORGANIGRAMA												
1. ¿Con el organigrama actual de la AUTODEMA, cree que los procesos de los servicios informáticos son eficientes sabiendo que depende estructuralmente de la Unidad de Logística y Servicios? Indique en que grado.												
4	3			2				1			0	
LM-013	COPIAS DE SEGURIDAD – BACKUP											
2. Indique en que grado cree usted que se preserva la información de los diferentes sistemas de la AUTODEMA.												
4	3			2				1			0	
3. ¿Cree que las copias de seguridad de los sistemas de la AUTODEMA son almacenados correctamente? Indique el grado de confianza que tiene de su almacenamiento.												
4	3			2				1			0	
LM-014	SOPORTE INFORMÁTICO											
4. ¿Cuál es su nivel de satisfacción con el soporte informático que se le brinda?												
4	3			2				1			0	
5. ¿En qué grado influye el procedimiento de soporte informático en el desarrollo de sus tareas habituales?												
4	3			2				1			0	
LM-015	SEGURIDAD, ACCESIBILIDAD A USUARIOS, REPORTE MENSUAL											
6. ¿Cuál es su nivel de satisfacción respecto a la gestión y seguridad de usuarios y correos corporativos?												
4	3			2				1			0	
7. ¿En qué grado tiene conocimiento acerca de los reportes mensuales realizados por el área de servicios informáticos?												
4	3			2				1			0	
LM-016	ADMINISTRADOR SISTEMAS S.I.G.A. Y S.I.A.F.											
8. ¿Cuál es su nivel de satisfacción respecto al soporte realizado por servicios informáticos de los sistemas S.I.G.A. y S.I.A.F.?												
4	3			2				1			0	
9. ¿Qué tan eficiente es la labor de servicios informáticos en cuanto a la creación de ítems / usuarios?												
4	3			2				1			0	
LM-017	SUPERVISIÓN DE SERVICIOS DE SISTEMAS TERCERIZADO											
10. ¿En qué grado se cumplen los términos de referencia con el servicio brindado por un tercero del área de servicios informáticos?												
4	3			2				1			0	
LM-018	CUMPLIMIENTO DE DIRECTIVA DE SEGURIDAD INFORMÁTICA											
11. ¿En qué grado tiene conocimiento de las directivas de seguridad de la información?												
4	3			2				1			0	
12. ¿En qué grado cree que las directivas de seguridad de la información se encuentran alineadas al negocio?												
4	3			2				1			0	

Figura 67. Modelo de Encuesta Estado Actual de la Organización AS -IS
Fuente: Elaboración propia

El modelo de las encuestas aplicadas a los trabajadores de la AUTODEMA acerca de la situación deseada de la organización se encuentra en la siguiente figura:

	ENCUESTA ACERCA DE LOS PROCESOS DE TECNOLOGÍAS DE INFORMACIÓN										N°:_____
Oficina / Unidad:											
Cargo:	Directivo			Profesional				Técnico			Servicios
	1	2	3	A	B	C	D	A	B	C	
ESTADO DESEADO DE LA ORGANIZACIÓN TO - BE											
Responda todas las preguntas utilizando la escala propuesta de manera descendente, donde cuatro(4) indica el mayor puntaje y cero(0) el menor puntaje.											
ORGANIGRAMA											
1. Si servicios informáticos se disgregaría en una Unidad, indique en que nivel mejoran los procesos de la Unidad de Tecnologías de la Información											
4	3			2				1			0
GTI-01	REALIZAR COPIAS DE SEGURIDAD – BACKUP										
2. ¿En qué grado cree usted que el Plan Anual de Copias de Seguridad apoya a la planificación, ejecución y control de los respaldos de la información de los sistemas de la AUTODEMA?											
4	3			2				1			0
3. ¿En que grado cree usted que la información respaldada se encontraría disponible, íntegra y privada?											
4	3			2				1			0
GTI-02	REALIZAR SOPORTE INFORMÁTICO										
4. ¿Qué nivel de satisfacción tendría usted si su requerimiento ha sido priorizado según la gravedad del incidente y los requerimientos en espera?											
4	3			2				1			0
5. ¿En qué grado cree usted que tener una base de conocimiento apoya a la solución de requerimientos de soporte informático?											
4	3			2				1			0
GTI-03	REALIZAR INFORME MENSUAL										
6. ¿En qué grado se cumplirían las metas de Tecnologías de Información conforme al reporte mensual elaborado por la Unidad?											
4	3			2				1			0
GTI-04	ADMINISTRAR SISTEMAS S.I.G.A. Y S.I.A.F.										
7. ¿En qué grado estaría satisfecho con el procedimiento de creación de ítems / usuarios de los sistemas S.I.G.A. y S.I.A.F.?											
4	3			2				1			0
8. ¿Cuál es su nivel de aceptación conforme a la labor de la Unidad de Tecnologías de la Información en cuanto a la solución de incidentes de los sistemas S.I.G.A. y S.I.A.F. con el apoyo del MEF?											
4	3			2				1			0
GTI-05	SUPERVISAR SERVICIOS TERCERIZADOS										
9. ¿En que grado cree usted que los servicios tercerizados de Tecnologías de la Información deben ser monitoreados por la Unidad y no por la Unidad de Logística y Servicios?											
4	3			2				1			0
10. ¿Cuál es su nivel de satisfacción conforme a que la Unidad de Tecnologías de Información realice los términos de referencia que incluyan Tecnología?											
4	3			2				1			0
GTI-06	SUPERVISAR CUMPLIMIENTO DE DIRECTIVAS DE SEGURIDAD DE LA INFORMACIÓN										
¿En qué grado cree usted que las Directivas de Seguridad de la Información deberían ser comunicadas a la Gerencia Ejecutiva?											
4	3			2				1			0
GTI-07	GESTIONAR LA RECEPCION DE BIENES O SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN										
11. ¿En qué grado cree usted que la Unidad de Tecnologías de la Información debe revisar los bienes o servicios para dar visto bueno a una adquisición de cualquier Unidad respecto a las Tecnologías de Información?											
4	3			2				1			0
GTI-08	LICENCIAMIENTO DE SOFTWARE										
12. ¿En qué grado cree usted que la Unidad de Tecnologías de la Información lleve el control de las licencias que se instalan en los equipos de cómputo de la AUTODEMA?											
4	3			2				1			0
GTI-09	ADMINISTRAR PORTAL WEB										
13. ¿Está usted de acuerdo con que la Unidad de Tecnologías de Información debe aprobar las solicitudes de actualización de información del sitio web?											
4	3			2				1			0
GTI-10	ASIGNAR EQUIPOS Y ACCESOS A NUEVO COLABORADOR										
14. ¿Cuál es su nivel de satisfacción respecto a que la Unidad de Tecnologías de Información revise los equipos de Tecnologías de la Información cuando es asignado a un trabajador?											
4	3			2				1			0

Figura 68. Modelo de Encuesta Estado Deseado de la Organización TO-BE
Fuente: Elaboración propia

4.1 RESULTADOS DE LA ENCUESTA DEL ESTADO ACTUAL DE LA ORGANIZACIÓN

1. ¿Con el organigrama actual de la AUTODEMA, cree que los procesos de los servicios informáticos son eficientes sabiendo que depende estructuralmente de la Unidad de Logística y Servicios? Indique en que grado.

Tabla 48. Respuesta a Pregunta N°1

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	1
1	Bajo	7
2	Medio	13
3	Alto	3
4	Muy Alto	2

Fuente: Elaboración propia

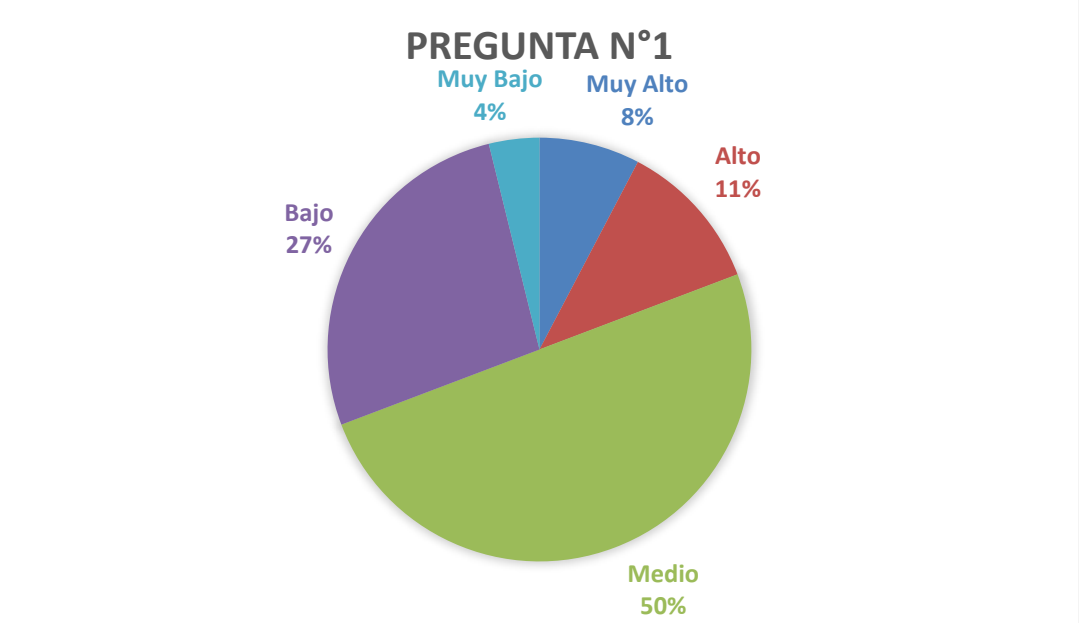


Figura 69. Gráfico Circular de la Pregunta N°1

Fuente: Elaboración propia

Interpretación

La mitad de los encuestados opina que los procesos de Servicios Informáticos son eficientes aunque ésta área depende de la Unidad de Logística y Servicios, por otro lado, existe un márgen considerable (27% de entrevistados) que opinan que los procesos de Servicios Informáticos no son eficientes.

2. Indique en que grado cree usted que se preserva la información de los diferentes sistemas de la AUTODEMA.

Tabla 49. Respuestas a Pregunta N°2

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	0
1	Bajo	10
2	Medio	9
3	Alto	6
4	Muy Alto	1

Fuente: Elaboración propia

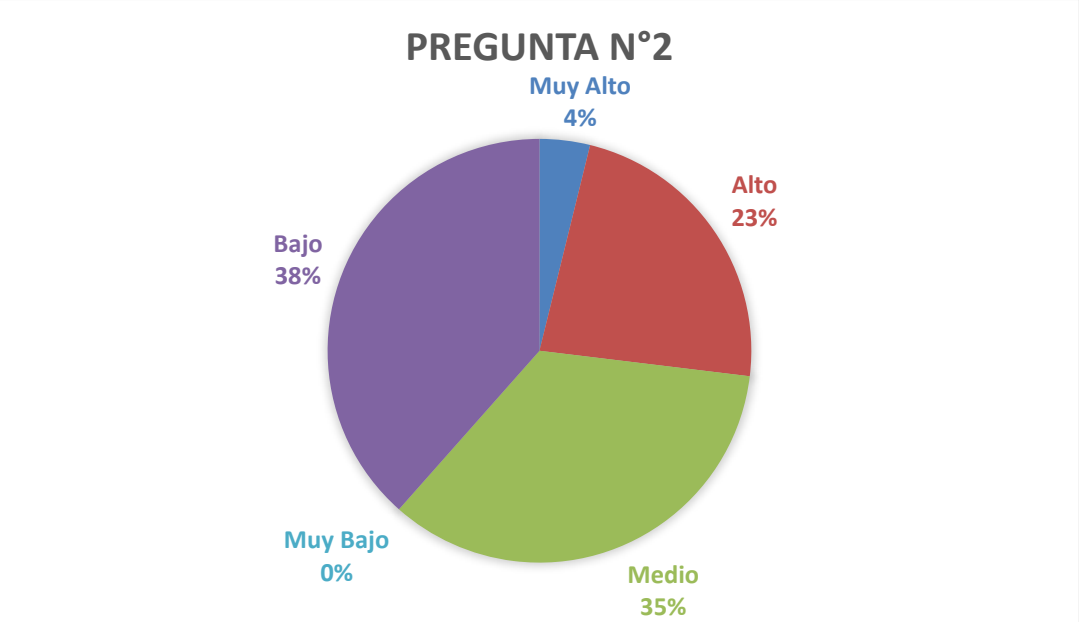


Figura 70. Gráfico Circular de la Pregunta N°2

Fuente: Elaboración propia

Interpretación

Los encuestados opinan que la información de los diferentes sistemas de la Autoridad Autónoma de Majes, se preserva en un grado medianamente bajo, sin embargo hay una pequeña porción que opina que su almacenamiento es alto.

3. ¿Cree que las copias de seguridad de los sistemas de la AUTODEMA son almacenados correctamente? Indique el grado de confianza que tiene de su almacenamiento.

Tabla 50. Respuesta a Pregunta N°3

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	0
1	Bajo	4
2	Medio	8
3	Alto	10
4	Muy Alto	3

Fuente: Elaboración propia

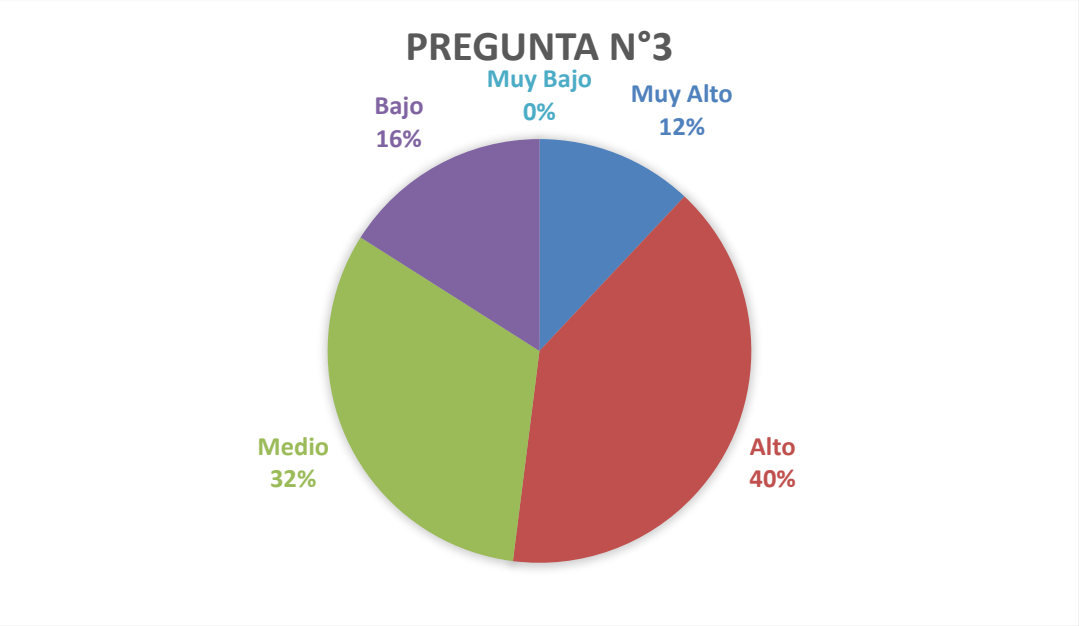


Figura 71. Gráfico Circular de la Pregunta N°3

Fuente: Elaboración propia

Interpretación

Un poco más de la mitad de los trabajadores de la Autoridad Autónoma de Majes creen que las copias de seguridad de los sistemas de la organización son medianamente alto almacenados correctamente, sin embargo, existe un margen considerable que opina que las copias de seguridad no son almacenadas correctamente.

4. ¿Cuál es su nivel de satisfacción con el soporte informático que se le brinda?

Tabla 51. Respuestas a Pregunta N°4

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	0
1	Bajo	2
2	Medio	4
3	Alto	16
4	Muy Alto	4

Fuente: Elaboración propia

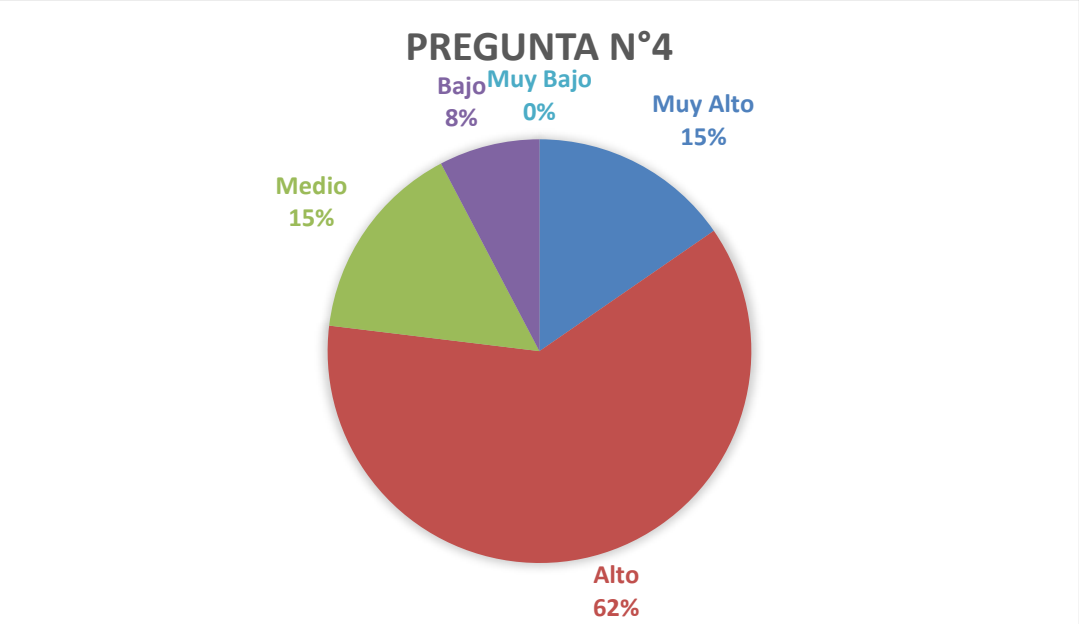


Figura 72. Gráfico Circular de la Pregunta N°4

Fuente: Elaboración propia

Interpretación

En general, los trabajadores de la AUTODEMA se encuentran satisfechos en un grado medianamente alto con el soporte informático que se les brinda.

5. ¿En qué grado influye el procedimiento de soporte informático en el desarrollo de sus tareas habituales?

Tabla 52. Respuestas a Pregunta N°5

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	1
1	Bajo	1
2	Medio	8
3	Alto	8
4	Muy Alto	8

Fuente: Elaboración propia

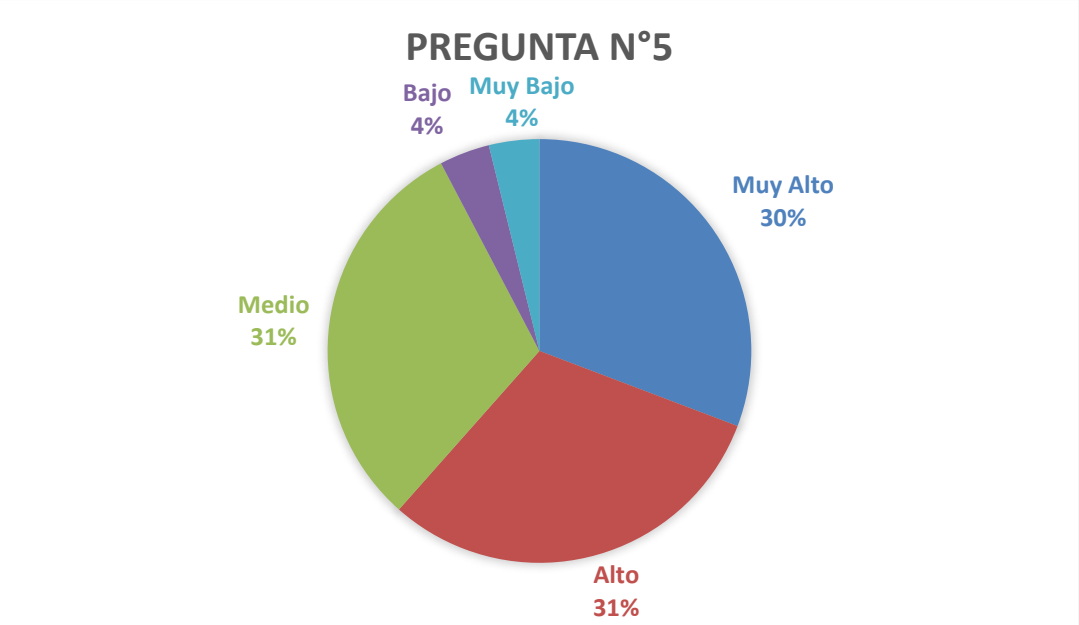


Figura 73. Gráfico Circular de la Pregunta N°5

Fuente: Elaboración propia

Interpretación

Existen similitudes en el grado de satisfacción de los encuestados acerca de la influencia del soporte informático brindado durante el desarrollo de sus actividades habituales, con una tendencia mediana a muy alta.

6. ¿Cuál es su nivel de satisfacción respecto a la gestión y seguridad de usuarios y correos corporativos?

Tabla 53. Respuestas a Pregunta N°6

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	2
1	Bajo	4
2	Medio	9
3	Alto	9
4	Muy Alto	2

Fuente: Elaboración propia

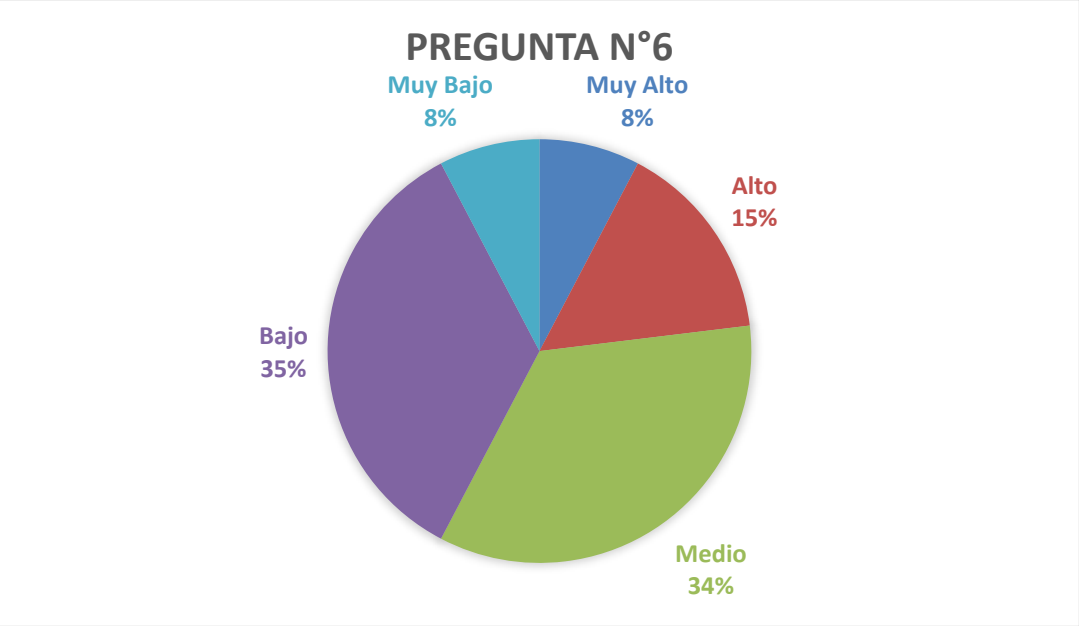


Figura 74. Gráfico Circular de la Pregunta N°6

Fuente: Elaboración propia

Interpretación

El nivel de satisfacción respecto a la gestión y seguridad de usuarios y correos corporativos es discrepante, ya que, existe un tercio de los encuestados que opina que el nivel es bajo, mientras que un tercio opina que es medio y un poco menos de un tercio, alto a muy alto.

7. ¿En qué grado tiene conocimiento acerca de los reportes mensuales realizados por el área de servicios informáticos?

Tabla 54. Respuestas a Pregunta N°7

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	5
1	Bajo	3
2	Medio	15
3	Alto	2
4	Muy Alto	1

Fuente: Elaboración propia

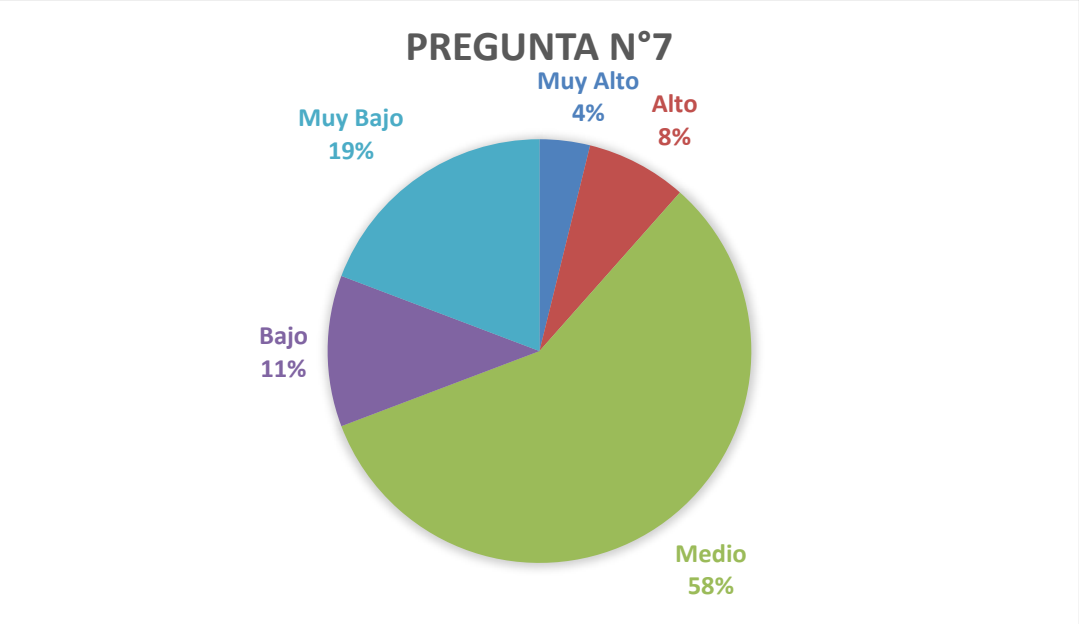


Figura 75. Gráfico Circular de la Pregunta N°7

Fuente: Elaboración propia

Interpretación

El personal de la AUTODEMA tiene mediano conocimiento de los reportes mensuales del área de Servicios Informáticos con más de la mitad de encuestados, teniendo un pequeño porcentaje de rezagados que su conocimiento es bajo.

8. ¿Cuál es su nivel de satisfacción respecto al soporte realizado por servicios informáticos de los sistemas S.I.G.A. y S.I.A.F.?

Tabla 55. Respuestas a Pregunta N°8

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	2
1	Bajo	1
2	Medio	10
3	Alto	11
4	Muy Alto	2

Fuente: Elaboración propia

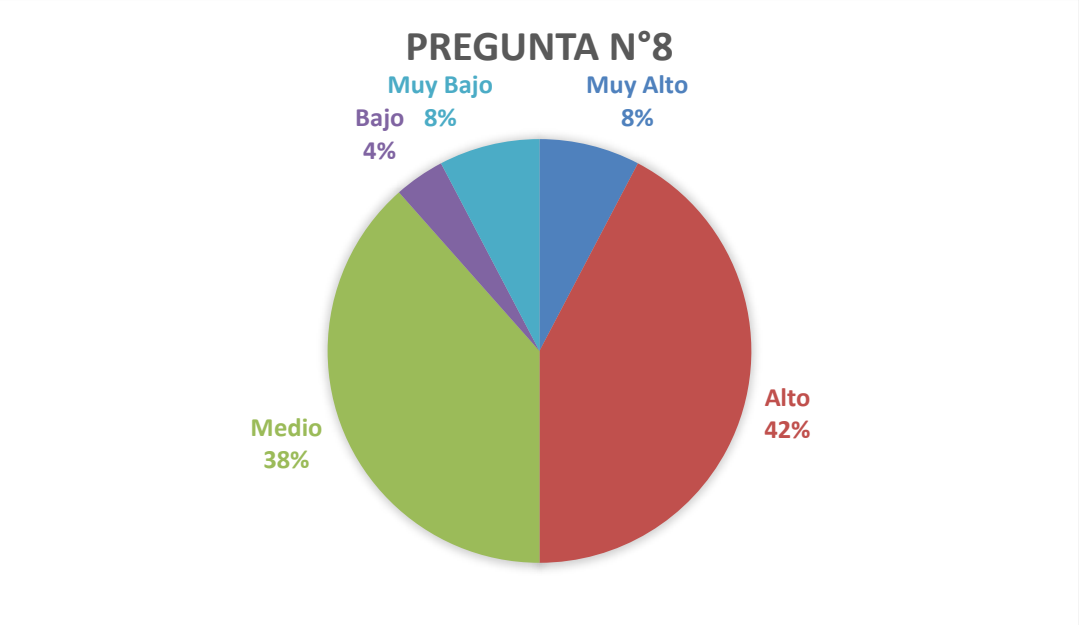


Figura 76. Gráfico Circular de la Pregunta N°8

Fuente: Elaboración propia

Interpretación

Respecto a los sistemas S.I.G.A. y S.I.A.F., los encuestados se encuentran medianamente alto satisfechos con el soporte realizado por Servicios Informáticos.

9. ¿Qué tan eficiente es la labor de servicios informáticos en cuanto a la creación de ítems / usuarios?

Tabla 56. Respuestas a Pregunta N°9

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	0
1	Bajo	5
2	Medio	7
3	Alto	7
4	Muy Alto	7

Fuente: Elaboración propia

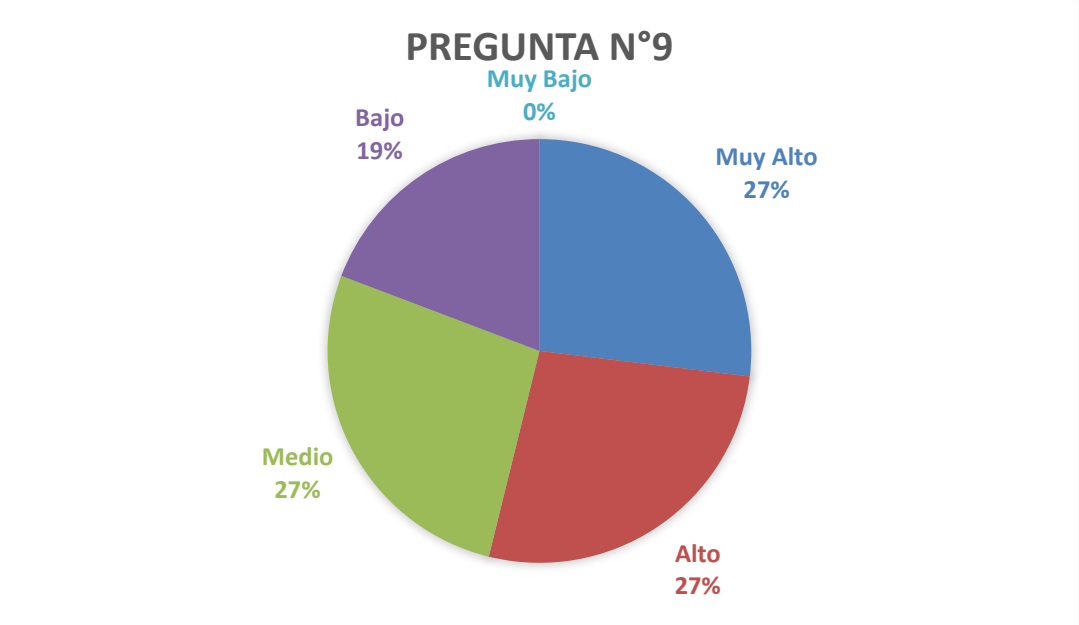


Figura 77. Gráfico Circular de la Pregunta N°9

Fuente: Elaboración propia

Interpretación

La mayoría de los encuestados de la Autoridad Autónoma de Majes aprueban el trabajo de Servicios Informáticos como nexo en la creación de ítems y/o usuarios de los mismos con un grado de medio a muy alto.

10. ¿En qué grado se cumplen los términos de referencia con el servicio brindado por un tercero del área de servicios informáticos?

Tabla 57. Respuestas a Pregunta N°10

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	2
1	Bajo	1
2	Medio	10
3	Alto	10
4	Muy Alto	3

Fuente: Elaboración propia

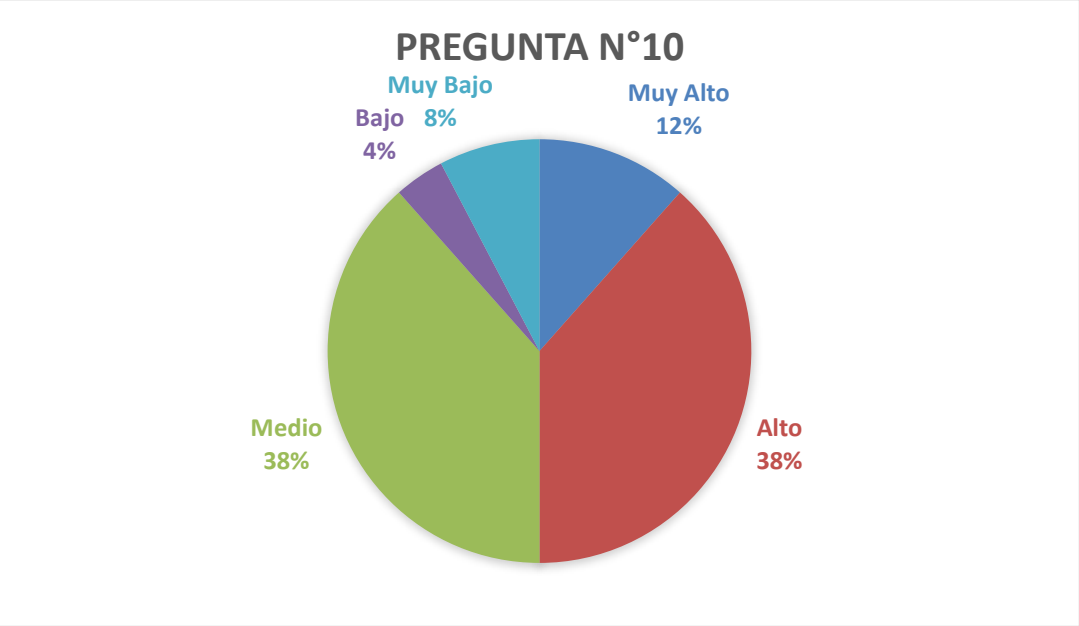


Figura 78. Gráfico Circular de la Pregunta N°10

Fuente: Elaboración propia

Interpretación

Los encuestados de la AUTODEMA se encuentran medianamente alto satisfechos con los servicios brindados por terceros que involucren a Servicios Informáticos.

11. ¿En qué grado tiene conocimiento de las directivas de seguridad de la información?

Tabla 58. Respuestas a Pregunta N°11

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	3
1	Bajo	6
2	Medio	11
3	Alto	5
4	Muy Alto	1

Fuente: Elaboración propia

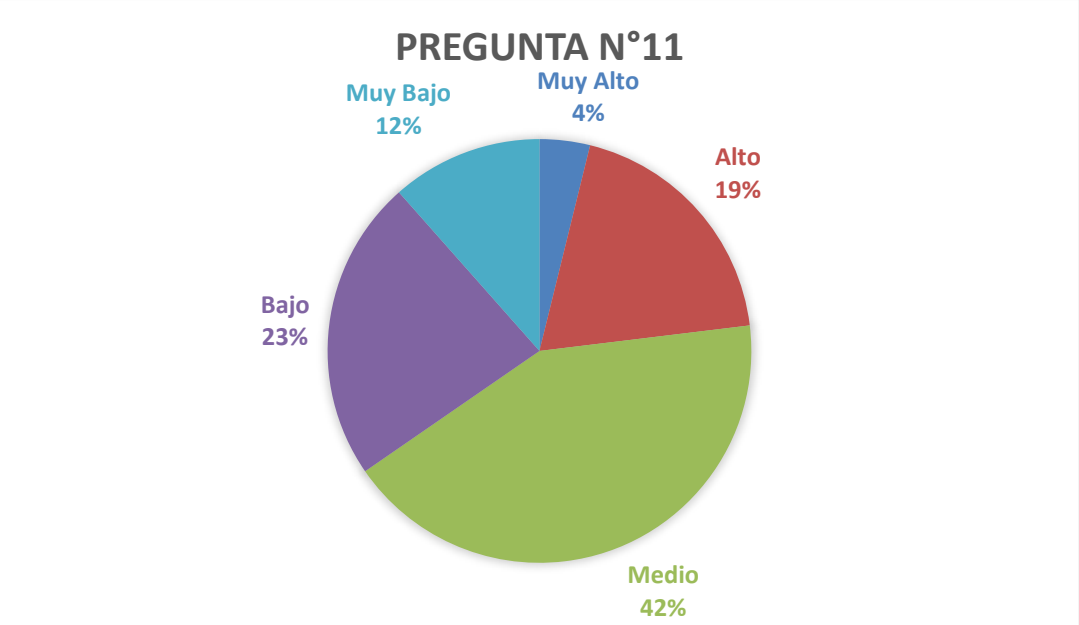


Figura 79. Gráfico Circular de la Pregunta N°11

Fuente: Elaboración propia

Interpretación

Conforme a las directivas de seguridad de la información, el personal de la AUTODEMA tiene opiniones divididas en su grado, siendo en su mayoría medio.

12. ¿En qué grado cree que las directivas de seguridad de la información se encuentran alineadas al negocio?

Tabla 59. Respuestas a Pregunta N°12

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	4
1	Bajo	4
2	Medio	11
3	Alto	6
4	Muy Alto	1

Fuente: Elaboración propia

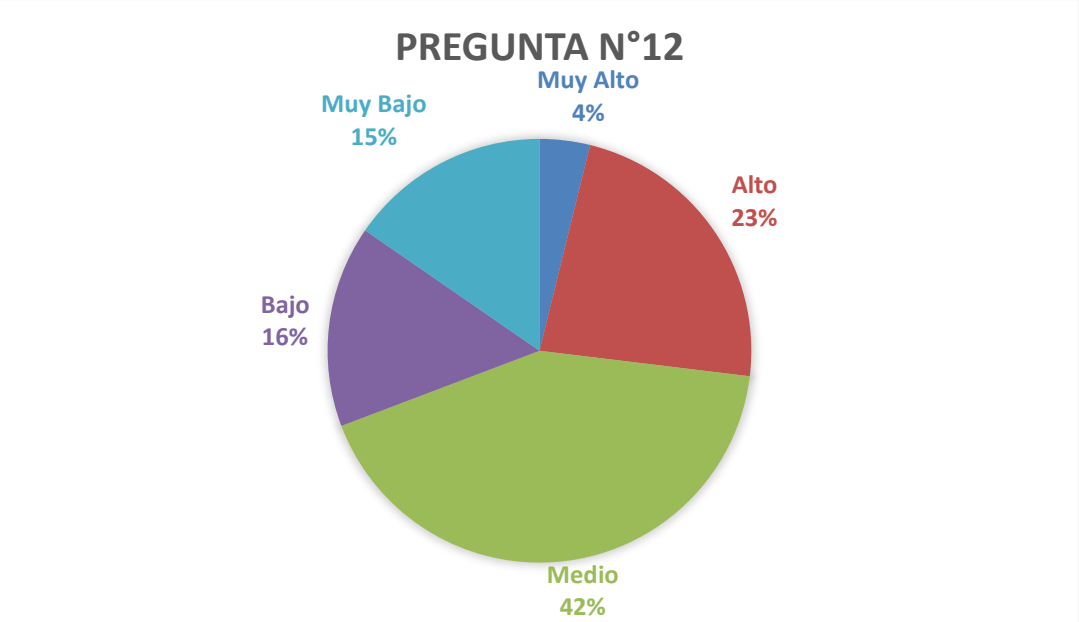


Figura 80. Gráfico Circular de la Pregunta N°12

Fuente: Elaboración propia

Interpretación

Los encuestados opinan que las directivas de seguridad de la información se encuentran medianamente alineadas al negocio.

Un resumen general de la encuesta del estado actual de la organización se encuentra en la siguiente tabla:

Tabla 60. Resumen de Respuestas de Encuesta de Estado Actual de la Organización

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	17
1	Bajo	40
2	Medio	104
3	Alto	88
4	Muy Alto	34

Fuente: Elaboración propia

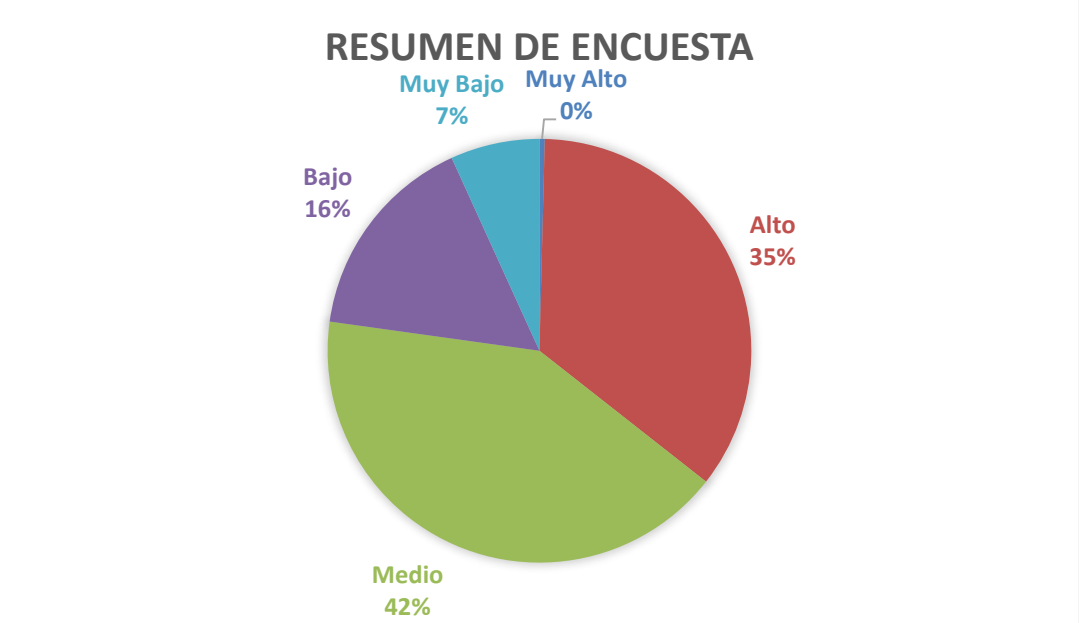


Figura 81. Gráfico Circular Resumen de Encuestas de Estado Actual de la Organización
Fuente: Elaboración propia

4.2 RESULTADOS DE LA ENCUESTA DEL ESTADO DESEADO DE LA ORGANIZACIÓN

1. ¿Si servicios informáticos se disgregaría en una Unidad, indique en que nivel mejoran los procesos de la Unidad de Tecnologías de la Información

Tabla 61. Respuestas a Pregunta N°1

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	0
1	Bajo	1
2	Medio	2
3	Alto	14
4	Muy Alto	9

Fuente: Elaboración propia

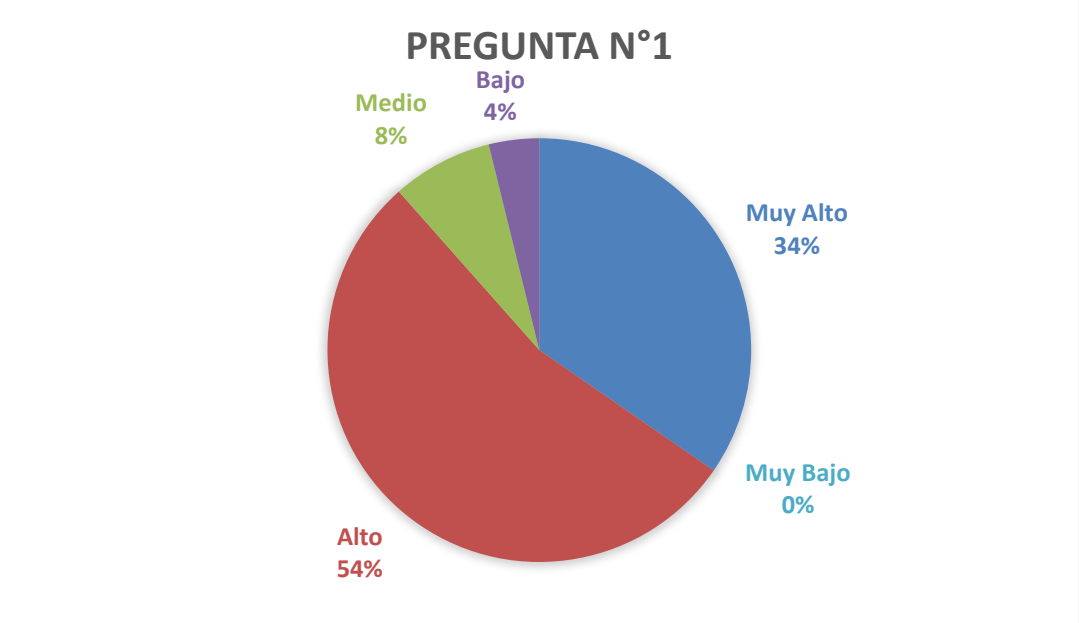


Figura 82. Gráfico Circular de la Pregunta N°1

Fuente: Elaboración propia

Interpretación

Los trabajadores de la Autoridad Autónoma de Majes opinan en su mayoría que los procesos mejorarían si Servicios Informáticos se disgrega en un Unidad autónoma.

2. ¿En qué grado cree usted que el Plan Anual de Copias de Seguridad apoya a la planificación, ejecución y control de los respaldos de la información de los sistemas de la AUTODEMA?

Tabla 62. Respuestas a Pregunta N°2

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	0
1	Bajo	2
2	Medio	2
3	Alto	14
4	Muy Alto	7

Fuente: Elaboración propia

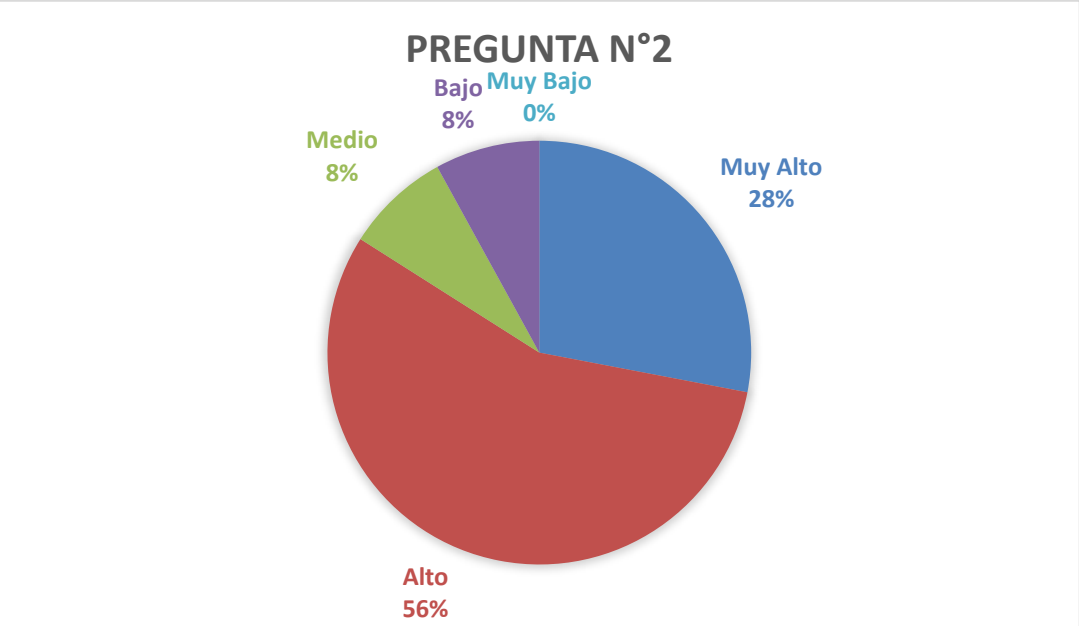


Figura 83. Gráfico Circular de la Pregunta N°2

Fuente: Elaboración propia

Interpretación

La mayoría de los encuestados opinan que la planificación, ejecución y control de los respaldos de información, mejorarían con un Plan Anual de Copias de Seguridad.

3. ¿En que grado cree usted que la información respaldada se encontraría disponible, íntegra y privada?

Tabla 63. Respuestas a Pregunta N°3

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	0
1	Bajo	3
2	Medio	7
3	Alto	11
4	Muy Alto	6

Fuente: Elaboración propia

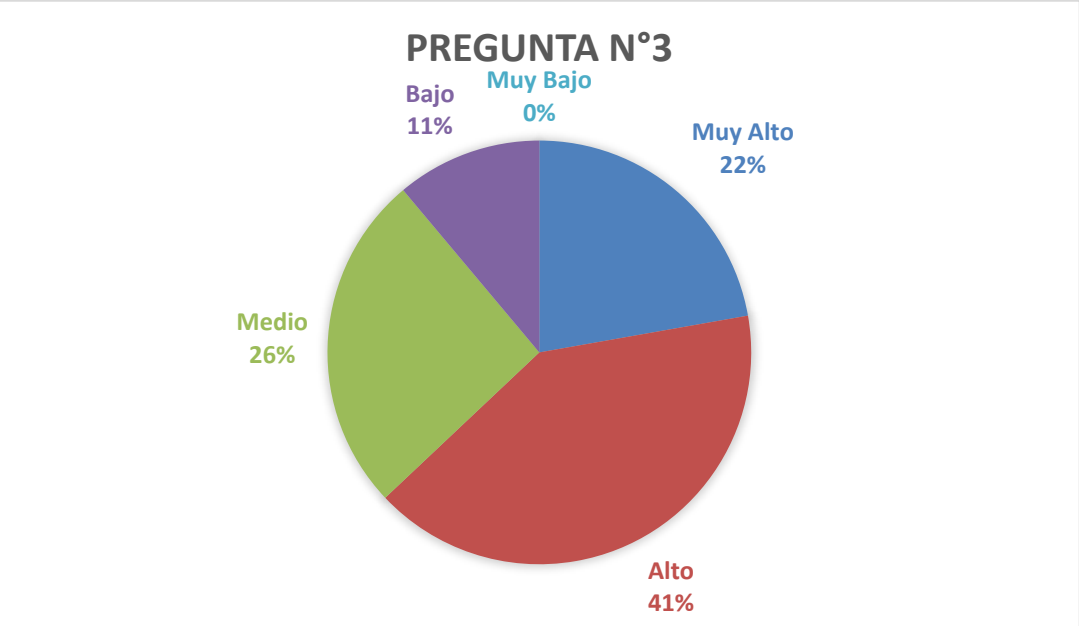


Figura 84. Gráfico Circular de la Pregunta N°3

Fuente: Elaboración propia

Interpretación

La mayoría de los encuestados de la Autoridad Autónoma de Majes opina que la información se mantendría disponible, íntegra y privada.

4. ¿Qué nivel de satisfacción tendría usted si su requerimiento ha sido priorizado según la gravedad del incidente y los requerimientos en espera?

Tabla 64. Respuestas a Pregunta N°4

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	0
1	Bajo	1
2	Medio	3
3	Alto	11
4	Muy Alto	11

Fuente: Elaboración propia

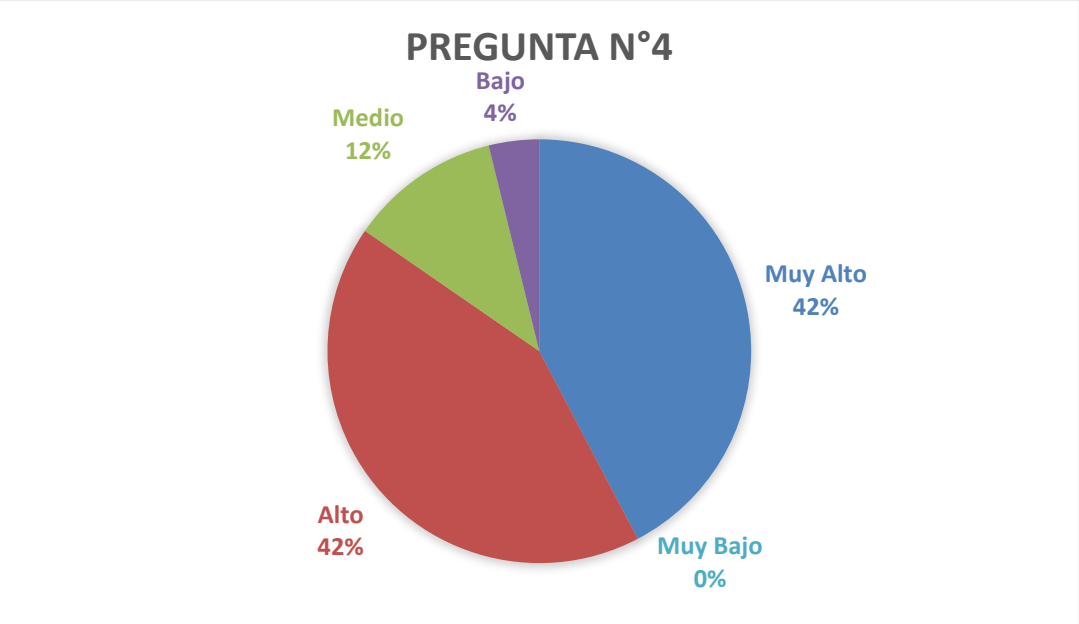


Figura 85. Gráfico Circular de la Pregunta N°4

Fuente: Elaboración propia

Interpretación

La priorización de requerimientos es satisfactoria de gran manera por los encuestados con más del 80%.

5. ¿En qué grado cree usted que tener una base de conocimiento apoya a la solución de requerimientos de soporte informático?

Tabla 65. Respuestas a Pregunta N°5

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	0
1	Bajo	1
2	Medio	5
3	Alto	11
4	Muy Alto	9

Fuente: Elaboración propia

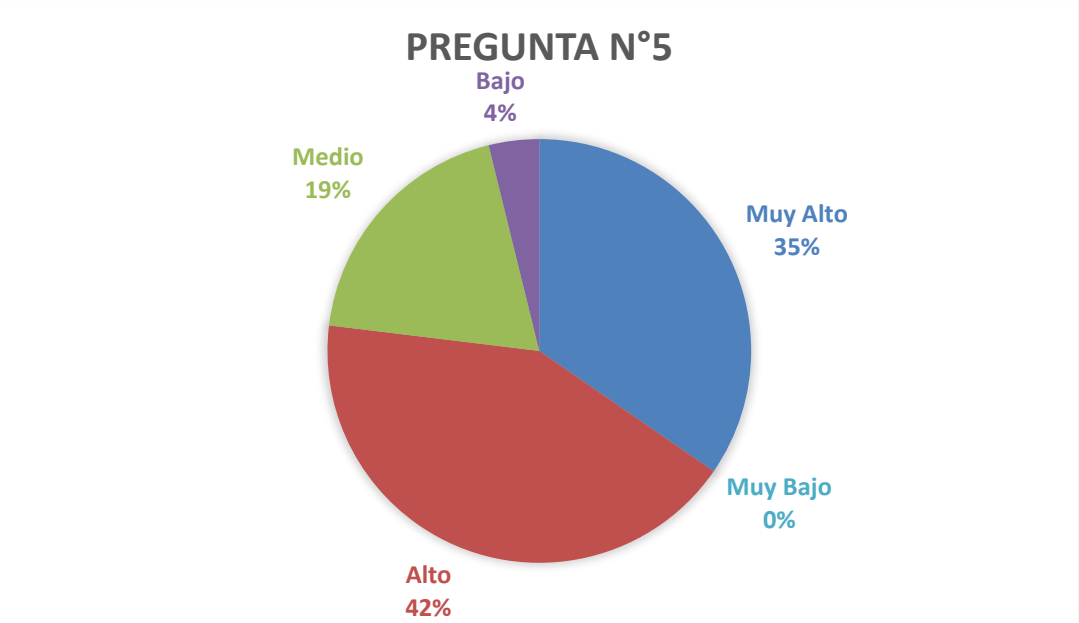


Figura 86. Gráfico Circular de la Pregunta N°5

Fuente: Elaboración propia

Interpretación

La creación de una base de conocimientos, también aportaría a la resolución de requerimientos de soporte informático según los encuestados de la Autoridad Autónoma de Majes.

6. ¿En qué grado se cumplirían las metas de Tecnologías de Información conforme al reporte mensual elaborado por la Unidad?

Tabla 66. Respuestas a Pregunta N°6

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	0
1	Bajo	1
2	Medio	7
3	Alto	18
4	Muy Alto	2

Fuente: Elaboración propia

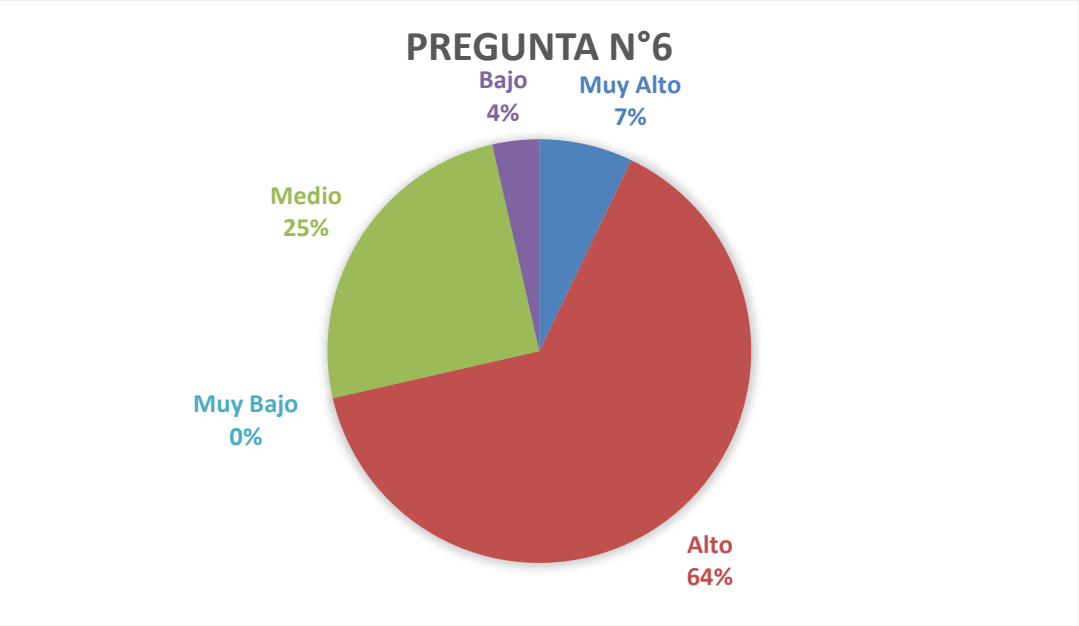


Figura 87. Gráfico Circular de la Pregunta N°6

Fuente: Elaboración propia

Intepretación

Los encuestados opinan en su mayoría que las metas de tecnologías de información se cumplirían con la elaboración de un reporte mensual con lo realizado.

7. ¿En qué grado estaría satisfecho con el procedimiento de creación de ítems / usuarios de los sistemas S.I.G.A. y S.I.A.F.?

Tabla 67. Respuestas a Pregunta N°7

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	1
1	Bajo	1
2	Medio	5
3	Alto	14
4	Muy Alto	5

Fuente: Elaboración propia

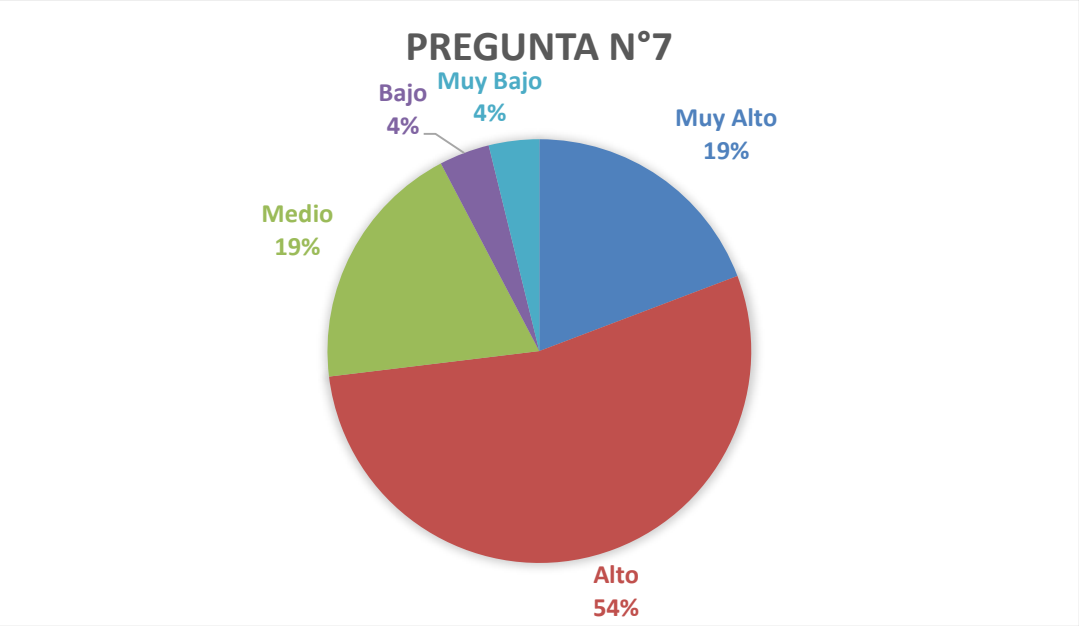


Figura 88. Gráfico Circular de la Pregunta N°7

Fuente: Elaboración propia

Interpretación

Los encuestados opinan que con la nueva definición del procedimiento de creación de ítems y usuarios, su nivel de satisfacción sería alto en su mayoría.

8. ¿Cuál es su nivel de aceptación conforme a la labor de la Unidad de Tecnologías de la Información en cuanto a la solución de incidentes de los sistemas S.I.G.A. y S.I.A.F. con el apoyo del MEF?

Tabla 68. Respuestas a Pregunta N°8

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	1
1	Bajo	1
2	Medio	5
3	Alto	13
4	Muy Alto	6

Fuente: Elaboración propia

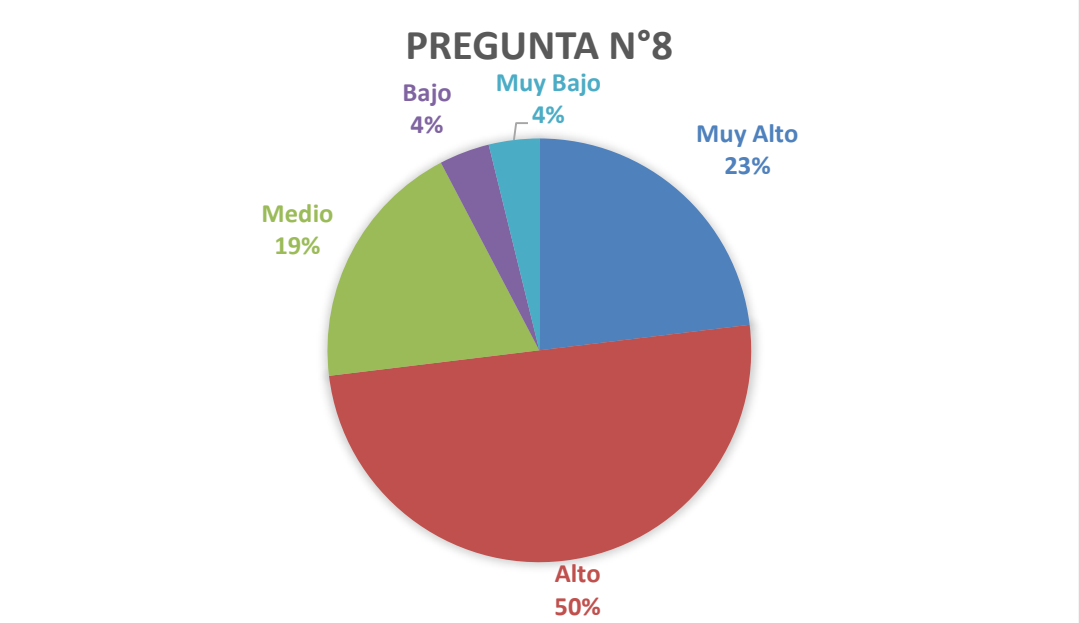


Figura 89. Gráfico Circular de la Pregunta N°8

Fuente: Elaboración propia

Interpretación

La mayoría de los encuestados opina que la labor de la Unidad de Tecnologías de Información en cuanto a la solución de incidentes del S.I.G.A. y S.I.A.F. con apoyo del MEF, es alta.

9. ¿En que grado cree usted que los servicios tercerizados de Tecnologías de la Información deben ser monitoreados por la Unidad y no por la Unidad de Logística y Servicios?

Tabla 69. Respuestas a Pregunta N°9

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	0
1	Bajo	1
2	Medio	3
3	Alto	9
4	Muy Alto	13

Fuente: Elaboración propia

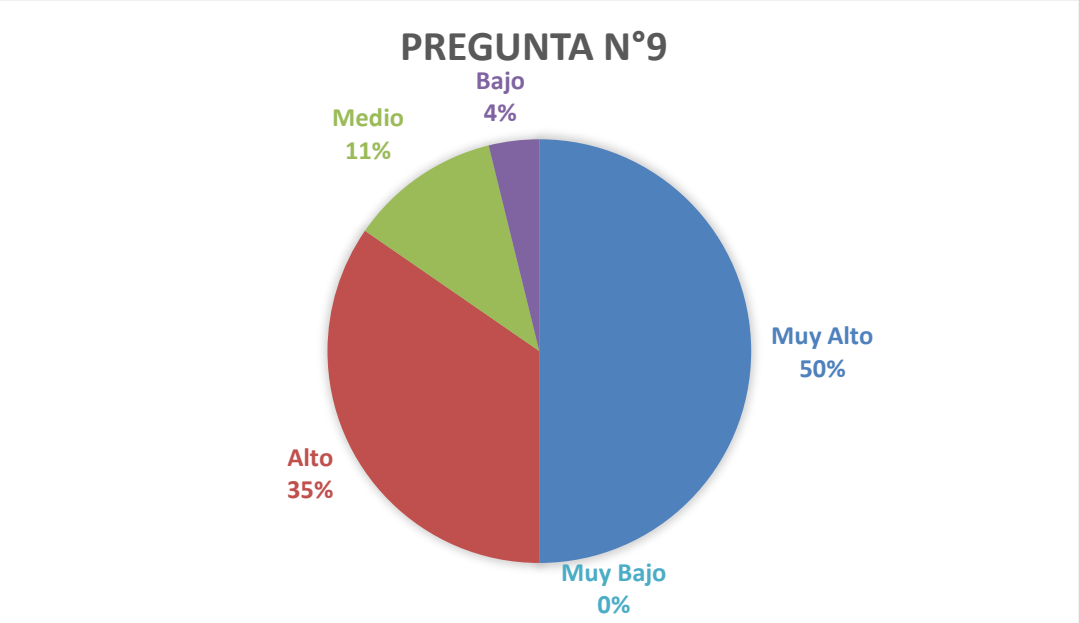


Figura 90. Gráfico Circular de la Pregunta N°9

Fuente: Elaboración propia

Interpretación

En su mayoría, los trabajadores de la AUTODEMA opinan que los servicios tercerizados deben ser monitoreados siempre por la Unidad de Tecnologías de la Información siempre y cuando correspondan.

10. ¿Cuál es su nivel de satisfacción conforme a que la Unidad de Tecnologías de Información realice los términos de referencia que incluyan Tecnología?

Tabla 70. Respuestas a Pregunta N°10

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	0
1	Bajo	1
2	Medio	3
3	Alto	9
4	Muy Alto	13

Fuente: Elaboración propia

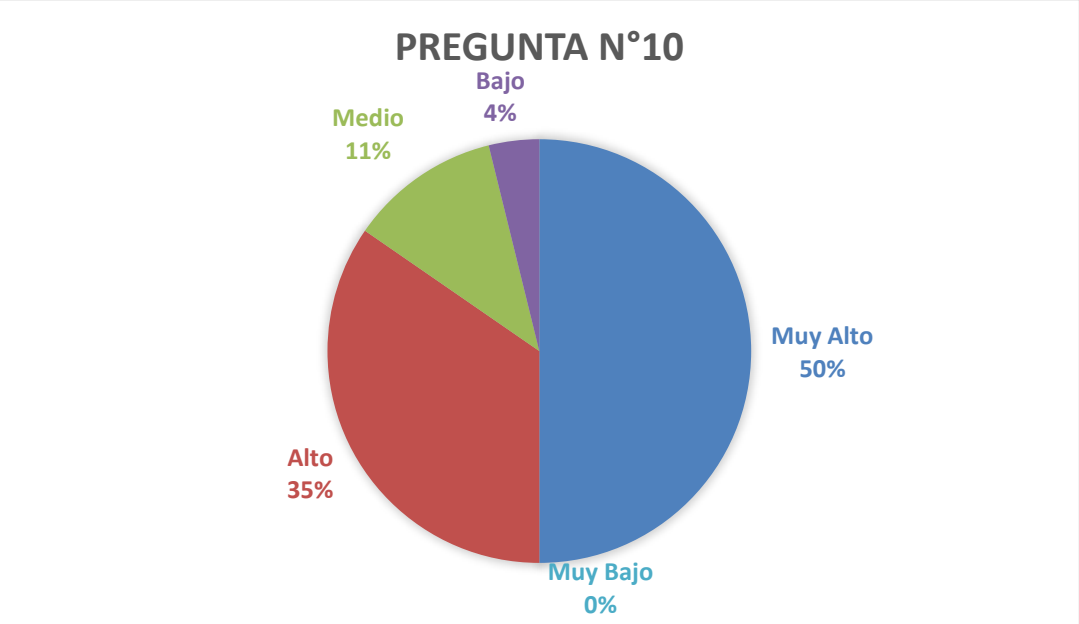


Figura 91. Gráfico Circular de la Pregunta N°10

Fuente: Elaboración propia

Interpretación

Los trabajadores de la Autoridad Autónoma de Majes opinan satisfactoriamente que la Unidad de Tecnologías de Información elabore los términos de referencia que incluyan tecnología, así como que se revisen los bienes o servicios para dar visto bueno a todo lo que corresponda a tecnología.

11. ¿ En qué grado cree usted que las Directivas de Seguridad de la Información deberían ser comunicadas a la Gerencia Ejecutiva?

Tabla 71. Respuestas a Pregunta N°11

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	0
1	Bajo	0
2	Medio	5
3	Alto	9
4	Muy Alto	12

Fuente: Elaboración propia

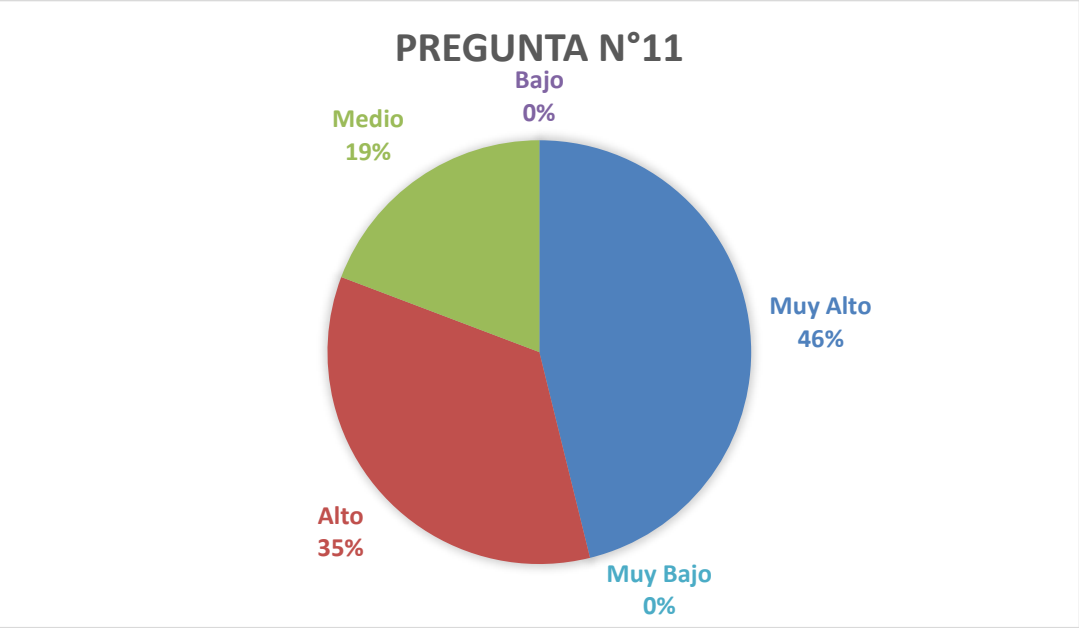


Figura 92. Gráfico Circular de la Pregunta N°11

Fuente: Elaboración propia

Interpretación

Los encuestados creen en un grado muy alto que todas las Directivas de Seguridad de la Información deberían ser comunicadas a la Gerencia Ejecutiva.

12. ¿En qué grado cree usted que la Unidad de Tecnologías de la Información debe revisar los bienes o servicios para dar visto bueno a una adquisición de cualquier Unidad respecto a las Tecnologías de Información?

Tabla 72. Respuestas a Pregunta N°12

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	0
1	Bajo	1
2	Medio	3
3	Alto	14
4	Muy Alto	8

Fuente: Elaboración propia

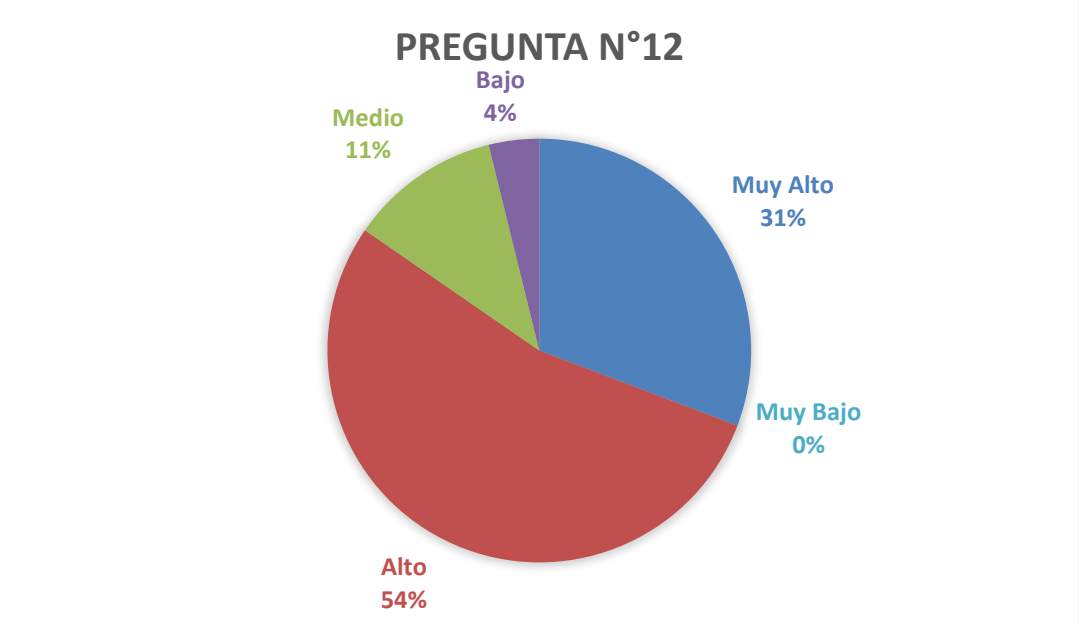


Figura 93. Gráfico Circular de la Pregunta N°12

Fuente: Elaboración propia

Interpretación

Los encuestados opinan en un grado alto que todos los bienes deben recibir el visto bueno cuando se realizan adquisiciones respecto a las Tecnologías de la Información.

13. ¿ En qué grado cree usted que la Unidad de Tecnologías de la Información lleve el control de las licencias que se instalan en los equipos de cómputo de la AUTODEMA?

Tabla 73. Respuestas a Pregunta N°13

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	0
1	Bajo	0
2	Medio	4
3	Alto	5
4	Muy Alto	17

Fuente: Elaboración propia

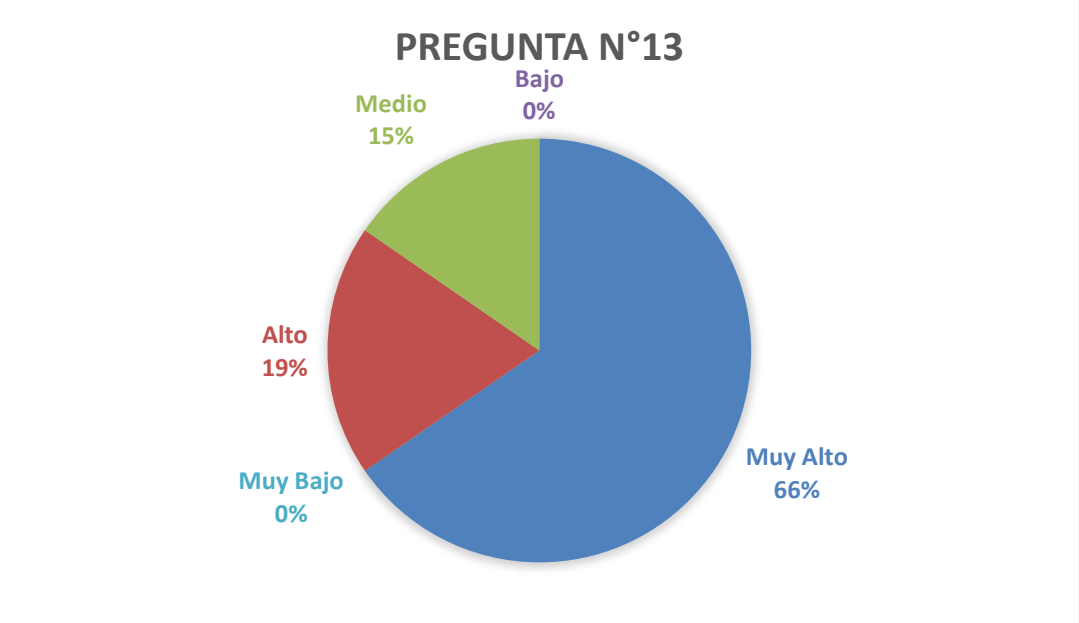


Figura 94. Gráfico Circular de la Pregunta N°13

Fuente: Elaboración propia

Interpretación

Los trabajadores de la AUTODEMA opinan en un grado muy alto en su mayoría, que las licencias instaladas en los equipos de cómputo seaan gestionadas por la Unidad de Tecnologías de la Información.

14. ¿Está usted de acuerdo con que la Unidad de Tecnologías de Información debe aprobar las solicitudes de actualización de información del sitio web?

Tabla 74. Respuestas a Pregunta N°14

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	0
1	Bajo	2
2	Medio	6
3	Alto	3
4	Muy Alto	15

Fuente: Elaboración propia

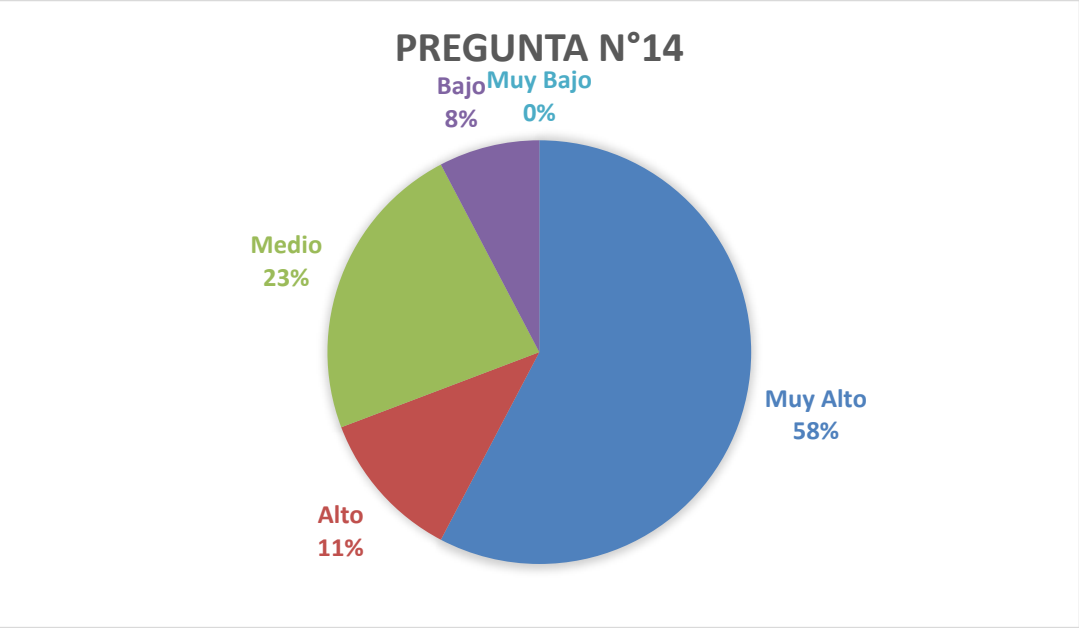


Figura 95. Gráfico Circular de la Pregunta N°14

Fuente: Elaboración propia

Interpretación

La mayoría de los encuestados de la Autoridad Autónoma de Majes opinan en un grado alto que la información debe ser previamente aprobada por la Unidad de Tecnologías de Información para su subida al sitio web.

15. ¿Cuál es su nivel de satisfacción respecto a que la Unidad de Tecnologías de Información revise los equipos de Tecnologías de la Información cuando es asignado a un trabajador?

Tabla 75. Respuestas a Pregunta N°15

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	0
1	Bajo	2
2	Medio	1
3	Alto	13
4	Muy Alto	10

Fuente: Elaboración propia

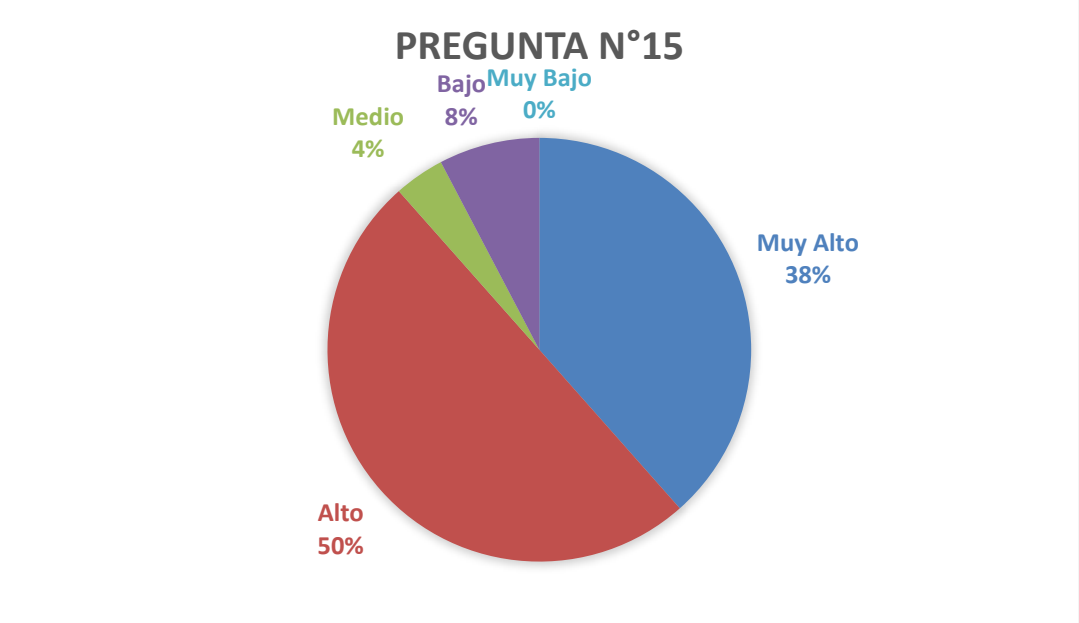


Figura 96. Gráfico Circular de la Pregunta N°15

Fuente: Elaboración propia

Interpretación

La gran mayoría de los encuestados de la Autoridad Autónoma de Majes opinan con un grado alto a muy alto que la Unidad de Tecnologías de Información debe revisar los equipos previamente a entregarse a un trabajador.

Un resumen general de la encuesta del estado deseado de la organización se encuentra en la siguiente tabla:

Tabla 76. Resumen de Respuestas de Encuesta de Estado Actual de la Organización

Escala	Grado de Satisfacción	Respuesta
0	Muy Bajo	2
1	Bajo	18
2	Medio	61
3	Alto	168
4	Muy Alto	143

Fuente: Elaboración propia

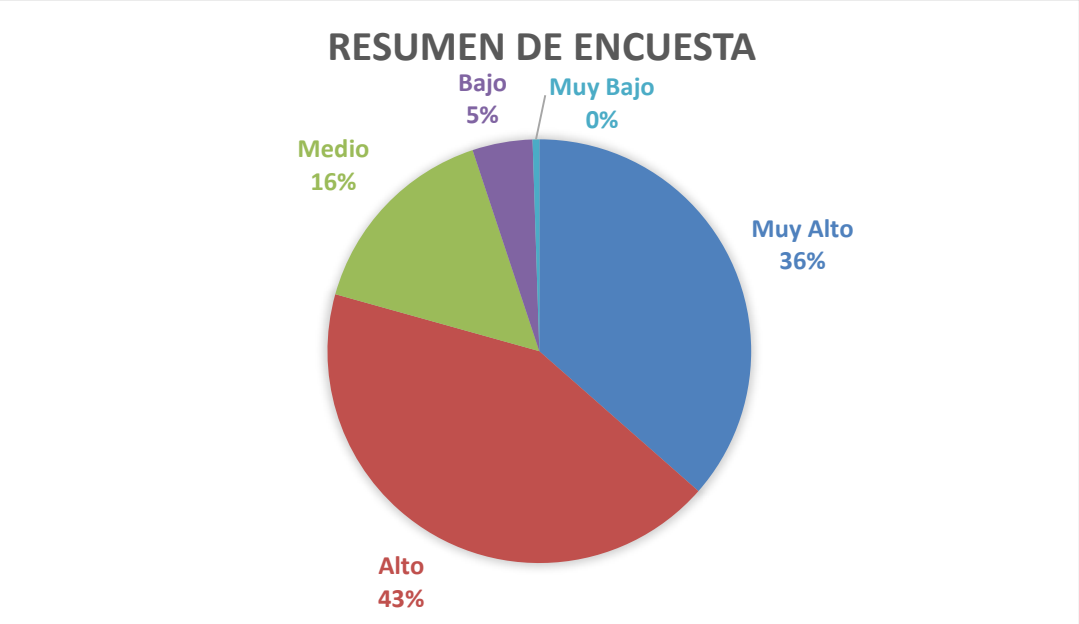


Figura 97. Gráfico Circular Resumen de Encuesta de Estado Deseado de la Organización
Fuente: Elaboración propia

CONCLUSIONES

Primera.- Se realizó la mejora de los procesos de tecnologías de información de la Autoridad Autónoma de Majes aplicando COBIT 5.0 y la norma técnica peruana NTP-ISO 27001: 2014, mediante el análisis y rediseño de procesos de tecnologías de información, la aplicación de los principios claves de COBIT 5 y el análisis y gestión de riesgos para la mejora de los mismos.

Segunda.- Los procesos que se realizan en el día a día no están acorde a los definidos en el Manual Optimizado de Procedimientos, ya que muchos de éstos no son cumplidos a su totalidad y otros no se encuentran correctamente documentados y son realizados por necesidad sin planificación.

Tercera.- El área de Servicios Informáticos de la AUTODEMA no tiene conocimiento de muchos recursos y servicios que forman parte de las tecnologías de la información, por falta de comunicación con las demás áreas y/o falta de documentación.

Cuarta.- Ninguno de los procesos de tecnologías de la información de la Autoridad Autónoma de Majes tiene como base alguna metodología de gobernanza o gestión de buenas prácticas de tecnologías de información.

Quinta.- Los miembros de la Autoridad Autónoma de Majes tienen desconocimiento parcial o total de los procesos de la organización incluyendo a los procesos a cargo del Encargado de Servicios Informáticos.

Sexta.- Según la documentación existente, el Encargado de Servicios Informáticos es el único responsable y ejecutor de todos los procesos de tecnologías de la información, siendo diferente a lo realizado en la práctica.

Sétima.- Al ser el Encargado de Servicios Informáticos dependiente de la Unidad de Logística y Servicios, no tiene capacidad directa de toma de decisiones, así como pierde objetividad en las conformidades de adquisición de bienes o pedidos de servicio, al ser parte de la Unidad encargada de los procesos de compra y pedidos de servicio.

RECOMENDACIONES Y TRABAJOS FUTUROS

Primera.- Aplicar los dominios restantes de COBIT 5 a los procesos de tecnologías de información para lograr la mejora continua de los mismos y mayor grado de madurez.

Segunda.- Establecer una directiva para el desarrollo e implementación de proyectos de acciones de mejora de los procesos de tecnologías de información, con el fin de asegurar la mejora continua de la Unidad de Tecnologías de la Información.

Tercera.- Definir un Sistema de Gestión de Seguridad de la Información que permita el desarrollo de un plan que asegure la información, evite mayores costos operativos y mitigue la baja productividad de toda la Autoridad Autónoma de Majes.

Cuarta.- Elaborar el Plan Estratégico de Tecnologías de la Información, para poder gestionar los recursos de tecnologías de la información, aplicar marcos de trabajo y planes de trabajo.

Quinta.- Implementar el proceso de Organización y Métodos para la alineación de los procesos de la Autoridad Autónoma de Majes con sus objetivos empresariales.

REFERENCIAS BIBLIOGRÁFICAS

Ahmad, A., Maynard, S., & Shanks, G. (2015). A case analysis of information systems and security incident responses. International Journal of Information Management, 35(6), 717–723.

Beingolea, H. (2015). Diseño de un modelo de gobierno de TI utilizando el marco de trabajo de COBIT 5 con enfoque en seguridad de la información. Caso de estudio: una empresa privada administradora de fondos de pensiones. Pontificia Universidad Católica del Perú.

Lucio, T., Colomo, R., & Mora, A. (2012). Hacia una Oficina de Gestión de Servicios en el ámbito de ITIL. Revista Procesos y Métricas, 9(1), 12-28.

Cumandá, J. (2015). Estudio analítico de la compatibilidad entre la norma ISO 38500 y COBIT 5 referente a gobernanza de TI. Universidad de las fuerzas armadas.

De los Ríos, F. (2013). *Un marco de referencia de negocio para el gobierno y la gestión de las TI de la empresa*. Presentación.

Delgado, M. (s.f.). Taller de Implementación de la norma ISO 27001. *Oficina Nacional de Gobierno Electrónico E Informática*.

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security*, *56*, 63–69.

Horna, C. (2016). NTP – ISO/IEC 27001: 2014 Técnicas de seguridad. Sistemas de gestión de seguridad de la información. *Instituto Nacional de Calidad*.

INDECOPI. (2014). NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. *Normas Técnicas Peruanas*, 45.

ISACA. (2012). Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa - COBIT 5.

ISACA. (2012). COBIT 5: Procesos Catalizadores.

Mayadunne, S., y Park, S. (2016). An economic model to evaluate information security investment of risk-taking small and medium enterprises. *International Journal of Production Economics*, *182*(February), 519–530.

Mezzomo, E., & Gregianin, M. (2011). Controles de Governança de Tecnologia da Informação para a terceirização de processos de negócio: Uma proposta a partir do COBIT. *JISTEM Journal of Information Systems and Technology Management*, *8*(1), 237–262.

Manual normativo de clasificación de cargos de la Administración Pública. (1995) (7th ed., Vol. 2). Instituto Nacional de la Administración Pública.

Manual optimizado de procedimientos de AUTODEMA. (2009). *Autoridad Autónoma de Majes Proyecto Especial Majes Siguas*.

Mendoza, M. (2015). Implementación de ISO 27001 (1st ed.). *Buenos Aires: Eset Latinoamérica*.

Oficina de Seguridad de las Redes Informáticas. (2013). Metodología para la Gestión de la Seguridad Informática (Proyecto). *La Habana: Dirección de Seguridad y Protección.*

Ordenanza Regional N°270-Arequipa. (2014). *Gobierno Regional Arequipa*.

Plan Estratégico 2013-2017 (2012). *Autoridad Autónoma de Majes.*

Poggio, J. (2013). IT Management model for financial report issuance and regulatory and legal compliance, *Journal of Information Systems and Technology Management*, *10*(3), pp. 597-620.

*Resolución Gerencial Ejecutiva N°376-2012-GRA-PEMS-GG/OAI.(*2012). Autoridad Autónoma de Majes.

Safa, N.S., y Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442–451.

Salazar, J. (2016). *Evaluación del nivel de madurez de los procesos de TI aplicando COBIT en el Gobierno Regional de Piura*. Universidad Nacional Pedro Ruiz Gallo.

Sánchez, J., Fernández Vicente, E., & Moratilla, A. (2013). ITIL, COBIT and EFQM: Can They Work Together? *International Journal of Combinatorial Optimization Problems & Informatics*, *4*(1), 54–64.

Santana, M. (2011). *¿Qué tan importante resulta la TI en las empresas? Esan.edu.pe*. Revisado de: https://www.esan.edu.pe/conexion/actualidad/2011/10/14/que-tan-importante-resulta-la-ti-en-las-empresas/

Secretaría de Gestión Pública de la Presidencia del Consejo de Ministros. (2013). Lineamientos Para La Implementación De La Gestión Por Procesos En Las Entidades De La Administración Pública En El Marco Del D.S. N° 004-2013-Pcm – Política Nacional De Modernización De La Gestión Pública Al 2021. *Presidencia Del Consejo de Ministros*, 1–8.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of Information Security Risk Assessment (ISRA). *Computers & Security*, *57*, 14–30.

Vieira, M., & Souza, J. (2016). Information technology service management processes maturity in the Brazilian Federal direct administration. *Journal of Information Systems and Technology Management*, *12*(3), 663–686.

Yan, F., & Zavala, C. (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*. Universidad Privada Antenor Orrego.

ANEXOS

Arequipa, 27 de Octubre de 2017

57

GOBIERNO REGIONAL AREQUIPA
Autoridad Autónoma de Majes
Trámite Documentario
Oficina de Arequipa
27 OCT. 2017
Doc. Nº 827954 Exp. Nº 559708
Folio: 57 Hora: 1:22 Firma:

Señor

Econ. Eduardo Benitez Pérez

Jefe de la Oficina de Planificación y Presupuesto

Presente.-

REF: SOLICITUD DE REVISIÓN DE PROPUESTA DE MEJORA DE PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA AUTODEMA

De mi consideración:

Es grato dirigirme a usted a fin de solicitarle la revisión de mi propuesta de Mejora de Procesos de Tecnologías de la Información de la AUTODEMA, que he desarrollado para mi proyecto de tesis titulado "Mejora de los Procesos de Tecnologías de la Información aplicando COBIT 5 y la Norma Técnica Peruana NTP-ISO 27001:2014. Caso: Autoridad Autónoma de Majes".

Adjunto los siguientes documentos:

GOBIERNO REGIONAL AREQUIPA
Autoridad Autónoma de Majes
Proyecto Especial Majes - Siguas
Oficina de Planificación y Presupuesto
27 OCT 2017
Registro: 1967
Folios:
Firma: Hora: 14:51

- Propuesta de Organigrama de la Organización
- Propuesta de Procedimiento GTI – 01
- Diseño de Proceso GTI – 01
- Propuesta de Procedimiento GTI – 02
- Diseño de Proceso GTI – 02
- Propuesta de Procedimiento GTI – 03
- Diseño de Proceso GTI – 03
- Propuesta de Procedimiento GTI – 04
- Diseño de Proceso GTI – 04
- Propuesta de Procedimiento GTI – 05
- Diseño de Proceso GTI – 05
- Propuesta de Procedimiento GTI – 06
- Diseño de Proceso GTI – 06
- Propuesta de Procedimiento GTI – 07
- Diseño de Proceso GTI – 07
- Propuesta de Procedimiento GTI – 08
- Diseño de Proceso GTI – 08
- Propuesta de Procedimiento GTI – 09
- Diseño de Proceso GTI – 09
- Propuesta de Procedimiento GTI – 10
- Diseño de Proceso GTI – 10

Agradezco de antemano la atención que brinda a la presente, me despido.

Atentamente

Javier Fernando Angulo Osorio

Bachiller en Ingeniería de Sistemas

Oficina de Planificación y Presupuesto
Pase A: Racion.
Para: evaluar
30/10/17
Fecha Firma

OBJETIVO:	Normar el proceso a seguir para la realización de copias de seguridad de toda la información de los sistemas de información a cargo de la Unidad de Tecnologías de Información.
ALCANCE:	Comprende desde la clasificación del periodo de realización de la copia de seguridad, hasta su almacenamiento.

I. RESUMEN DEL PROCESO	
RESPONSABLE	**ACTIVIDADES**
Encargado de Seguridad de la Información /Jefe de Unidad de Tecnologías de Información / Jefe de Oficina de Administración	1. Planificación de copias de seguridad - BACKUP
Encargado de Seguridad de la Información /Jefe de Unidad de Tecnologías de Información	2. Desarrollo de cronograma de copias de seguridad - BACKUP
Encargado de Seguridad de la Información /Jefe de Unidad de Tecnologías de Información	3. Almacenamiento de copias de seguridad - BACKUP

I. PROCESO AL DETALLE

RESPONSABLE	ACTIVIDADES
1. PLANIFICACIÓN DE COPIAS DE SEGURIDAD - BACKUP	
Encargado de Seguridad de la Información	1.1. Realiza la evaluación de los mantenimientos correctivos realizados en el año anterior, a fin de presentar las incidencias ocurridas y atenciones realizadas.
Encargado de Seguridad de la Información	1.2. Prepara el Plan Anual de Copias de Seguridad considerando: – Sistemas de Información en uso. – Criticidad de la información.
Jefe de Unidad de Tecnologías de Información	1.3. Recibe el Plan Anual de Copias de Seguridad, para su revisión y conformidad. De existir observaciones devuelve el mismo para su corrección; caso contrario, continúa con el siguiente punto.
Jefe de Oficina de Administración	1.4. Recibe el Plan Anual de Copias de Seguridad, aprobado por el Jefe de Unidad de Tecnologías de Información, para su revisión y conformidad. De existir observaciones devuelve el mismo para su corrección; caso contrario, continúa con el siguiente punto.
Encargado de Seguridad de la Información	1.5. Recibe el Plan Anual de copias de seguridad con la conformidad del Jefe de Unidad de Tecnologías de Información y el Jefe de la Oficina de Administración.
2. DESARROLLO DE CRONOGRAMA DE COPIAS DE SEGURIDAD - BACKUP	
Encargado de Seguridad de la Información	2.1. Comunica a Jefe de la Unidad de Tecnologías de Información realización de copia de seguridad.
Jefe de Unidad de Tecnologías de Información	2.2. Informa al área usuaria que deben salir del sistema de información por mantenimiento.
Encargado de Seguridad de la Información	2.3. Realiza copia de seguridad de la base de datos de los sistemas de información.
Encargado de Seguridad de la Información	2.4. Realiza almacenamiento de copia de seguridad en disco duro externo y/o en un CD.
Encargado de Seguridad de la Información	2.5. Entrega CD a Jefe de Unidad de Tecnologías de Información.
Jefe de Unidad de Tecnologías de Información	2.6. Recibe CD de copia de seguridad, para su revisión y conformidad. De existir observaciones devuelve el mismo para su corrección; caso contrario, continúa con el siguiente punto.
Jefe de Unidad de Tecnologías de Información.	2.7. Registra ficha de copia de seguridad.

3. ALMACENAMIENTO DE COPIAS DE SEGURIDAD - BACKUP	
Jefe de Unidad de Tecnologías de Información.	3.1 Guarda CD de copia de seguridad en histórico de copias de seguridad.

REFERENCIA HISTÓRICA DE MODIFICACIONES					
	VER.	REALIZADA POR	FECHA	DESCRIPCIÓN DEL CAMBIO	REVISIÓN
ELAB.	01	JA	12/10/2017	DEFINICIÓN DE PROCEDIMIENTO	
MODIF.					
MODIF.					

	FORMATO DE PLAN ANUAL DE COPIAS DE SEGURIDAD	FORMATO N°01	
Autoridad Autónoma de Majes		SEGURIDAD DE LA INFORMACIÓN	
Encargado:		**N°:**	
Sistemas:	**S.I.G.A.:** S.G.	**S.I.A.F.: S.F.**	**S.I.A.T.D.: S.T.**	**Inventarios:** IN

PROGRAMACIÓN DE COPIA DE SEGURIDAD

Mes: Enero

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Observaciones:

Mes: Febrero

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Observaciones:

Mes: Marzo

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Observaciones:

Mes: Abril

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Observaciones:

Mes: Mayo

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Observaciones:

Mes: Junio

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Observaciones:

Mes: Julio

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Observaciones:

Mes: Agosto

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Observaciones:

Mes: Setiembre

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Observaciones:

Mes: Octubre

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Observaciones:

Mes: Noviembre

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Observaciones:

Mes: Diciembre

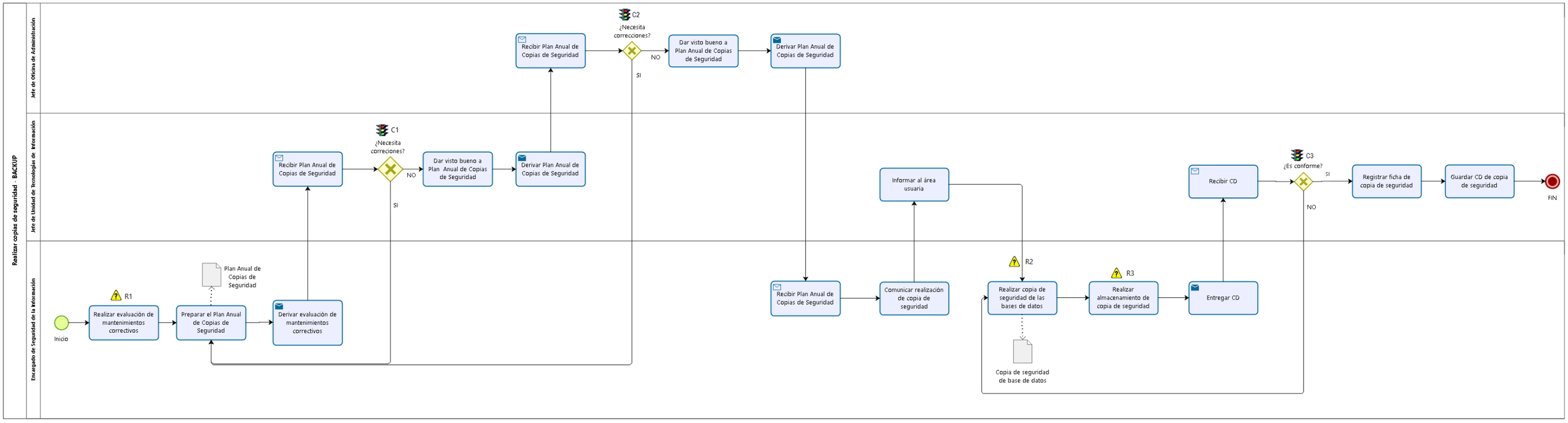
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Observaciones:

_____	_____
Jefe de Unidad de Tecnologías de Información	Encargado de Seguridad de la Información

	FORMATO DE COPIA DE SEGURIDAD -BACKUP	FORMATO N°02			
Autoridad Autónoma de Majes		SEGURIDAD DE LA INFORMACIÓN			
Encargado:		**N°:**			
IP Servidor:		**FECHA:**			
Sistemas de Información:	S.I.G.A. ☐ S.I.A.F. ☐ S.I.A.T.D. ☐ Inventarios ☐ Otros:_____				

_____	_____
Jefe de Unidad de Tecnologías de Información	Encargado de Seguridad de la Información


Realizar copias de seguridad - BACKUP
Jefe de Oficina de Administración
Jefe de Unidad de Tecnologías de Información
Encargado de Seguridad de la Información
Inicio
Realizar evaluación de mantenimientos correctivos
R1
Plan Anual de Copias de Seguridad
Preparar el Plan Anual de Copias de Seguridad
Derivar evaluación de mantenimientos correctivos
Recibir Plan Anual de Copias de Seguridad
C1
¿Necesita correciones?
NO
SI
Dar visto bueno a Plan Anual de Copias de Seguridad
Derivar Plan Anual de Copias de Seguridad
C2
¿Necesita correcciones?
NO
SI
Dar visto bueno a Plan Anual de Copias de Seguridad
Derivar Plan Anual de Copias de Seguridad
Recibir Plan Anual de Copias de Seguridad
Comunicar realización de copia de seguridad
Informar al área usuaria
R2
Realizar copia de seguridad de las bases de datos
Copia de seguridad de base de datos
R3
Realizar almacenamiento de copia de seguridad
Entregar CD
Recibir CD
C3
¿Es conforme?
SI
NO
Registrar ficha de copia de seguridad
Guardar CD de copia de seguridad
FIN

OBJETIVO:	Normar el proceso a seguir para la realización de soporte informático al área usuaria de la AUTODEMA, garantizando el buen funcionamiento de los equipos, red y programas.
ALCANCE:	Comprende desde la recepción de solicitud de soporte informático por parte del usuario, hasta su conformidad de solución.

I. RESUMEN DEL PROCESO	
RESPONSABLE	**ACTIVIDADES**
Usuario PEMS / Mesa de Ayuda	1. Recepción de requerimiento de servicio informático
Mesa de ayuda / Mesa de Servicio / Encargado de Infraestructura de Tecnologías de Información / Jefe de Unidad de Tecnologías de Información	2. Brindar soporte informático
Mesa de Ayuda / Mesa de Servicio / Encargado de Infraestructura de Tecnologías de Información	3. Registro de solución en base de conocimiento

I. PROCESO AL DETALLE	
RESPONSABLE	**ACTIVIDADES**
1. RECEPCIÓN DE REQUERIMIENTO DE SERVICIO INFORMÁTICO	
Usuario PEMS	1.1. Realiza requerimiento de manera verbal, escrita o telefónica de soporte informático.
Mesa de Ayuda	1.2. Recibe y analiza requerimiento del Usuario PEMS y prioriza requerimiento según nivel de importancia: – Alto: Compromete continuidad del negocio. – Medio: Compromete tiempo de ejecución del negocio. – Bajo: No compromete la continuidad del negocio.
2. BRINDAR SOPORTE INFORMÁTICO	
Mesa de Ayuda	2.1. Realiza requerimiento solicitado. De no satisfacer requerimiento, deriva requerimiento a Mesa de Servicio.
Mesa de Servicio	2.2. Recibe requerimiento de Mesa de Ayuda y realiza soporte informático. De no satisfacer requerimiento, deriva requerimiento al Encargado de Infraestructura de Tecnologías de Información
Encargado de Infraestructura de Tecnologías de Información	2.3. Recibe requerimiento de Mesa de Servicio y realiza soporte informático. De ser necesaria la compra de un repuesto o contratar un servicio especializado, elabora un informe técnico y lo envía al Jefe de Unidad de Tecnologías de Información
Jefe de Unidad de Tecnologías de Información	2.4. Recibe informe técnico, pasa revisión y conformidad y lo envía a Usuario PEMS.
3. REGISTRO DE SOLUCIÓN EN BASE DE CONOCIMIENTO	
Mesa de Ayuda	3.1 Registra ficha de soporte informático, de haber sido derivado el requerimiento a la Mesa de Servicio, recibe ficha de soporte informático.
Mesa de Servicio	3.2 Registra ficha de soporte informático, de haber sido derivado el requerimiento al Encargado de Infraestructura de Tecnologías de Información, recibe ficha de soporte informático.
Encargado de Infraestructura de Tecnologías de Información	3.3 Registra ficha de soporte informático, de haber un informe técnico, adjuntarlo a la ficha.

REFERENCIA HISTÓRICA DE MODIFICACIONES					
	VER.	REALIZADA POR	FECHA	DESCRIPCIÓN DEL CAMBIO	REVISIÓN
ELAB.	01	JA	12/10/2017	DEFINICIÓN DE PROCEDIMIENTO	
MODIF.					
MODIF.					

	FORMATO DE SOPORTE INFORMÁTICO		FORMATO N°02	
Autoridad Autónoma de Majes			MESA DE SERVICIO INFRAESTRUCTURA DE T. I.	
Área Solicitante:			**N°:**	
Usuario Solicitante:			**FECHA:**	
Encargado de requerimiento:				
Prioridad:		**Adjunta:**		
Requerimiento:	_____ _____ _____ _____ _____			
Solución:	_____ _____ _____ _____ _____ _____			

_____ Jefe de Unidad de Tecnologías de Información	_____ Encargado

AUTORIDAD AUTÓNOMA DE MAJES

"AÑO DEL BUEN SERVICIO AL CIUDADANO"

INFORME Nº XXX–XXXX–GRA–PEMS/TECNOLOGÍAS DE INFORMACIÓN

PARA :

ASUNTO :

REFERENCIA:

FECHA :

APROBACIÓN:	FECHA:

Realizar soporte informático

Jefe de Unidad de Tecnologías de Información

Recibir informe técnico

C8
¿Visto bueno?

SI

Enviar informe técnico

NO

Encargado de Infraestructura de Tecnologías de Información

Informe técnico

C7
¿Se cumplió requerimiento?

R7

Recibir requermiento

Realizar soporte informático

NO

Elaborar informe técnico

Derivar informe técnico

SI

Ficha de soporte informático

Registrar ficha de requerimiento solucionado

Enviar ficha de requerimiento solucionado

Mesa de Servicio

Ficha de soporte informático

Derivar requerimiento

R6

Recibir requermiento de Mesa de Ayuda

Realizar soporte informático

NO

¿Se cumplió requerimiento?

C6

SI

Registrar ficha de requerimiento solucionado

Enviar ficha de requerimiento solucionado

Mesa de Ayuda

Ficha de soporte informático

Derivar requermiento a Mesa de Servicio

NO

Recibir requerimiento de soporte informático

Priorizar requerimiento

NO

¿Es mayor a requerimientos en cola?

C4

SI

Realizar soporte informático

¿Se cumplió requerimiento?

C5

SI

Registrar ficha de requerimiento solucionado

Archivar ficha de requerimiento solucionado

Usuario PEMS

INICI

Realizar requerimiento de soporte informático

R4

Recibir informe técnico

FIN

OBJETIVO:	Normar el proceso a seguir para la elaboración del reporte mensual de trabajo de la Unidad de Tecnologías de la Información
ALCANCE:	Comprende desde la solicitud de informe de actividades hasta la comunicación a la Gerencia Ejecutiva y al Jefe de Oficina de Administración acerca de las actividades realizadas en el mes.

I. RESUMEN DEL PROCESO	
RESPONSABLE	**ACTIVIDADES**
Jefe de Unidad de Tecnologías de Información / Encargado de Infraestructura de Tecnologías de Información / Encargado de Seguridad de la Información / Mesa de Servicio	1. Elaboración de informe mensual

I. PROCESO AL DETALLE

RESPONSABLE	ACTIVIDADES
1. ELABORACIÓN DE REPORTE MENSUAL	
Jefe de Unidad de Tecnologías de Información	1.1. Solicita a Mesa de Servicio, Encargado de Infraestructura de Tecnologías de Información y a Encargado de Seguridad de la Información informe mensual de las actividades realizadas en el mes.
Mesa de Servicio	1.2. Realiza informe mensual con las actividades realizadas en el mes y lo entrega a Jefe de Unidad de Tecnologías de Información.
Encargado de Infraestructura de Tecnologías de Información	1.3. Realiza informe mensual con las actividades realizadas en el mes y lo entrega a Jefe de Unidad de Tecnologías de Información.
Encargado de Seguridad de la Información	1.4. Realiza informe mensual con las actividades realizadas en el mes y lo entrega a Jefe de Unidad de Tecnologías de Información.
Jefe de Unidad de Tecnologías de Información	1.5. Recibe, evalúa y compara si las actividades realizadas por los Encargados de la Unidad de Tecnologías de Información están alineadas a las metas mensuales.
Jefe de Unidad de Tecnologías de Información	1.6. Convoca a reunión para establecer metas de mes que apoyen a los objetivos anuales de la Unidad.
Jefe de Unidad de Tecnologías de Información	1.7. Elabora informe consolidado.
Jefe de Unidad de Tecnologías de Información	1.8. Envía copia de informe consolidado a Gerencia Ejecutiva y a Jefe de Oficina de Administración.

REFERENCIA HISTÓRICA DE MODIFICACIONES					
	VER.	REALIZADA POR	FECHA	DESCRIPCIÓN DEL CAMBIO	REVISIÓN
ELAB.	01	JA	12/10/2017	DEFINICIÓN DE PROCEDIMIENTO	
MODIF.					
MODIF.					

APROBACIÓN:	FECHA:

AUTORIDAD AUTÓNOMA DE MAJES

"AÑO DEL BUEN SERVICIO AL CIUDADANO"

GOBIERNO REGIONAL

INFORME Nº XXX–XXXX–GRA–PEMS/TECNOLOGÍAS DE INFORMACIÓN

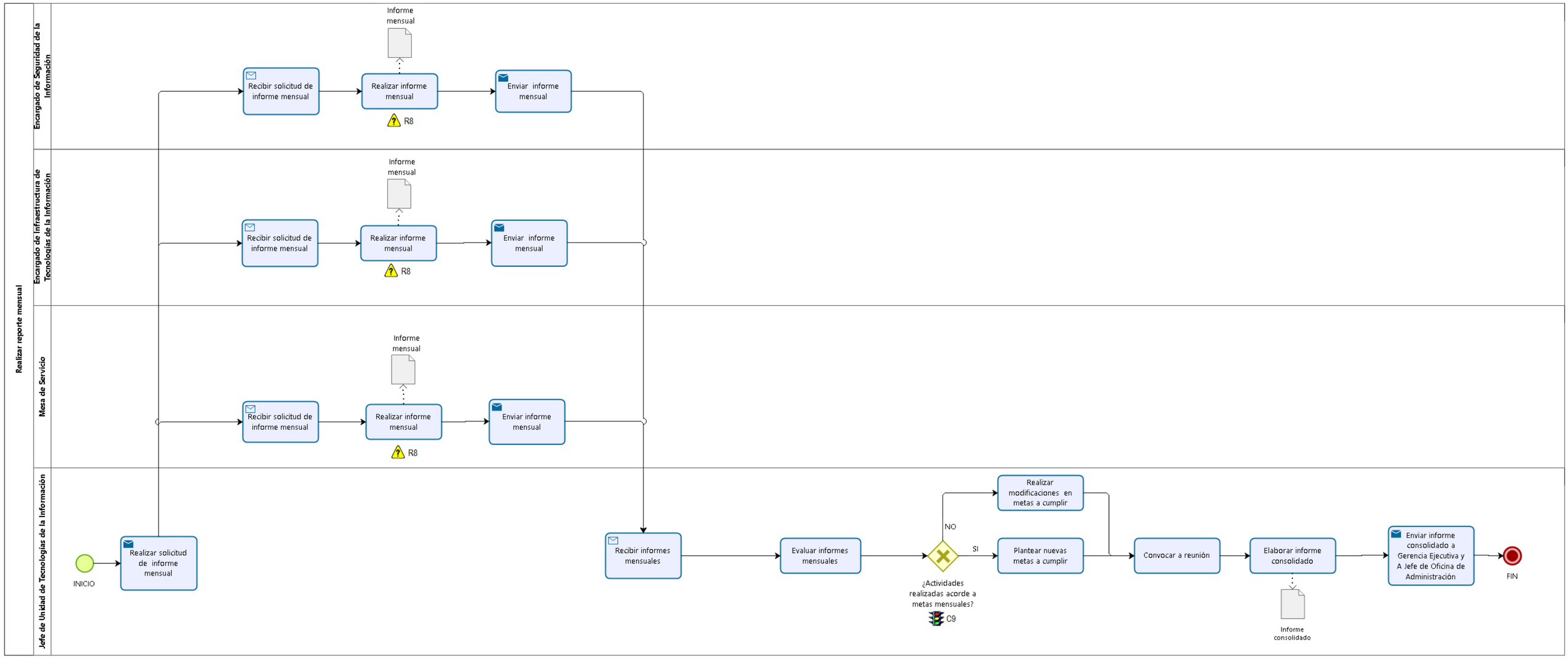
PARA :

ASUNTO :

REFERENCIA:

FECHA :

APROBACIÓN:	FECHA:


Realizar reporte mensual
Encargado de Seguridad de la Información
Informe mensual
Recibir solicitud de informe mensual
Realizar informe mensual
R8
Enviar informe mensual
Encargado de Infraestructura de Tecnologías de la Información
Informe mensual
Recibir solicitud de informe mensual
Realizar informe mensual
R8
Enviar informe mensual
Mesa de Servicio
Informe mensual
Recibir solicitud de informe mensual
Realizar informe mensual
R8
Enviar informe mensual
Jefe de Unidad de Tecnologías de la Información
INICIO
Realizar solicitud de informe mensual
Recibir informes mensuales
Evaluar informes mensuales
¿Actividades realizadas acorde a metas mensuales?
C9
NO
SI
Realizar modificaciones en metas a cumplir
Plantear nuevas metas a cumplir
Convocar a reunión
Elaborar informe consolidado
Informe consolidado
Enviar informe consolidado a Gerencia Ejecutiva y A Jefe de Oficina de Administración
FIN

OBJETIVO:	Normar el proceso a seguir para la administración de los sistemas de información S.I.G.A. y S.I.A.F.
ALCANCE:	El proceso comienza en el requerimiento del Usuario PEMS y termina en la notificación de la solución al requerimiento.

I. RESUMEN DEL PROCESO	
RESPONSABLE	**ACTIVIDADES**
Usuario PEMS / Jefe de Unidad / Jefe de Unidad de Tecnologías de Información	1. Gestión de usuarios en el sistema de información S.I.G.A. y/o S.I.A.F.
Mesa de Ayuda / Encargado de Seguridad de la Información / Jefe de Unidad de Tecnologías de Información / Secretaria de Recursos Humanos	2. Gestión de requerimiento interna.
Sectorista Regional	3. Gestión de requerimiento externa.

I. PROCESO AL DETALLE	
RESPONSABLE	**ACTIVIDADES**
1. RECEPCIÓN DE REQUERIMIENTO DEL SISTEMA DE INFORMACIÓN S.I.G.A. Y/O S.I.A.F.	
Usuario PEMS	1.1. Realiza requerimiento del sistema S.I.G.A. o S.I.A.F. a Jefe de Unidad
Jefe de Unidad	1.2. Recibe requerimiento, da conformidad y deriva solicitud a Jefe de Unidad de Tecnologías de Información, en caso la rechace termina el proceso.
Jefe de Unidad de Tecnologías de Información	1.3. Recibe requerimiento y analiza si puede solucionarse en el Área o es necesario el soporte externo del Ministerio de Economía y Finanzas, en caso sea interno, lo deriva a Mesa de Ayuda, en caso sea externo, lo deriva a Sectorista Regional.
2. GESTIÓN DE REQUERIMIENTO INTERNA	
Mesa de Ayuda	2.1. Recibe requerimiento, lo analiza y realiza soporte técnico. En caso de ser necesaria la creación de credenciales de acceso o ítems lo deriva al Encargado de Seguridad de la Información.
Encargado de Seguridad de la Información	2.2. Recibe el requerimiento, en caso sea necesaria la creación de usuario, solicita datos a Jefe de Unidad de Tecnologías de Información: – Apellidos y nombres – Código – Profesión – Teléfono – Email – Denominación de cargo – Dependencia En caso sea necesaria la creación de ítem, solicita datos a Jefe de Unidad de Tecnologías de Información: – Descripción del producto – Link de referencia – Imagen del producto
Jefe de Unidad de Tecnologías de Información	2.3. Recibe solicitud y la deriva a Secretaria de Recursos Humanos.
Secretaria de Recursos Humanos	2.4. Recibe solicitud y envía datos requeridos a Jefe de Unidad de Tecnologías de la Información.
Jefe de Unidad de Tecnologías de Información	2.5. Recibe datos y los envía a Encargado de Seguridad de la Información.

Encargado de Seguridad de la Información	2.6. Recibe los datos, realiza la creación de usuario/ítem y la notifica.
3. GESTIÓN DE REQUERIMIENTO EXTERNA	
Sectorista Regional	3.1 Recibe requerimiento, realiza la solución del mismo y notifica su solución, en caso no haya satisfecho el requerimiento lo deriva al Sectorista Nacional.

REFERENCIA HISTÓRICA DE MODIFICACIONES					
	VER.	**REALIZADA POR**	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**	**REVISIÓN**
ELAB.	01	JA	12/10/2017	DEFINICIÓN DE PROCEDIMIENTO	
MODIF.					
MODIF.					

Administrar sistemas S.I.G.A. y S.I.A.F.

Sectorista Regional MEF

Derivar requerimiento a sectorista nacional
Recibir requerimiento
Realizar soporte técnico
¿Requerimiento satisfecho?
NO
SI
Notificar solución
C13
C15
¿Información correcta?
Recibir información
SI
Realizar procedimiento
Notificar creación
NO

Mesa de Ayuda

Recibir requerimiento
C12
¿Es necesaria la gestión de credenciales/ ítems?
NO
SI
Realizar soporte informático
Derivar requerimiento a encargado de Seguridad de la Información
FIN

Encargado de Seguridad de la Información

C14
¿Es necesaria la creación de usuario?
Recibir requerimiento
NO
SI
Solicitar información
Solicitar información
Recibir Información
Recibir información
Enviar información
Realizar creación de usuario
Notificar creación

Jefe de Unidad de Tecnologías de Información

Derivar requerimiento
NO
Recibir requerimiento de S.I.G.A. / S.I.A.F.
¿Se necesita soporte externo?
SI
Enviar requerimiento
C11
Recibir solicitud
Solicitar información

Secretaria de Recursos Humanos

Recibir solicitud
Enviar información

Jefe de Unidad

SI
Recibir requerimiento
¿Es viable?
NO
C10

Usuario PEMS

INICIO
Realizar requerimiento de S.I.G.A. / S.I.A.F.
Recibir solicitud
Enviar información

OBJETIVO:	Normar el proceso a seguir para la supervisión de los servicios tercerizados de la Unidad de Tecnologías de Información
ALCANCE:	Comprende desde la elaboración del requerimiento del servicio, hasta la emisión de conformidad del servicio.

I. RESUMEN DEL PROCESO	
RESPONSABLE	**ACTIVIDADES**
Usuario PEMS / Jefe de Unidad de Tecnologías de Información / Jefe de Oficina de Administración / Encargado de Infraestructura de Tecnologías de la Información	1. Supervisión de servicios tercerizados.

I. PROCESO AL DETALLE

RESPONSABLE	ACTIVIDADES
1. SUPERVISIÓN DE SERVICIOS TERCERIZADOS	
Usuario PEMS	1.1. Realiza requerimiento de manera escrita de términos de referencia para el desarrollo de sistema de información.
Jefe de Unidad de Tecnologías de Información	1.2. Recibe y analiza requerimiento del Usuario PEMS, en caso de dar visto bueno, realiza términos de referencia y los devuelve a área usuaria.
Usuario PEMS	1.3. Elabora informe y lo envía para su aprobación a Oficina de Administración con copia a Unidad de Tecnologías de Información.
Jefe de Oficina de Administración	1.4. Recibe y analiza informe, en caso de dar conformidad, envía a Logística requerimiento de Servicio.
Encargado de Infraestructura de Tecnologías de Información	1.5. Controla y monitorea implementación del servicio.
Jefe de Unidad de Tecnologías de Información	1.6. Recibe y deriva documentación del servicio al área usuaria.
Jefe de Unidad de Tecnologías de Información	1.7. Emite conformidad de servicio y la envía a usuario PEMS.

REFERENCIA HISTÓRICA DE MODIFICACIONES

	VER.	REALIZADA POR	FECHA	DESCRIPCIÓN DEL CAMBIO	REVISIÓN
ELAB.	01	JA	12/10/2017	DEFINICIÓN DE PROCEDIMIENTO	
MODIF.					
MODIF.					

APROBACIÓN:	FECHA:

AUTORIDAD AUTÓNOMA DE MAJES

"AÑO DEL BUEN SERVICIO AL CIUDADANO"

TERMINOS DE REFERENCIA

SERVICIO PARA XXXXXXXxxxxxxx

I. OBJETO DE LA CONTRATACION.

Seleccionar al proveedor sea persona natural o jurídica que realice el **"SERVICIO XXXXXXXXxxxxxxx"**

II. FINALIDAD

III. ENTIDAD CONVOCANTE

Autoridad Autónoma de majes

IV. BASE LEGAL

- Ley Nº 04764/2016-PE de Presupuesto del Sector público para el año Fiscal 2016.
- Código Civil libro VII- Titulo IX, Capitulo 11 Art.1764
- Ley de Contrataciones del estado, Aprobada mediante D.L. Nº 1017, su Reglamento, aprobado por D.S. Nº 184-2008 y demás normas modificatorias (de aplicación supletoria por disposición del art. 3 del RLCE).

V. CARACTERISTICAS Y ALCANCES DEL SERVICIO.

VI. PERFIL DE LA PERSONA NATURAL O JURIDICA QUE DEBERA PRESTAR EL SERVICO SEGÚN LA NATURALEZA DE LA CONTRATACION.

VII. LUGAR Y PLAZO DE EJECUCION.

VIII. VALOR REFERENCIAL.

IX. PERIODO DE CONTRATACION O PLAZO.

X. FORMA DE PAGO

XI. INICIO DEL SERVICIO

XII. OBLIGACIONES Y RESPONSABILIDADES DEL PROVEEDOR

XIII. SUPERVISION Y CONFORMIDAD DE SERVICIO.

AUTORIDAD AUTÓNOMA DE MAJES

"AÑO DEL BUEN SERVICIO AL CIUDADANO"

INFORME Nº XXX–XXXX–GRA–PEMS/TECNOLOGÍAS DE INFORMACIÓN

PARA :

ASUNTO :

REFERENCIA:

FECHA :

APROBACIÓN:	FECHA:

AUTORIDAD AUTÓNOMA DE MAJES

"AÑO DEL BUEN SERVICIO AL CIUDADANO"

INFORME Nº XXX–XXXX–GRA–PEMS/TECNOLOGÍAS DE INFORMACIÓN

PARA : Jefe de la Oficina de Administración

ASUNTO : Conformidad de Servicio

REFERENCIA :

FECHA :

Tipo de Servicios

Periodo

Monto Total a Pagar

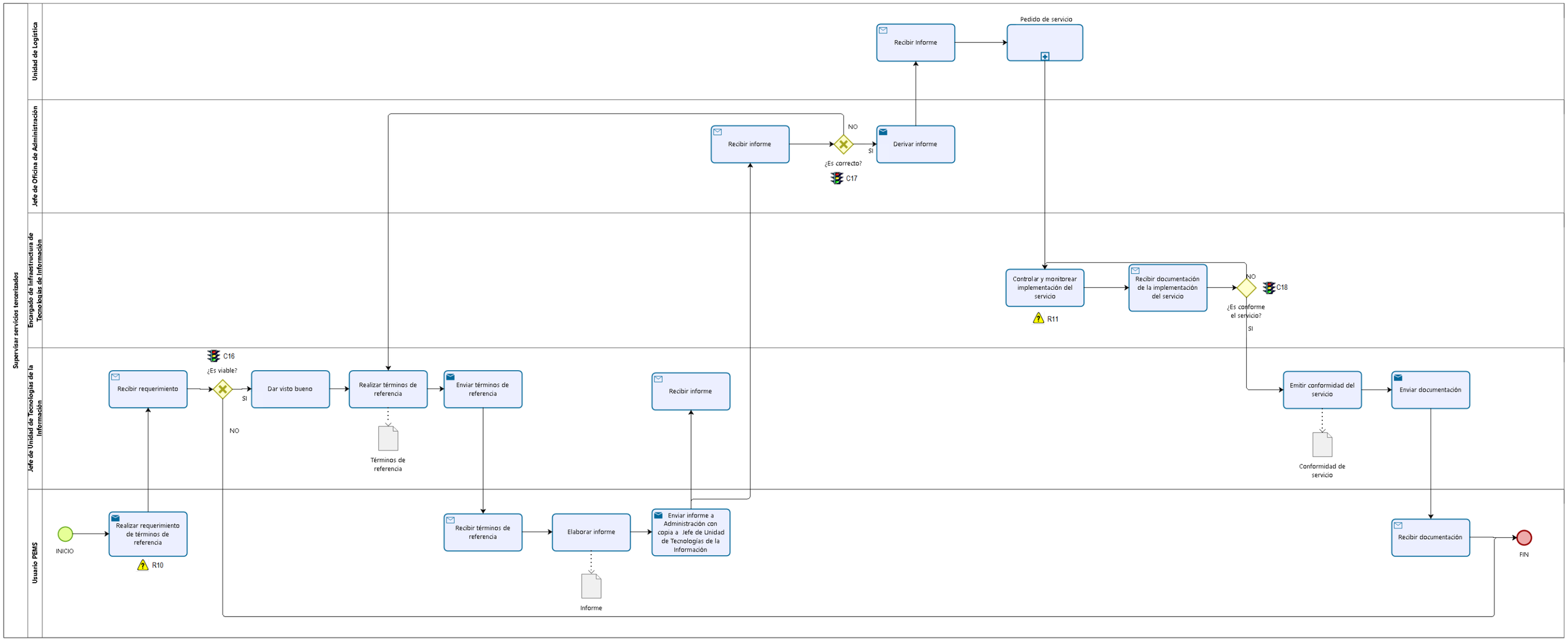
Responsable

Se otorga conformidad al presente servicio.
Fecha:.....

.....

Jefe de Unidad de Tecnologías de Información

Reg. Doc.:	
Reg. Exp.:	


Supervisar servicios tercerizados
Unidad de Logística
Jefe de Oficina de Administración
Encargado de Infraestructura de Tecnologías de Información
Jefe de Unidad de Tecnologías de la Información
Usuario PEMS
Recibir Informe
Pedido de servicio
Recibir informe
NO
SI
Derivar informe
¿Es correcto?
C17
Controlar y monitorear implementación del servicio
R11
Recibir documentación de la implementación del servicio
NO
C18
¿Es conforme el servicio?
SI
C16
¿Es viable?
Recibir requerimiento
SI
Dar visto bueno
Realizar términos de referencia
Enviar términos de referencia
Términos de referencia
Recibir informe
NO
Emitir conformidad del servicio
Enviar documentación
Conformidad de servicio
INICIO
Realizar requerimiento de términos de referencia
R10
Recibir términos de referencia
Elaborar informe
Informe
Enviar informe a Administración con copia a Jefe de Unidad de Tecnologías de la Información
Recibir documentación
FIN

OBJETIVO:	Normar el proceso a seguir para la elaboración y supervisión del cumplimiento de directivas de seguridad de la información.
ALCANCE:	Comprende desde el análisis del cumplimiento de las directivas de seguridad de la información hasta su difusión al área usuaria.

I. RESUMEN DEL PROCESO	
RESPONSABLE	**ACTIVIDADES**
Encargado de Seguridad de la Información / Jefe de Unidad de Tecnologías de Información / Jefe de Oficina de Administración	1. Elaboración de directivas de seguridad de la información.
Encargado de Seguridad de la Información	2. Supervisión de directivas de seguridad de la información.

I. PROCESO AL DETALLE	
RESPONSABLE	**ACTIVIDADES**
1. ELABORACIÓN DE DIRECTIVAS DE SEGURIDAD DE LA INFORMACIÓN	
Encargado de Seguridad de la Información	1.1. Analiza situación actual de la seguridad de la información de la AUTODEMA.
Encargado de Seguridad de la Información	1.2. Realiza actualización de Directivas de Seguridad de la Información y las deriva al Jefe de Unidad de Tecnologías de Información para su aprobación.
Jefe de Unidad de Tecnologías de Información	1.3. Recibe Directivas de Seguridad de la Información para su revisión y conformidad. De existir observaciones devuelve el mismo para su corrección; caso contrario, lo deriva al Jefe de Oficina de Administración para su aprobación.
Jefe de Oficina de Administración	1.4. Recibe las Directivas de Seguridad de la Información para su revisión y conformidad. De existir observaciones devuelve el mismo para su corrección; caso contrario, lo visa y envía a gerencia para su difusión mediante resolución administrativa.
2. SUPERVISIÓN DE DIRECTIVAS DE SEGURIDAD DE LA INFORMACIÓN	
Encargado de Seguridad de la Información	2.1.Realiza monitoreo continuo del uso de la información de la AUTODEMA.

REFERENCIA HISTÓRICA DE MODIFICACIONES					
	VER.	**REALIZADA POR**	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**	**REVISIÓN**
ELAB.	01	JA	12/10/2017	DEFINICIÓN DE PROCEDIMIENTO	GR
MODIF.					
MODIF.					

APROBACIÓN:	**FECHA:**

AUTORIDAD AUTÓNOMA DE MAJES

"AÑO DEL BUEN SERVICIO AL CIUDADANO"

DIRECTIVAS DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

ii. Limitaciones de horario
iii. Administración de contraseñas
iv. Inactividad del sistema
v. Estándares de autenticación en los sistemas

p. Control de acceso de aplicación
q. Restricciones de acceso a información
r. Aislamiento de sistemas críticos
s. Monitoreo del acceso y uso de los sistemas
   i. Sincronización del reloj
   ii. Responsabilidades generales
   iii. Registro de eventos del sistema
t. CUMPLIMIENTO NORMATIVO
   i. Registros
   ii. Revisión de la directiva de seguridad y cumplimiento técnico
   iii. Propiedad de los programas
u. INFORMACIÓN ALMACENADA EN MEDIOS DIGITALES Y FÍSICOS
   i. Etiquetado de la información
   ii. Copiado de la información
   iii. Distribución de la información
   iv. Almacenamiento de la información
   v. Eliminación de la información

Supervisar cumplimiento de directivas de seguridad de la información

Jefe de Oficina de Administración

Recibir directivas de seguridad de la información

C20
¿Directivas correctas?

SI

Dar conformidad

Enviar directivas de seguridad de la información a Gerencia Ejecutiva

FIN

NO

Realizar observaciones

Devolver directivas de seguridad de la información

Jefe de Unidad de Tecnologías de la Información

Recibir directivas de seguridad de la información

¿Directivas correctas?

SI

Dar conformidad

Enviar directivas de seguridad de la información

NO

Realizar observaciones

Devolver directivas de seguridad de la información

Encargado de Seguridad de la Información

INICI

R12

Analizar situación de seguridad de la información

C19
¿Directivas correctas?

SI

NO

R13

Actualizar directivas de seguridad de la información

Directivas de seguridad de la información

Enviar directivas de seguridad de la información

OBJETIVO:	Normar el proceso a seguir para la gestión de recepción de bienes o servicios relacionados a las Tecnologías de Información.
ALCANCE:	Comprende desde la recepción del bien o servicio, hasta su conformidad.

I. RESUMEN DEL PROCESO	
RESPONSABLE	**ACTIVIDADES**
Jefe de Unidad de Tecnologías de Información / Encargado de Infraestructura de Tecnologías de Información / Encargado de Compras	1. Recepción de bien
Encargado de Servicios / Jefe de Unidad de Tecnologías de Información / Agente Externo de Servicios	2. Recepción de servicio

I. PROCESO AL DETALLE	
RESPONSABLE	**ACTIVIDADES**
1. RECEPCIÓN DE BIEN	
Jefe de Unidad de Tecnologías de Información	1.1. Recibe bien y lo entrega al Encargado de Infraestructura de Tecnologías de Información para su revisión.
Encargado de Infraestructura de Tecnologías de Información	1.2. Recibe bien y solicita especificaciones técnicas a Encargado de Compras.
Encargado de Compras	1.3. Envía especificaciones técnicas a Encargado de Infraestructura de Tecnologías de Información.
Encargado de Infraestructura de Tecnologías de Información	1.4. Recibe especificaciones técnicas y corrobora que el bien adquirido las cumpla, da visto bueno y entrega equipo a Usuario PEMS. De haber alguna observación o desperfecto, elabora informe y lo deriva a Jefe de Unidad de Tecnologías de Información.
Jefe de Unidad de Tecnologías de Información	1.5. Recibe informe, da conformidad y lo deriva a Encargado de Compras para su solución.
Encargado de Infraestructura de Tecnologías de Información	1.6. Envía bien a almacén.
2. RECEPCIÓN DE SERVICIO	
Encargado de servicios	2.1. Notifica a Jefe de Unidad de Tecnologías de Información del inicio del servicio.
Jefe de Unidad de Tecnologías de Información	2.2. Informa a Encargado de Servicios comienzo de servicio. En caso de que no se cumpla en el periodo establecido, notifica a Encargado de Servicios.
Agente externo de servicios	2.3. Realiza servicio, elabora informe de trabajo y lo entrega a Jefe de Unidad de Tecnologías de Información para su aprobación.
Jefe de Unidad de Tecnologías de la Información	2.4. Recibe informe de trabajo, para su revisión y conformidad y lo entrega a Encargado de Servicios. En caso de que no se cumpla con lo solicitado en los términos de referencia, se lo comunica al Agente Externo de Servicios para su regularización.
Agente Externo de Servicios	2.5. Realiza servicio, actualiza informe de trabajo y lo entrega a Jefe de Unidad de Tecnologías de Información para su aprobación.

Jefe de Unidad de Tecnologías de Información	2.6. Recibe informe de trabajo, para su revisión y conformidad y lo entrega a Encargado de Servicios. En caso de que no se cumpla, notifica a Encargado de Servicios.

REFERENCIA HISTÓRICA DE MODIFICACIONES					
	VER.	REALIZADA POR	FECHA	DESCRIPCIÓN DEL CAMBIO	REVISIÓN
ELAB.	01	JA	12/10/2017	DEFINICIÓN DE PROCEDIMIENTO	
MODIF.					
MODIF.					

AUTORIDAD AUTÓNOMA DE MAJES

"AÑO DEL BUEN SERVICIO AL CIUDADANO"

GOBIERNO REGIONAL

INFORME Nº XXX–XXXX–GRA–PEMS/TECNOLOGÍAS DE INFORMACIÓN

PARA :

ASUNTO :

REFERENCIA:

FECHA :

APROBACIÓN:	FECHA:

Gestionar la recepción de bienes o servicios de tecnologías de la información

Agente Externo de Servicios

Encargado de Servicios

Encargado de Compras

Encargado de Infraestructura de Tecnologías de Información

Jefe de Unidad de Tecnologías de Información

Recibir solicitud

Enviar especificaciones técnicas

Recibir informe

Pedido de servicios

R14

Recibir bien para revisión

Solicitar especificaciones técnicas

Recibir especificaciones técnicas

C22

¿Cumple especificaciones técnicas?

SI

Dar visto bueno

Entregar equipo

FIN

NO

Informe

Elaborar informe

Enviar equipo a almacén

Derivar informe

R15

INICI

Recibir bien

Enviar bien para revisión

Recibir informe

C23

¿Alguna observación?

NO

Derivar informe

SI

OBJETIVO:	Normar el proceso a seguir para el licenciamiento de software para su posterior instalación en los equipos de cómputo.
ALCANCE:	Comprende desde la solicitud del usuario PEMS hasta la instalación de *software* licenciado por parte de Mesa de Ayuda.

I. RESUMEN DEL PROCESO	
RESPONSABLE	**ACTIVIDADES**
Usuario PEMS / Jefe de Unidad de Tecnologías de Información / Encargado de Infraestructura de Tecnologías de Información / Mesa de Ayuda	1. Instalación de *software* licenciado

I. PROCESO AL DETALLE	
RESPONSABLE	**ACTIVIDADES**
1. INSTALACIÓN DE *SOFTWARE* LICENCIADO	
Usuario PEMS	1.1. Solicita instalación de *software* en su equipo de cómputo al Jefe de Unidad de Tecnologías de Información.
Jefe de Unidad de Tecnologías de Información	1.2. Recibe solicitud de instalación de *software*, para su revisión y conformidad y la deriva a Encargado de Infraestructura de Tecnologías de Información. De no dar conformidad, se deniega solicitud; caso contrario, continúa con el siguiente punto.
Encargado de Infraestructura de Tecnologías de Información	1.3. Recibe solicitud de instalación de *software*, da conformidad, asigna licencia a equipo de cómputo, actualiza formato de asignación de equipo y entrega licencia a Mesa de Ayuda para su instalación. De no haber licencia, solicita adquisición a Jefe de Unidad de Tecnologías de Información.
Jefe de Unidad de Tecnologías de Información	1.4. Realiza requerimiento de compra.
Mesa de Ayuda	1.5. Recibe licencia de *software* y realiza instalación de *software* en equipo de cómputo

REFERENCIA HISTÓRICA DE MODIFICACIONES					
	VER.	**REALIZADA POR**	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**	**REVISIÓN**
ELAB.	01	JA	12/10/2017	DEFINICIÓN DE PROCEDIMIENTO	
MODIF.					
MODIF.					

	FORMATO DE ASIGNACIÓN DE EQUIPO	FORMATO N°01
Autoridad Autónoma de Majes		INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN

Asignado:					**FECHA:**		
Unidad:					**SBN:**		
Sistema Operativo				**SBN:**			
Windows XP		**Windows 8**		**Windows Server 2008**		**Linux**	
Windows Vista		**Windows 8.1**		**Windows Server 2012**		**Otro**	
Windows 7		**Windows 10**		**Windows Server 2016**			
Ofimática				**SBN:**			
Office 2007		**Office 2013**		**Visio 2013**		**Otro**	
Office 2010		**Office 2016**		**Project 2013**			
Desarrollo e Ingeniería							
Visual Studio		**SQL Server 2000**		**SQL Server 2012**		**S10**	
Visual Fox Pro		**SQL Server 2005**		**SQL Server 2016**		**Autocad**	
Crystal Reports		**SQL Server 2008**		**Arcgis**		**Otro**	
Utilitarios							
Winrar		**Nitro PDF**		**Google Chrome**		**Antivirus**	
Google Earth		**Nero**		**Power DVD**		**Vencimiento:**	
Adobe Reader		**Mozilla Firefox**		**VLC Player**		**Otro**	
Sistemas y aplicaciones							
S.I.A.F.		**S.I.A.T.D.**		**Retenciones**		**PDT / PLE**	
S.I.G.A.		**LORD-PRO**		**Planillas**		**Otro**	
Diseño							
Adobe Photoshop		**Adobe After Effects**		**Adobe Fireworks**		**Otros**	

Adobe Dreamweaver		**Adobe Illustrator**		**Corel Draw**		

Toda reproducción o utilización de software sin tener la licencia correspondiente otorgada por el titular del derecho de autor o su representante se considera ilícita y posible de sanción administrativa y/o judicial, conforme a la R.M. N°073-2004-PCM "Administración eficiente del software legal en la administración pública".

_____ Jefe de Unidad de Tecnologías de Información	_____ Encargado de Infraestructura de Tecnologías de Información

Licenciamiento de software

Mesa de Ayuda

Realizar instalación en equipo de cómputo

FIN

Encargado de Infraestructura de Tecnologías de Información

C25

¿Hay licencia?

Recibir solicitud de instalación de software

SI

Actualizar formato de asignación de equipo

Enviar licencia

NO

Solicitar adquisición

Jefe de Unidad de Tecnologías de Información

Recibir solicitud de instalación de software

¿Es necesario?

C24

SI

Derivar solicitud de instalación de software

Recibir solicitud

Pedido de compra

Usuario PEMS

INICI

Solicitar instalación de software

R16

OBJETIVO:	Normar el proceso a seguir para la administración del portal web de la AUTODEMA.
ALCANCE:	Comprende desde la solicitud de actualización de la información, hasta la notificación al Jefe de Unidad de Tecnologías de la Información.

I. RESUMEN DEL PROCESO	
RESPONSABLE	**ACTIVIDADES**
Encargado de Seguridad de la Información /Jefe de Unidad de Tecnologías de Información / Jefe de Oficina de Administración	1. Actualizar información de portal web
Trámite Documentario / Jefe de Unidad de Tecnologías de Información / Encargado de Infraestructura de Tecnologías de Información	2. Subir resoluciones ejecutivas a portal web

I. PROCESO AL DETALLE	
RESPONSABLE	**ACTIVIDADES**
1. ACTUALIZAR INFORMACIÓN DE PORTAL WEB	
Jefe de Unidad	1.1. Solicita a Jefe de Unidad de Tecnologías de Información la actualización de información de portal web.
Jefe de Unidad de Tecnologías de Información	1.2. Recibe la solicitud de actualización de información, para su revisión y conformidad y la deriva a Encargado de Infraestructura de Tecnologías de Información. De no proceder, deniega solicitud; caso contrario, continúa con el siguiente punto.
Encargado de Infraestructura de Tecnologías de Información	1.3. Recibe la solicitud de actualización de información realiza las modificaciones solicitadas, elabora y envía informe a Jefe de Unidad con copia a Jefe de Unidad de Tecnologías de Información.
2. SUBIR RESOLUCIONES EJECUTIVAS A PORTAL WEB	
Trámite Documentario	2.1. Envía resolución ejecutiva a Jefe de Unidad de Tecnologías de Información.
Jefe de Unidad de Tecnologías de Información	2.2. Recibe y deriva resolución ejecutiva a Encargado de Infraestructura de Tecnologías de Información.
Encargado de Infraestructura de Tecnologías de la Información	2.3. Recibe, digitaliza y sube archivo .pdf a portal web.
Encargado de Infraestructura de Tecnologías de Información	2.4. Archiva resolución ejecutiva y notifica a Jefe de Unidad de Tecnologías de Información.

REFERENCIA HISTÓRICA DE MODIFICACIONES					
	VER.	**REALIZADA POR**	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**	**REVISIÓN**
ELAB.	01	JA	12/10/2017	DEFINICIÓN DE PROCEDIMIENTO	
MODIF.					
MODIF.					

APROBACIÓN:	**FECHA:**

AUTORIDAD AUTÓNOMA DE MAJES

"AÑO DEL BUEN SERVICIO AL CIUDADANO"

GOBIERNO REGIONAL

INFORME Nº XXX–XXXX–GRA–PEMS/TECNOLOGÍAS DE INFORMACIÓN

PARA :

ASUNTO :

REFERENCIA:

FECHA :

APROBACIÓN:	FECHA:

Administrar portal web

Encargado de Infraestructura de Tecnologías de Información

Recibir solicitud

Realizar actualización de información

Elaborar informe

Informe

Enviar informe a Jefe de Unidad de Tecnologías de Información con copia a Jefe de Unidad solicitante

Jefe de Unidad de Tecnologías de Información

C26

¿Es aplicable?

SI

NO

Recibir solicitud de actualización de información del portal web

Dar visto bueno

Derivar solicitud

Denegar solicitud

FIN

Jefe de Unidad

INICI

Solicitar actualización de información del portal web

R17

OBJETIVO:	Normar el proceso a seguir para la asignación de equipo de cómputo o impresora, *software,* así como los accesos a la red de la AUTODEMA y correo corporativo al nuevo colaborador.
ALCANCE:	Comprende desde la solicitud de equipo de cómputo hasta la configuración y entrega de accesos a usuario PEMS.

I. RESUMEN DEL PROCESO	
RESPONSABLE	**ACTIVIDADES**
Jefe de Unidad / Encargado de Patrimonio / Jefe de Unidad de Tecnologías de Información / Encargado de Infraestructura de Tecnologías de Información / Encargado de Patrimonio / Secretaria de Recursos Humanos /Mesa de Ayuda	1. Asignación de equipo
Secretaria de Recursos Humanos / Jefe de Unidad de Tecnologías de Información / Encargado de Seguridad de la Información / Mesa de Ayuda	2. Asignación de accesos

I. PROCESO AL DETALLE	
RESPONSABLE	**ACTIVIDADES**
1. ASIGNACIÓN DE EQUIPO	
Jefe de Unidad	1.1. Solicita equipo de cómputo u impresora a Encargado de Patrimonio.
Encargado de Patrimonio	1.2. Revisa inventario de activos y deriva la solicitud a Jefe de Tecnologías de Información. De no tener en inventario equipo de cómputo u impresora disponible, informa a Jefe de Unidad que haga un pedido de compra.
Jefe de Unidad de Tecnologías de Información	1.3. Deriva solicitud a Encargado de Infraestructura de Tecnologías de Información.
Encargado de Infraestructura de Tecnologías de Información	1.4. Realiza la verificación del estado del equipo, formatea equipo de cómputo e instala *software* solicitado por Jefe de Unidad.
Encargado de Infraestructura de Tecnologías de Información	1.5. Registra formato de asignación de equipo y envía una copia a Recursos Humanos y a Patrimonio.
Encargado de Patrimonio	1.6. Recibe ficha de asignación de equipo y hace descargo de equipo de cómputo u impresora.
Secretaria de Recursos Humanos	1.7. Recibe ficha de asignación de equipo y adjunta a *file* personal de trabajador.
Mesa de Ayuda	1.8. Realiza instalación de equipo de cómputo u impresora en estación de trabajo.
2. ASIGNACIÓN DE ACCESOS	
Encargado de Seguridad de la Información	2.1. Solicita a Jefe de la Unidad de Tecnologías de Información la creación de usuario en *Active Directory* con los siguientes datos: – Apellidos y nombres – Código – Profesión – Teléfono – Email – Denominación de cargo – Dependencia
Jefe de la Unidad de Tecnologías de Información	2.2. Recibe solicitud y la deriva a Secretaria de Recursos Humanos.

Secretaria de Recursos Humanos	2.3. Recibe solicitud y envía datos requeridos a Jefe de Unidad de Tecnologías de Información.
Jefe de Unidad de Tecnologías de Información	2.4. Recibe datos y los deriva a Encargado de Seguridad de la Información.
Encargado de Seguridad de la Información	2.5. Recibe datos, crea usuario en *Active Directory* para su acceso al dominio y crea correo electrónico corporativo.
Encargado de Seguridad de la Información	2.6. Envía información a Mesa de ayuda.
Mesa de Ayuda	2.7. Recibe información, realiza la configuración del usuario en equipo de cómputo y accesos a equipo y correo corporativo.

REFERENCIA HISTÓRICA DE MODIFICACIONES					
	VER.	REALIZADA POR	FECHA	DESCRIPCIÓN DEL CAMBIO	REVISIÓN
ELAB.	01	JA	12/10/2017	DEFINICIÓN DE PROCEDIMIENTO	
MODIF.					
MODIF.					

Autoridad Autónoma de Majes	**FORMATO DE ASIGNACIÓN DE EQUIPO**					**FORMATO N°01**		
						INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN		
Asignado:						**FECHA:**		
Unidad:						**SBN:**		
Sistema Operativo				**SBN:**				
Windows XP		**Windows 8**		**Windows Server 2008**		**Linux**		
Windows Vista		**Windows 8.1**		**Windows Server 2012**		**Otro**		
Windows 7		**Windows 10**		**Windows Server 2016**				
Ofimática				**SBN:**				
Office 2007		**Office 2013**		**Visio 2013**		**Otro**		
Office 2010		**Office 2016**		**Project 2013**				
Desarrollo e Ingeniería								
Visual Studio		**SQL Server 2000**		**SQL Server 2012**		**S10**		
Visual Fox Pro		**SQL Server 2005**		**SQL Server 2016**		**Autocad**		
Crystal Reports		**SQL Server 2008**		**Arcgis**		**Otro**		
Utilitarios								
Winrar		**Nitro PDF**		**Google Chrome**		**Antivirus**		
Google Earth		**Nero**		**Power DVD**		**Vencimiento:**		
Adobe Reader		**Mozilla Firefox**		**VLC Player**		**Otro**		
Sistemas y aplicaciones								
S.I.A.F.		**S.I.A.T.D.**		**Retenciones**		**PDT / PLE**		
S.I.G.A.		**LORD-PRO**		**Planillas**		**Otro**		
Diseño								

Adobe Photoshop		**Adobe After Effects**		**Adobe Fireworks**		**Otros**
Adobe Dreamweaver		**Adobe Illustrator**		**Corel Draw**		

Toda reproducción o utilización de software sin tener la licencia correspondiente otorgada por el titular del derecho de autor o su representante se considera ilícita y posible de sanción administrativa y/o judicial, conforme a la R.M. N°073-2004-PCM "Administración eficiente del software legal en la administración pública".

_____ Jefe de Unidad de Tecnologías de Información	_____ Encargado de Infraestructura de Tecnologías de Información

Asignar equipo y accesos a nuevo colaborador

Mesa de Ayuda

Recibir equipo e información

Instalar y configurar equipo

FIN

Encargado de Seguridad de la Información

Solicitar datos del trabajador

Crear usuario en Active Directory

Enviar equipo e información

Encargado de Infraestructura de Tecnologías de Información

Recibir solicitud

R18

Verificar estado del equipo

C27

¿Funcionamiento correcto?

SI

NO

¿Equipo de cómputo?

SI

Formatear equipo de cómputo

Licenciamiento de software

NO

Jefe de Unidad de Tecnologías de Información

Recibir solicitud

Derivar solicitud

Recibir solicitud

Derivar solicitud

Recibir datos

Enviar datos

Secretaria de Recursos Humanos

Recibir solicitud

Enviar datos

Encargado de Patrimonio

Revisar inventario de activos

¿Hay equipo en inventario?

SI

Derivar solicitud

NO

Informar para pedido de compra

Jefe de Unidad

INICIO

Solicitar equipo de cómputo u impresora

Realizar pedido de compra

Orden de compra

RIESGOS Y CONTROLES DE LOS PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA AUTODEMA

Proceso			Riesgo				Evaluación inherente			Control													Evaluación residual			Planes de acción			
Macroproceso	Proceso	Subproceso	Código del Riesgo	Riesgo	Causa	Factor de Riesgo	Probabilidad	Impacto	Nivel de Riesgo Inherente	Código del Control	Descripción del Control	ISO 27001	COBIT 5.0	Responsable	Tipo	Ejecución	Documentación	Periodicidad	Responsabilidad	Segregación de funciones	¿Reduce la probabilidad?	¿Reduce el impacto?	Probabilidad	Impacto	Nivel de Riesgo Residual	Tratamiento	Código de Plan de Acción	Plan de Acción	Responsable
		Copias de Seguridad - BACKUP	R1	Realizar una evaluación incompleta o errónea de los mantenimientos correctivos.	Falta de juicio de expertos.	Personal	2	4	Alto	C1	Una vez que el Encargado de Seguridad de la Información desarrolla el Plan anual de copias de seguridad el Jefe de Unidad de Tecnologías de Información lo verifica, en caso de que tenga alguna discrepancia o algo no le parezca se lo devuelve al Encargado de Seguridad de la Información para su modificación.	4.2 Comprender las necesidades y expectativas de las partes interesadas 5. Políticas, 6.1 Acciones para abordar los riesgos y oportunidades, 7.5 Documentar Información 9.3 Revisión de la gestión, 10.2 Mejora continua .	APO 01.06 Definir información y propietarios del sistema, APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 04.02 Mantener un entendimiento del ambiente de la empresa, APO 08.05, Apoyo a la mejora continua APO 09.01 Identificar los servicios de TI, APO 09.02 Catálogo de servicios permitidos por TI APO 12.04 Articular el riesgo, APO12.05 Definir un portafolio de gestión de riesgos.	Jefe de Unidad de Tecnologías de Información	Preventivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	No	1	4	Alto	Transferir	PA1	El Encargado de Seguridad de la Información debe hacer la modificación del Plan Anual de Seguridad de la Información según las correcciones del Jefe de Unidad de Tecnologías de Información.	Encargado de Seguridad de la Información
					Mala documentación de los mantenimientos correctivos.	Procesos internos	4	4	Extremo	C2	El Jefe de Oficina de Administración revisa el Plan Anual de Copias de Seguridad, en caso de que tenga alguna discrepancia o algo no le parezca se lo devuelve al Encargado de Seguridad de la Información para su modificación.	5. Políticas, 9.3 Revisión de la gestión, 10.2 Mejora continua.	APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 08.05, Apoyo a la mejora continua, APO 12.04 Articular el riesgo.	Jefe de Oficina de Administración	Preventivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	No	1	4	Alto	Transferir	PA2	El Encargado de Seguridad de la Información debe hacer la modificación del Plan Anual de Seguridad de la Información según las correcciones del Jefe de la Oficina de Administración	Encargado de Seguridad de la Información
			R2	Realizar copia de seguridad corrupta.	La copia de seguridad de la base de datos se interrumpió o se generó dañada.	Procesos internos	2	5	Extremo	C3	El Jefe de Unidad de Tecnologías de Información realiza la verificación de la copia de seguridad a almacenarse.	5. Políticas, 9.3 Revisión de la gestión, 10.2 Mejora continua.	APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 08.05, Apoyo a la mejora continua, APO 12.04 Articular el riesgo.	Jefe de Unidad de Tecnologías de Información	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	No	1	5	Alto	Mitigar	PA3	El Jefe de Unidad de Tecnologías de Información debe verificar cada una de las copias de seguridad realizadas para garantizar la integridad.	Jefe de Unidad de Tecnologías de Información
			R3	Almacenar copia de seguridad corrupta.	La copia de seguridad de la base de datos se generó dañada.	Tecnología de la Información	2	5	Extremo																			
		Realizar Soporte informático	R4	Solicitar atención de requerimiento de soporte informático inmediato.	El usuario PEMS piensa que su requerimiento es el más importante.	Personal	5	3	Extremo	C4	Mesa de Ayuda al hacer el primer contacto con el usuario PEMS, asigna la prioridad respectiva al requerimiento realizado a partir de los demás requerimientos que están en cola.	5. Políticas, 6.1Acciones para dirigir los riesgos y oportunidades, 7.5 Documentar Información, 9.3 Revisión de la gestión, 10.2 Mejora continua.	APO 01.06 Definir información y propietarios del sistema, APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 02.03 Definir las capacidades de TI y sus objetivos, APO 08.05 Aportar a la mejora continua de los servicios, APO 12.02 Analizar el riesgo, APO 12.03 Mantener el portafolio de riesgo.	Mesa de Ayuda	Preventivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	Si	3	2	Moderado	Mitigar	PA4	La Mesa de Ayuda prioriza cada una de las solicitudes de atención de requerimientos	Mesa de Ayuda
			R5	Realizar soporte informático que no esté en la base de conocimiento.	Requerimiento no descrito en base de conocimiento.	Procesos internos	4	3	Alto	C5	Mesa de Ayuda si realiza soporte informático, hace el llenado de una ficha de requerimiento solucionado que servirá como base de conocimiento para la solución de requerimientos similares. En caso contrario lo deriva a un nivel superior para su solución.	5. Políticas, 6.1Acciones para dirigir los riesgos y oportunidades, 7.5 Documentar Información, 9.3 Revisión de la gestión, 10.2 Mejora continua.	APO 01.06 Definir información y propietarios del sistema, APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 02.03 Definir las capacidades de TI y sus objetivos, APO 08.05 Aportar a la mejora continua de los servicios, APO 12.02 Analizar el riesgo, APO 12.03 Mantener el portafolio de riesgo.	Mesa de Ayuda	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	Si	2	2	Bajo	Aceptar	N/A	N/A	N/A
			R6	Realizar soporte informático no solucionado por Mesa de Ayuda.	Requerimiento no descrito en base de conocimiento.	Procesos internos	3	3	Alto	C6	Mesa de Servicio si realiza soporte informático, hace el llenado de una ficha de requerimiento solucionado que servirá como base de conocimiento para la solución de requerimientos similares. En caso contrario lo deriva a un nivel superior para su solución.	5. Políticas, 6.1Acciones para dirigir los riesgos y oportunidades, 7.5 Documentar Información, 9.3 Revisión de la gestión, 10.2 Mejora continua.	APO 01.06 Definir información y propietarios del sistema, APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 02.03 Definir las capacidades de TI y sus objetivos, APO 08.05 Aportar a la mejora continua de los servicios, APO 12.02 Analizar el riesgo, APO 12.03 Mantener el portafolio de riesgo.	Mesa de Servicios	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	Si	2	1	Bajo	Aceptar	N/A	N/A	N/A
			R7	Realizar soporte informático no solucionado por Mesa de Servicio.	Requerimiento no descrito en base de conocimiento.	Procesos internos	2	3	Moderado	C7	Encargado de Infraestructura de Tecnologías de Información si realiza soporte informático, hace el llenado de una ficha de requerimiento solucionado que servirá como base de conocimiento para la solución de requerimientos similares. En caso contrario elabora un Informe Técnico para su entrega al Jefe de Unidad de Tecnologías de la Información.	5. Políticas, 6.1Acciones para dirigir los riesgos y oportunidades, 7.5 Documentar Información, 9.3 Revisión de la gestión, 10.2 Mejora continua.	APO 01.06 Definir información y propietarios del sistema, APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 02.03 Definir las capacidades de TI y sus objetivos, APO 08.05 Aportar a la mejora continua de los servicios, APO 12.02 Analizar el riesgo, APO 12.03 Mantener el portafolio de riesgo.	Encargado de Infraestructura de Tecnologías de Información	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	Si	1	1	Bajo	Transferir	PA5	Se deriva el informe técnico al Jefe de Unidad de Tecnologías de Información, el cual será para la adquisición de nuevos bienes o servicios.	Jefe de Unidad de Tecnologías de Información
										C8	Revisa el Informe Técnico realizado por el Encargado de Infraestructura de Tecnologías de la Información para su posterior entrega al usuario PEMS. En caso de que necesite correcciones lo devuelve.	5. Políticas, 6.1Acciones para dirigir los riesgos y oportunidades, 7.5 Documentar Información, 9.3 Revisión de la gestión, 10.2 Mejora continua.	APO 01.06 Definir información y propietarios del sistema, APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 02.03 Definir las capacidades de TI y sus objetivos, APO 08.05 Aportar a la mejora continua de los servicios, APO 12.02 Analizar el riesgo, APO 12.03 Mantener el portafolio de riesgo.	Jefe de Unidad de Tecnologías de Información	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	No	Si	1	1	Bajo	Mitigar	PA6	Se revisa el informe técnico para dar la conformidad del mismo y entregárselo al usuario PEMS.	Jefe de Unidad de Tecnologías de Información

RIESGOS Y CONTROLES DE LOS PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA AUTODEMA

Proceso			Riesgo				Evaluación inherente			Control												Evaluación residual			Planes de acción			
Macroproceso	Proceso	Subproceso	Código del Riesgo	Riesgo	Causa	Factor de Riesgo	Probabilidad	Impacto	Nivel de Riesgo Inherente	Código del Control	Descripción del Control	ISO 27001	COBIT 5.0	Responsable	Tipo	Ejecución	Documentación	Periodicidad	Responsabilidad	Segregación de funciones	¿Reduce la probabilidad?	¿Reduce el impacto?	Probabilidad	Impacto	Nivel de Riesgo Residual	Tratamiento	Código de Plan de Acción	Plan de Acción	Responsable
Tecnologías de la Información	Gestión de las Tecnologías de la Información	Realizar Reporte Mensual	R8	Realizar informe mensual que no refleja a lo realizado en el mes.	El responsable de su elaboración no refleja las actividades realizadas en el mes en su Informe Mensual.	Personal	2	3	Moderado	C9	Revisa el Informe Mensual y corrobora que las actividades realizadas estén acorde a las metas planteadas para el mes, en caso éstas no hayan sido cumplidas, se analiza la razón y se reprograman. Si éstas han sido cumplidas, se asignan nuevas metas a cumplir.	4.2 Comprender las necesidades y expectativas de las partes interesadas, 5.1 Liderazgo y compromiso, 5.3 Roles organizacionales y responsabilidades. 6 Planeamiento 6.1 Acciones para dirigir los riesgos y oportunidades. 6.2 Objetivos de Seguridad de Información y planes para alcanzarlos, 7.2 Competencias, 9.1 Monitoreo, medición, análisis y evaluación, 9.3 Revisión de la gestión.	APO 01.02 Establecer roles y responsabilidades, APO 01.04 Comunicar objetivos y dirección de administración, APO01.08 Mantener la conformidad con políticas y procedimientos, APO 04.03 Monitorear y observar el ambiente tecnológico, APO 07.01 Mantener una asignación de tareas adecuada y apropiada, APO 07.04 Evaluar el desempeño laboral del personal, APO 08.01 Entender las expectativas del negocio, APO 08.02 Identificar las oportunidades, riesgos y limitaciones de TI para la mejora del negocio, APO 09.04 Monitorear y reportar los niveles de servicio, APO 12.04 Articular el riesgo, APO 12.05 Definir un portafolio de gestión de riesgos, APO 12.06 Respuesta al riesgo, , APO 13.02 Definir y administrar un plan de tratamiento de riesgos de seguridad de la información	Jefe de Unidad de Tecnologías de Información	Correctivo	Manual	Documentado	Mensual	Asignada	Adecuada	Si	Si	1	2	Bajo	Mitigar	PA7	Se analizan las actividades realizadas con las metas del mes, si éstas van a ser actualizadas, se realizan a partir de las metas del mes vigente y anterior.	Jefe de Unidad de Tecnologías de Información
		Administrar Sistemas S.I.G.A. y S.I.A.F.	R9	Realizar un requerimiento que no amerita ser atendido.	El usuario PEMS realiza un requerimiento innecesario para el desarrollo del negocio.	Personal	4	1	Moderado	C10	El Jefe de Unidad decide si el requerimiento solicitado por el usuario PEMS amerita ser derivado a la Unidad de Tecnologías de Información.	4.2 Comprender las necesidades y expectativas de las partes interesadas.	APO 01.02 Establecer roles y responsabilidades, APO 02.01 Entender la dirección de la empresa, APO 04.02 Mantener un entendimiento del ambiente de la empresa.	Jefe de Unidad	Detectivo	Manual	Sin Documentar	Cada vez que ocurre	No Asignada	N/E	Si	No	3	1	Bajo	Transferir	PA8	Se realiza el filtrado de requerimientos.	Jefe de Unidad
										C11	Verifica si el requerimiento solicitado necesita intervernción del MEF para ser cumplio o puede realizarse en la institución.	4.2 Comprender las necesidades y expectativas de las partes interesadas.	APO 01.02 Establecer roles y responsabilidades, APO 02.01 Entender la dirección de la empresa, APO 04.02 Mantener un entendimiento del ambiente de la empresa.	Jefe de Unidad de Tecnologías de Información	Detectivo	Manual	Sin Documentar	Cada vez que ocurre	No Asignada	Adecuada	Si	No	2	1	Bajo	Transferir	PA9	Se realiza el filtrado de requerimientos.	Jefe de Unidad de Tecnologías de Información
										C12	Se verifica si el requerimiento es de gestión de credenciales o de gestión de ítems para su derivación.	4.2 Comprender las necesidades y expectativas de las partes interesadas.	APO 01.02 Establecer roles y responsabilidades, APO 02.01 Entender la dirección de la empresa, APO 04.02 Mantener un entendimiento del ambiente de la empresa.	Mesa de Ayuda	Detectivo	Manual	Sin Documentar	Cada vez que ocurre	No Asignada	Adecuada	Si	No	1	1	Bajo	Aceptar	N/A	N/A	N/A
										C13	Se verifica si el requerimiento ha sido satisfecho, en caso éste no haya podido ser solucionado lo deriva a un nivel más alto del MEF.	4.2 Comprender las necesidades y expectativas de las partes interesadas.	APO 01.02 Establecer roles y responsabilidades, APO 02.01 Entender la dirección de la empresa, APO 04.02 Mantener un entendimiento del ambiente de la empresa.	Sectorista Regional MEF	Correctivo	Combinado	Sin Documentar	Cada vez que ocurre	Asignada	Adecuada	Si	No	1	1	Bajo	Transferir	PA10	Se realiza el filtrado de requerimientos.	Sesctorista Regional
										C14	Se verifica si el usuario realizó el requerimiento de creación de credenciales, para la asignación de permisos respectiva para que pueda trabajar en el sistema.	4.2 Comprender las necesidades y expectativas de las partes interesadas.	APO 01.02 Establecer roles y responsabilidades, APO 02.01 Entender la dirección de la empresa, APO 04.02 Mantener un entendimiento del ambiente de la empresa.	Encargado de Seguridad de la Información	Detectivo	Manual	Sin Documentar	Cada vez que ocurre	Asignada	Adecuada	Si	No	1	1	Bajo	Mitigar	PA11	Se realiza la creación de credenciales de acceso al sistema.	Encargado de Seguridad de la Información
										C15	Se verifica si el requerimiento cumple con brindar la información necesaria para la creación del ítem. En caso no cumpla, se realiza la devolución de la solicitud para su corrección.	4.2 Comprender las necesidades y expectativas de las partes interesadas.	APO 01.02 Establecer roles y responsabilidades, APO 02.01 Entender la dirección de la empresa, APO 04.02 Mantener un entendimiento del ambiente de la empresa.	Sectorista Regional MEF	Detectivo	Manual	Sin Documentar	Cada vez que ocurre	Asignada	Adecuada	Si	No	1	1	Bajo	Transferir	PA12	Se envía al MEF la información necesaria para la creación del ítem	Encargado de Seguridad de la Información
		Supervisar Servicios Tercerizados	R10	Realizar un requerimiento que no se encuentra planeado.	El usuario PEMS realiza un requerimiento innecesario para el desarrollo del negocio o no cuenta la Unidad para su ejecución.	Personal	3	3	Alto	C16	Se revisa el requerimiento realizado por el usuario PEMS. En caso de no ser viable se rechaza la solicitud.	5. Políticas, 6.1 Acciones para dirigir los riesgos y oportunidades. 7.4 Comunicaciones, 10.2 Mejora continua.	APO 01.07 Administrar la mejora continua de procesos, APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 05.03 Evaluar y elegir programa a financiar, APO 07.03 Mantener las habilidades y competencias del personal, APO 09.01 Identificar los servicios de TI.	Jefe de Unidad de Tecnologías de Información	Detectivo	Manual	Sin Documentar	Cada vez que ocurre	Asignada	Adecuada	No	Si	3	1	Bajo	Mitigar	PA13	Se realiza el filtrado de requerimientos.	Jefe de Unidad de Tecnologías de Información
										C17	Se revisa el informe con los términos de referencia. En caso esté mal elaborado, se devuelve para su corrección.	5. Políticas, 6.1 Acciones para dirigir los riesgos y oportunidades. 7.4 Comunicaciones, 10.2 Mejora continua, 15. Gestión de cambios de los servicios del proveedor.	APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 05.03 Evaluar y elegir programa a financiar, APO 07.03 Mantener las habilidades y competencias del personal, APO 07.06 Administrar personal de contrato, APO 09.01 Identificar los servicios de TI, APO 10.03 Gestionar las relaciones y contratos con el proveedor .	Jefe de Oficina de Administración	Detectivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	No	Si	3	2	Moderado	Transferir	PA14	Se revisa el Informe de Términos de Referencia según los requerimientos del negocio.	Jefe de Oficina de Administración
			R11	El servicio recibido no cumple el requerimiento.	El personal del servicio no cumple lo establecido en los Términos de Referencia.	Eventos Externos	2	4	Alto	C18	Se revisa el servicio recibido y se compara con lo requerido en los Términos de Referencia, si éste no cumple con lo especificado, el servicio tiene la obligación de corregirlo, una vez que cumpla lo establecido, se dá la conformidad de servicio.	5. Políticas, 6.1 Acciones para dirigir los riesgos y oportunidades. 7.4 Comunicaciones, 10.2 Mejora continua, 15. Gestión de cambios de los servicios del proveedor.	APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 05.03 Evaluar y elegir programa a financiar, APO 07.03 Mantener las habilidades y competencias del personal, APO 07.06 Administrar personal de contrato, APO 09.01 Identificar los servicios de TI, APO 10.03 Gestionar las relaciones y contratos con el proveedor APO 10.05 Monitorear el desempeño y cumplimiento del proveedor.	Jefe de Unidad de Tecnologías de Información	Correctivo	Combinado	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	Si	1	2	Bajo	Mitigar	PA15	Revisar y monitorear el cumplimiento del servicio tercerizado hasta que cumpla con o establecido en los Términos de Referencia y dar la Conformidad de Servicio, caso contrario hacer efectiva la cláusula de incumplimiento.	Jefe de Unidad de Tecnologías de Información
													APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 02.03 Definir las capacidades de TI y sus objetivos														

RIESGOS Y CONTROLES DE LOS PROCESOS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA AUTODEMA

Proceso			Riesgo				Evaluación inherente			Control											Evaluación residual			Planes de acción			
Macroproceso	Proceso	Subproceso	Código del Riesgo	Riesgo	Causa	Factor de Riesgo	Probabilidad	Impacto	Nivel de Riesgo Inherente	Código del Control	Descripción del Control	ISO 27001	COBIT 5.0	Responsable	Tipo	Ejecución	Documentación	Periodicidad	Responsabilidad	Segregación de funciones	¿Reduce la probabilidad?	¿Reduce el impacto?	Probabilidad	Impacto	Nivel de Riesgo Residual	Tratamiento	Código de Plan de Acción	Plan de Acción	Responsable
		Supervisar Cumplimiento de Directivas de Seguridad de la Información	R12	Realizar un análisis que no refleje la situación actual.	El encargado de Seguridad de la Información realiza un análisis de la situación de seguridad de la información sin detalle o incompleto.	Personal	3	3	Alto	C19	Se revisan las directivas de Seguridad de la Información anteriores para corroborar la situación de la Seguridad de la Información. En caso no estén correctas se realiza la actualización de las mismas	4.2 Comprender las necesidades y expectativas de las partes interesadas, 5. Políticas, 6 Planeamiento, 6.1 Acciones para dirigir los riesgos y oportunidades, 7.5 Control de la información documentada, 8.3 Tratamiento de riesgos de Seguridad de la Información, 9.1 Monitoreo, medición, análisis y evaluación, 9.3 Revisión de la gestión, 10.2 Mejora continua,	APO 04.03 Monitorear y observar el ambiente tecnológico, APO 08.01 Entender las expectativas del negocio, APO 08.02 Identificar las oportunidades, riesgos y limitaciones de TI para mejorar el negocio, APO 08.05 Aportar a la mejora continua de los servicios, APO 09.02 Catálogo de servicios permitidos por TI, APO 09.04 Monitorear y reportar los niveles de servicio, APO 12.02 Analizar el riesgo, APO 12.03 Mantener el portafolio de riesgo, APO 12.04 Articular el riesgo, APO 12.05 Definir un portafolio de gestión de riesgos, APO 12.06 Respuesta al riesgo, APO 13.02 Definir y administrar un plan de tratamiento de riesgos de seguridad de la información.	Encargado de Seguridad de la Información	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	Si	2	1	Bajo	Mitigar	PA16	Se realizan las correcciones realizadas por el Jefe de Unidad de Tecnologías de Información.	Encargado de Seguridad de la Información
			R13	Se definen directivas de seguridad de la información innecesarias o mal definidas.	El encargado de Seguridad de la Información define directivas que no son necesarias para mantener la disponibilidad, integridad y confidencialidad de los datos.	Personal	2	4	Alto	C20	Se revisan las Directivas de Seguridad de la Información presentada por el Encargado de Seguridad de Información. En caso no estén correctas, realiza observaciones y se las devuelve.	4.2 Comprender las necesidades y expectativas de las partes interesadas, 5. Políticas 6.1 Acciones para dirigir los riesgos y oportunidades, 6.2 Objetivos de Seguridad de Información y planes para alcanzarlos, 7.4 Comunicaciones, 7.5 Control de la información documentada, 8.3 Tratamiento de riesgos de Seguridad de la Información, 9.1 Monitoreo, medición, análisis y evaluación, 9.3 Revisión de la gestión, 10. Mejora continua.	APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 02.03 Definir las capacidades de TI y sus objetivos, APO 02.06 Comunicar la estrategia y la dirección de TI, APO 04.03 Monitorear y observar el ambiente tecnológico, APO 08.01 Entender las expectativas del negocio, APO 08.02 Identificar las oportunidades, riesgos y limitaciones de TI para mejorar el negocio, APO 08.05 Aportar a la mejora continua de los servicios, APO 09.02 Catálogo de servicios permitidos por TI, APO 09.04 Monitorear y reportar los niveles de servicio, APO 12.02 Analizar el riesgo, APO 12.03 Mantener el portafolio de riesgo, APO 12.04 Articular el riesgo, APO 12.05 Definir un portafolio de gestión de riesgos, APO 12.06 Respuesta al riesgo, APO 13.02 Definir y administrar un plan de tratamiento de riesgos de seguridad de la información.	Jefe de Unidad de Tecnologías de Información	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	No	1	4	Alto	Transferir	PA17	Se realizan las correcciones solicitadas por el Jefe de Unidad de Tecnologías de Información.	Jefe de Unidad de Tecnologías de Información
										C21	Se revisan las directivas de Seguridad de la Información presentada por el Encargado de Seguridad de Información y revisadas por el Jefe de Unidad de Tecnologías de Información. En caso no estén correctas, realiza observaciones y se las devuelve.	4.2 Comprender las necesidades y expectativas de las partes interesadas, 5. Políticas 5.1 Liderazgo y compromiso, 5.1 Acciones para dirigir los riesgos y oportunidades, 6.2 Objetivos de Seguridad de Información y planes para alcanzarlos, 7.4 Comunicaciones, 7.5 Control de la información documentada, 8.3 Tratamiento de riesgos de Seguridad de la Información, 9.1 Monitoreo, medición, análisis y evaluación, 9.3 Revisión de la gestión, 10. Mejora continua.	APO 01.04 Comunicar objetivos y dirección de administración, APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 02.03 Definir las capacidades de TI y sus objetivos, APO 02.06 Comunicar la estrategia y la dirección de TI, APO 04.03 Monitorear y observar el ambiente tecnológico, APO 08.01 Entender las expectativas del negocio, APO 08.02 Identificar las oportunidades, riesgos y limitaciones de TI para mejorar el negocio, APO 08.04 Coordinar y comunicar, APO 08.05 Aportar a la mejora continua de los servicios, APO 09.02 Catálogo de servicios permitidos por TI, APO 09.04 Monitorear y reportar los niveles de servicio, APO 12.02 Analizar el riesgo, APO 12.03 Mantener el portafolio de riesgo, APO 12.04 Articular el riesgo, APO 12.05 Definir un portafolio de gestión de riesgos, APO 12.06 Respuesta al riesgo, APO 13.02 Definir y administrar un plan de tratamiento de riesgos de seguridad de la información.	Jefe de Oficina de Administración	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	Si	No	1	4	Alto	Mitigar	PA18	Se realizan las correcciones solicitadas por el Jefe de Unidad de Tecnologías de Información.	Encargado de Seguridad de la Información
	Gestionar la Recepción de Bienes o Servicios de Tecnologías de Información		R14	Revisión incompleta del bien.	Encargado de Infraestructura de Tecnologías de Información solo corrobora el funcionamiento del bien, mas no sus Especificaciones Técnicas.	Personal	2	3	Moderado	C22	Después de haber recibido el bien y las especificaciones técnicas se realiza la corroboración de cada una de las características que debería tener el equipo. En caso no sean cumplidas se elabora un informe para el proveedor.	5. Políticas, 7.4 Comunicaciones, 6.1 Acciones para dirigir los riesgos y oportunidades, 7.5 Control de la información documentada	APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 05.03 Evaluar y elegir programa a financiar, APO 09.01 Identificar los servicios de TI, APO 09.02 Catálogo de servicios permitidos por TI.	Encargado de Infraestructura de Tecnologías de Información	Detectivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	No	Si	2	2	Bajo	Transferir	PA19	Elaborar un informe con copia al proveedor y al usuario solicitante con el incumplimiento de características que presenta el bien según las Especificaciones Técnicas.	Encargado de Infraestructura de Tecnologías de Información
										C23	Se realiza la revisión del informe realizado por el Encargado de Infraestructura de Tecnologías de Información. En caso existan observaciones, lo devuelve para su corrección.	5. Políticas, 6.1 Acciones para dirigir los riesgos y oportunidades, 7.5 Control de la información documentada.	APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 09.01 Identificar los servicios de TI, APO 09.02 Catálogo de servicios permitidos por TI.	Jefe de Unidad de Tecnologías de Información	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	No	Si	2	2	Bajo	Transferir	PA20	Se realizan las correcciones solicitadas por el Jefe de Unidad de Tecnologías de Información.	Encargado de Infraestructura de Tecnologías de Información
	Licenciamiento de Software		R15	El usuario solicita la instalación de software innecesario para el negocio o que perjudique el funcionamiento del negocio.	El usuario PEMS solicita instalación de software desconociendo la necesidad de licenciamiento, el contrato de licencia del mismo o su fin.	Personal	4	2	Alto	C24	Se revisa si la solicitud de instalación es necesaria para el correcto funcionamiento del negocio. En caso no lo sea, es rechazada.	5. Políticas 5.1 Liderazgo y compromiso, 7.4 Comunicaciones, 6.1 Acciones para dirigir los riesgos y oportunidades, 7.5 Control de la información documentada .	APO 01.04 Comunicar objetivos y dirección de administración, APO 01.08 Mantener la conformidad con políticas y procedimientos, APO 09.01 Identificar los servicios de TI, APO 09.02 Catálogo de servicios permitidos por TI .	Jefe de Unidad de Tecnologías de Información	Detectivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	No	Si	4	1	Moderado	Evitar	N/A	N/A	N/A
										C25	Se revisa si el software requiere licencia de paga. En caso necesite licenciamiento se solicita la adquisición de licencia.	5.1 Liderazgo y compromiso, 7.4 Comunicaciones, 7.5 Control de la información documentada, 15.2 Gestión de cambios de los servicios del proveedor.	APO 01.04 Comunicar objetivos y dirección de administración, APO 05.03 Evaluar y elegir programa a financiar, APO 09.02 Catálogo de servicios permitidos por TI, APO 10.03 Gestionar las relaciones y contratos con el proveedor, APO 10.05 Monitorear el desempeño y cumplimiento del proveedor.	Encargado de Infraestructura de Tecnologías de Información	Correctivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	No	Si	4	1	Moderado	Aceptar	N/A	Se solicita al área que realizó el requerimiento el Pedido de Compra del software.	Área solicitante
	Administrar Portal Web		R17	El Jefe de Unidad solicita actualizar información en el sitio web que incumpla con la Ley de Transparencia o la Ley de Protección de Datos Personales.	Desconocimiento de la Ley de Transparencia o la Ley de Protección de Datos Personales por parte del solicitante.	Personal	3	2	Moderado	C26	Se revisa la información a publicar en el sitio web. En caso transgredan la Ley de Transparencia o la Ley de Protección de Datos Personales, se rechaza.	4.2 Comprender las necesidades y expectativas de las partes interesadas, 5. Políticas, 15.2 Gestión de cambios de los servicios del proveedor.	APO 01.08 Mantener la conformidad con políticas y procedimientos APO 02.01 Entender la dirección de la empresa, APO 09.02 Catálogo de servicios permitidos por TI, APO 10.03 Gestionar las relaciones y contratos con el proveedor, APO 10.05 Monitorear el desempeño y cumplimiento del proveedor.	Jefe de Unidad de Tecnologías de Información	Detectivo	Manual	Documentado	Cada vez que ocurre	Asignada	Adecuada	No	Si	3	1	Bajo	Evitar	N/A	N/A	N/A
	Asignar Equipo y Accesos a Nuevo Colaborador		R18	El equipo entregado no tiene correcto funcionamiento.	Cuando se realizó la compra del bien, no pasó por la Unidad de Tecnologías de Información para su aprobación.	Procesos internos	2	3	Moderado	C27	Encargado de Infraestructura de Tecnologías de Información hace la revisión del bien para corroborar su buen funcionamiento. En caso éste no funcione correctamente, lo devuelve a Patrimonio.	4.2 Comprendiendo las necesidades y expectativas de las partes interesadas, 5.3 Roles organizacionales, responsabilidades y autoridades, 7.5 Control de la información documentada.	APO 01.02 Establecer roles y responsabilidades, APO 02.0.1 Entender la dirección de la empresa, APO 02.02 Evaluar el entorno actual, las capacidades y el rendimiento, APO 04.02 Mantener un entendimiento del ambiente de la empresa, APO 09.02 Catálogo de servicios permitidos por TI.	Encargado de Infraestructura de Tecnologías de Información	Detectivo	Manual	Sin Documentar	Cada vez que ocurre	Asignada	Adecuada	No	Si	2	2	Bajo	Transferir	PA21	En caso el bien no funcione correctamente se devuelve a Patrimonio para que realice el procedimiento de cambio de bien con el proveedor o su entrega al Jefe de Unidad solicitante del Pedido de Compra.	Encargado de Patrimonio