PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR - MATRIZ

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y CONTABLES

TESIS DE MAGÍSTER EN ADMINISTRACIÓN DE EMPRESAS CON MENCIÓN EN GERENCIA DE LA CALIDAD Y PRODUCTIVIDAD

CALIDAD DE LA GESTIÓN EN LA SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO/IEC 27001, EN INSTITUCIONES PÚBLICAS, EN LA CIUDAD DE QUITO D.M.

ING. LUIS MIGUEL PAZMIÑO VALLEJO

DIRECTOR: INGENIERO PAÚL IDROBO DÁVALOS, MBA.

QUITO, 2015

DIRECTOR DE TESIS

Ing. Paúl Idrobo Dávalos, MBA.

INFORMANTES

Ing. Álvaro Burgos Yánez, MSc.

Ing. Hernán Carrillo Villarroel, MSc.

DEDICATORIA

Dedico este trabajo investigativo primero a Dios, quien es la luz de mi vida, a mi amada esposa Gisselita Jurado, quien con su amor incondicional estuvo día a día escuchándome, apoyándome y alentándome, para acabar este proyecto y a mis padres, hermano, abuelita, y a mi tío Santiago Vallejo, porque han estado siempre a mi lado, y han sido mis ejemplos de vida.

Mil gracias a mis amigos que estuvieron presentes en los buenos y malos momentos, y a todas las personas que de una u otra manera me ayudaron a conseguir este logro.

AGRADECIMIENTO

A la Pontificia Universidad Católica del Ecuador por todo el conocimiento y experiencias de vida transmitidos durante año y medio a través de los profesores, y mi mayor respeto y consideración al Ingeniero Paúl Idrobo, quien dio un gran aporte a esta investigación.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

El objetivo de la presente investigación es medir la calidad de gestión de la seguridad de la información, para ello se desarrolló una metodología que permita establecer y ubicar a las instituciones en un rango de madurez. Esta metodología se la aplicó en tres instituciones del sector público y se pudo determinar que es factible medir la calidad de la gestión en la seguridad de la información y a través de los resultados de la aplicación de dicha metodología se pudieron determinar las fortalezas y oportunidades de mejora en las once áreas críticas analizadas en las instituciones públicas.

El Gobierno ecuatoriano implementó como eje principal para la administración pública el Plan Nacional para el Buen Vivir, el mismo que tiene por objetivo articular la política mediante la gestión e inversión pública; para ello en el sector público se puso en marcha el Plan Nacional de Gobierno Electrónico, con el objetivo de mejorar cualitativamente los servicios de información mediante el uso de las Tecnologías de la Información y Comunicaciones (TIC).

Para controlar la creciente implementación de las TIC en las instituciones públicas y su penetración, la Secretaria Nacional de Administración Pública solicitó la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) como parte del Programa Nacional de Gobierno por Resultados(GPR), basada en la norma NTE INEN ISO/IEC 27001:2011, publicada por el Instituto Ecuatoriano de Normalización. Este esquema lo están aplicando en las instituciones públicas dependientes de la administración central de forma obligatoria, con la finalidad de asegurar la integridad, confidencialidad y disponibilidad de la información administrada y procesada por el sector público.

Una vez descrita la situación actual del Gobierno Ecuatoriano y su posición respecto a la gestión de la seguridad de la información en las instituciones públicas, se realiza un análisis de la Norma NTE INEN –ISO/IEC 27001:2011 – Sistema de Gestión de la Seguridad de la Información, a partir de la cual se desarrolla la metodología de evaluación.

Para ello se desarrolla una metodología de evaluación, basada en la norma NTE INEN – ISO/IEC 27001:2011, con el objetivo de medir la calidad de la gestión en la seguridad de la información, proponiendo un modelo que incluye once variables y 81 indicadores que responden a un conjunto de interrogantes. En la presente metodología se establece una escala de madurez con el cual se medirá el estado situacional real de la institución con respecto a los controles propuestos por la norma NTE INEN-ISO/IEC 27001.

Por último se realiza una investigación de campo en donde se ejecuta la metodología planteada, mediante herramientas basadas en técnicas de entrevista y observación en tres instituciones del sector público, el objetivo es validar la metodología planteada y conocer el nivel de calidad de gestión de la seguridad de la información, de acuerdo a las once variables propuestas por la metodología, con el fin de conocer las fortalezas y oportunidades de mejora de cada institución evaluada.

Finalmente, se concluye que la seguridad de la información en las tres instituciones objeto de la presente investigación, dispone de un nivel de madurez tres (Definido), lo que significa que los procesos que gestionan la seguridad de la información se encuentra caracterizados, comprendidos y se describen en estándares, procedimientos, herramientas y métodos de forma proactiva. Cabe recalcar que existen aspectos importantes por implementar y mejorar para llegar a un nivel óptimo de madurez. Los resultados obtenidos fueron entregados a los responsables de las instituciones evaluadas para su correspondiente análisis.

INTRODUCCIÓN

En Ecuador se empezaron a registrar delitos informáticos en el 2009; éstos a la fecha viven su apogeo, siendo cada día más común los ataques a servicios financieros, robo de cuentas bancarias, clonación de tarjetas e identidades, daño de la imagen corporativa, robo, alteración y espionaje a la información de las organizaciones, trayendo como resultado pérdidas económicas y desconfianza entre los usuarios. Estadísticas obtenidas en la fiscalía del Ecuador muestran la evolución de los casos de delitos informáticos, habiendo registrado, en el periodo de 2009 al 2011, un total de 3100 denuncias, sin embargo solo en el 2012 ya se habían registrado 3500 denuncias con un aumento del 70%. Estudios realizados por la empresa "Inforc Ecuador", en el año 2012, muestran que en Ecuador cada día son vulneradas las seguridades de al menos 7 sitios web de organizaciones públicas y privadas.

Viviendo pleno auge, las organizaciones ecuatorianas se enfrentan cada vez más a riesgos e inseguridades procedentes de una gran variedad de orígenes que pueden dañar de forma importante sus sistemas de información y pueden poner en peligro la continuidad del negocio. En muchos de los casos, se encargan la elaboración de sus portales o sistemas de información a terceros, descuidando el manteamiento y actualización de las plataformas, siendo el tema de seguridad de la información algo no incluido en la lista de sus prioridades.

En la época actual las organizaciones afrontan amenazas y vulnerabilidades que pueden dañar la información, poniendo en peligro la continuidad del negocio. Ante estos acontecimientos es importante que las organizaciones evalúen sus riesgos y establezcan estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información.

La información, en conjunto con sus procedimientos y sistemas que hagan uso de ella, es uno de los activos más importantes de una organización. La confidencialidad, integridad y disponibilidad de información pueden llegar a ser esenciales para salvaguardar los niveles

de competitividad, rentabilidad e imagen corporativa necesarias para lograr los objetivos de la organización.
Asegurar un nivel de protección total es prácticamente imposible, incluso disponiendo de recursos ilimitados. El propósito de gestionar la seguridad de la información es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por parte de la organización, adaptándose a los cambios que se produzcan en el entorno.

Por tanto, el objetivo de esta investigación es determinar mediante un diagnóstico el nivel de calidad de gestión en la seguridad de la información en instituciones públicas, utilizando como herramienta la norma NTE INEN –ISO/IEC 27001:2011

Los objetivos específicos planteados para esta investigación son los siguientes:

- Determinar la situación actual en el sector público.

- Analizar los fundamentos teóricos, alcances y objetivos de la Norma NTE INEN –ISO/IEC 27001:2011.

- Desarrollar una metodología de evaluación para las instituciones del sector público, que permita determinar el grado con el cual es gestionado la seguridad de la información con respecto a la norma NTE INEN –ISO/IEC 27001:2011.

- Ejecutar la metodología planteada en instituciones del sector público, con el fin de obtener el nivel de calidad de gestión en la seguridad de la información individual, junto a un detalle de las fortalezas y oportunidades de mejora de cada institución.

Durante la presente investigación se analizarán temas enfocados en la calidad de la seguridad de la información, utilizando como herramienta fundamental la norma ISO 27001 que proporciona los lineamientos necesarios para prever que la información sensible de la organización responda a tres parámetros básicos: confidencialidad, integridad y disponibilidad. Por otra parte, se estudiarán los problemas comunes que sufren las instituciones al momento de gestionar su información. También se desarrollará una

metodología de evaluación, con el fin de determinar su nivel de calidad en gestión de la seguridad de la información.

El trabajo de investigación se llevará a cabo en tres instituciones públicas de la ciudad de Quito D.M., No será requisito para la selección de las organizaciones que tengan implementada, o en proceso, la Norma ISO/IEC 27001.

1. ANÁLISIS DEL ENTORNO

El propósito del presente capítulo es exponer cómo está constituida la estructura del Estado Ecuatoriano para gestionar las políticas públicas de las tecnologías de la información y comunicaciones (TIC) en el ámbito público, privado y de la sociedad en general; esta información es fundamental, ya que sirve para comprender la evolución de las TIC en el Ecuador, así como los avances relacionados a la seguridad de las TIC.

Es necesario precisar que el órgano encargado de gestionar las políticas de gestión de las TIC es el Ministerio de Telecomunicaciones conjuntamente con la Secretaria Nacional de la Administración Pública.

1.1 Tecnologías de la Información y Comunicaciones (TIC)

De acuerdo al Ministerio de Telecomunicaciones del Ecuador, las Tecnologías de la Información y Comunicaciones (TIC) se refiere a la unificación de las comunicaciones como el conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información.

Para efectos de esta investigación, se entiende por TIC todas las actividades relacionadas a hardware, software, internet, telecomunicaciones y contenidos digitales.

Las TIC actúan como un catalizador para el crecimiento económico de los países y se asocian con algunos factores, siendo uno de los más importantes: la infraestructura de telecomunicaciones, como caso específico el acceso a la banda ancha, que permite un empoderamiento progresivo de las TIC a nivel ciudadano y empresarial, contribuyendo al desarrollo de la economía. Dicho empoderamiento fomenta el desarrollo de las industrias, generado nuevas plazas de empleos con el objetivo de crear nuevos productos y servicios tecnológicos, incrementando así su contribución a la economía del país. (Ministerio De Telecomunicaciones, 2014)

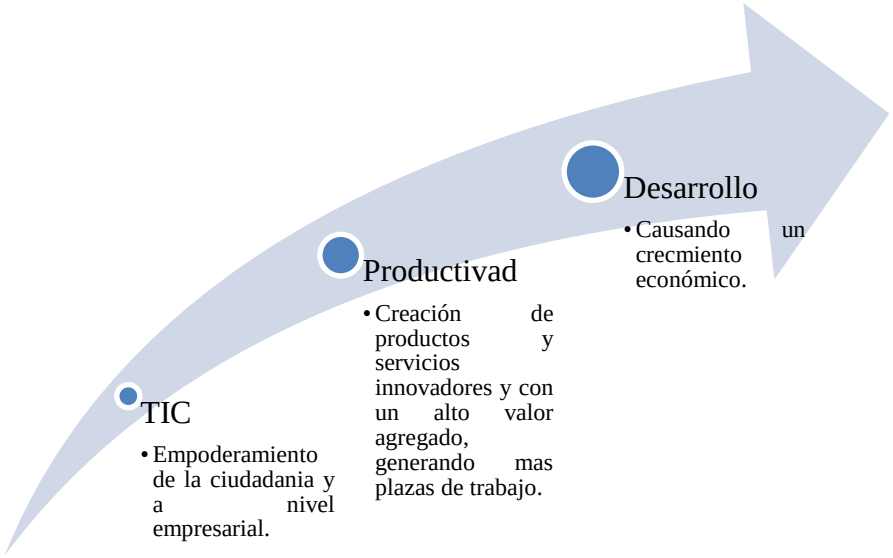

Figura 1: TIC Catalizador para el crecimiento.

1.2 Estado Ecuatoriano

De acuerdo a la Constitución de la República del Ecuador presentada en el año 2007, se define al Estado como constitucional de derechos y justicia, social, democrático, soberano, independiente, unitario, intercultural, plurinacional y laico. Se organiza en forma de república y se gobierna de manera descentralizada. La soberanía radica en el pueblo, cuya voluntad es el fundamento de la autoridad, y se ejerce a través de los órganos del poder público y de las formas de participación directa previstas en la Constitución. Los recursos naturales no renovables del territorio del Estado pertenecen a su patrimonio inalienable, irrenunciable e imprescriptible. (Asamblea Constituyente, 2007)

El sector público es el conjunto de organismos administrativos, mediante los cuales el Estado hace cumplir las políticas o decisiones expresadas en las Leyes existentes en el país.

Según el art. 118 de la Constitución de la República del Ecuador se considera organismo del Sector Público a: Organismos y Dependencias de las Funciones Legislativa, Ejecutiva y Judicial, Organismos Electorales, Organismos de Control y Regulación, Entidades que Integran el régimen seccional autónomo, Organismos creados por constitución y personas jurídicas creadas por el acto legislativo. (Asamblea Constituyente, 2007)

1.2.1 Estructura Orgánica del Estado Ecuatoriano

El sector público está constituido por diversas entidades y organizaciones, de acuerdo a la Constitución de la República del Ecuador, su estructura orgánica es la siguiente:

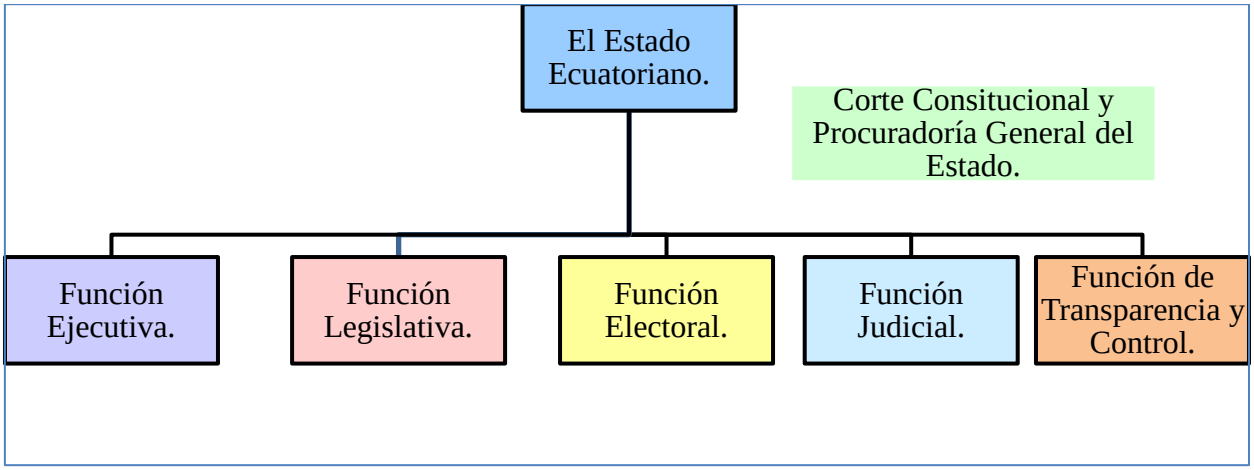

Figura 2: Estructura Organizacional del Estado Ecuatoriano.

A continuación se realiza una descripción de cada una de las funciones y su incidencia en la gestión de las TIC:

- **Función Ejecutiva:** Se considera como la administradora y ejecutora de la voluntad popular, a la cual representa y de la que debe ser su más firme garante y de acuerdo a la constitución ecuatoriana se asigna al Presidente de la República. El poder ejecutivo crea y ejecuta políticas generales de acuerdo a las leyes. (Asamblea Constituyente, 2007)

La Función Ejecutiva como organismo rector del Estado Ecuatoriano, es el responsable de crear y ejecutar las políticas públicas para la gestión de las tecnologías de la información y comunicaciones, para ello establece estrategias a largo plazo (2009-2017), que mediante la iniciativa presidencial del Plan Nacional del Buen Vivir en conjunto con la iniciativa presidencial del Cambio de la Matriz Productiva, se establecen los objetivos, metas y estrategias para brindar una mejora

en la gestión y calidad en la prestación de los servicios de las TIC, tanto a la ciudadanía como a clientes internos del estado.

- **Función Legislativa:** Es ejercida por la Asamblea Nacional, que tiene su sede en la ciudad de Quito, D.M., creada por mandato constitucional; su objetivo es aprobar y normar leyes que permitan un adecuado funcionamiento del Estado Ecuatoriano, así como fiscalizarlo. (Asamblea Constituyente, 2007)

  Siendo una de las atribulaciones principales de la función legislativa, el aprobar y normar leyes, en junio de 2013, la Asamblea Nacional expide una importante ley que influye directamente sobre el acceso a las TIC, esta es llamada Ley Orgánica de Comunicación, la cual tiene por objetivo garantizar el ejercicio y la plena vigencia de los derechos a la comunicación, así como aplicar de forma efectiva la libertad de expresión, de información, democratización de la comunicación, libre acceso a la información pública y el acceso universal a las tecnologías de información y comunicación (TIC). En el Art. 35 de la mencionada ley dice: "Todas las personas tienen derecho a acceder, capacitarse y usar las tecnologías de información y comunicación para potenciar el disfrute de sus derechos y oportunidades de desarrollo." (Asamblea Nacional, 2013)

  Como parte de la evolución de las TIC dentro de la estructura del Estado Ecuatoriano, la Asamblea Nacional implementó el Sistema de Curul Electrónico, el mismo que entró en funcionamiento en febrero de 2012. El objetivo de dicho sistema es ejecutar el Plan Cero Papeles, el mismo que servirá para mejorar la eficiencia administrativa.

  A través de esta herramienta digital compuesta de un computador y un programa específico, se gestionará las actividades de los/as asambleístas, la Secretaría, Presidencia, Vicepresidencias y demás actores del Pleno, siendo las siguientes sus funciones principales: administración de sesiones, convocatorias, conocer sesiones convocadas, suspendidas, clausuradas; registros de cuórum, votación, distribución digital de la documentación, registro para el debate, publicación de votaciones a la

ciudadanía y una bitácora de la sesión, pedido de palabra, de punto de información, punto de orden y solicitud de réplica. (Asamblea Nacional, 2012)

- **Función Electoral:** Tiene como objetivo garantizar los derechos políticos y de participación representativa, la organización y control de procesos electorales y el registro de partidos y movimientos políticos. (Asamblea Constituyente, 2007)

  Continuando la misma línea de evolución de las TIC, la función electoral implementa como parte del control de los procesos electorales, el sistema de votación electrónica, durante las elecciones de febrero de 2014, en las provincias Azuay, Santo Domingo de los Tsáchilas y en la zona La Morita, de Pichincha. Dicho sistema ofrecerá a la ciudadanía una opción confiable y válida para que los electores ejerzan el derecho al voto. El procedimiento de voto electrónico se cumple en cuatro pasos: acta de inicialización en cero, votación, escrutinio y transmisión de resultados. (Tribunal Contencioso Electoral del Ecuador, 2013)

- **Función Judicial:** Tiene como objetivo administrar la Justicia con base a la Ley Orgánica de la Función Judicial y la Constitución de la República. La Constitución de la República divide a la administración de Justicia en dos secciones: la Justicia ordinaria representada por el Consejo Nacional de la Judicatura, y la Justicia Indígena, siendo una administración de Justicia en base a un contexto cultural y ancestral. (Asamblea Constituyente, 2007)

  Los avances tecnológicos en la administración y modernización de la justicia a nivel nacional, empezó en el año 2012 con la implementación del sistema integral de administración de justicia "Justicia 2.0", para combatir la impunidad y fortalecer la seguridad ciudadana. "Justicia 2.0" es una solución tecnológica integrada que da soporte a los principios de oralidad, transparencia, publicidad y eficiencia demandados por los procesos de transformación de la Administración de Justicia en Ecuador. (Consejo de la Judicatura, 2012)

- **Función de Transparencia y Control:** Tiene como objetivo controlar al accionar público, promover la participación ciudadana y proteger los derechos

constitucionales, en todos sus niveles; transparencia, eficiencia, equidad y lucha contra la corrupción, dicha función se encuentra integrada por nueve instituciones, siendo una de ellas la Contraloría General del Estado, que es la encargada de velar por la transparencia en la gestión pública y otra institución muy importante es la Superintendencia de Telecomunicaciones, que se encarga del control del acceso a las tecnologías de la información y comunicaciones. (Asamblea Constituyente, 2007)

Como aporte al desarrollo de las TIC la Dirección de Auditoría de Tecnología de la Información y Comunicación, creada en el año 2013, concentró sus esfuerzos en controlar los recursos de tecnologías de la información y comunicación, que poseen las distintas entidades del sector público, para ello efectuó importantes auditorías a instituciones públicas, como a la Agencia Nacional de Tránsito, en donde se realizó un examen especial para asegurar que el proceso de gestión de licencias de conducir garantice la integridad, confidencialidad y disponibilidad de la información. Adicionalmente, llevo a cabo una auditoría al Gobierno Autónomo Descentralizado Municipal del Cantón Riobamba, en donde se expusieron importantes recomendaciones para evitar fraudes electrónicos a través de los sistemas de información que maneja el municipio. (Contraloria General del Estado, 2013)

- **Corte Constitucional:** Tiene como objetivo controlar la constitucionalidad del Estado Ecuatoriano, así como la interpretación de la constitución. Creada por mandato constitucional que goza de autonomía administrativa y financiera. (Asamblea Constituyente, 2007)

  La corte Constitucional siendo el organismo que resuelve todas las controversias jurídicas referentes a la vulneración de los derechos constitucionales, durante el periodo de noviembre de 2012 a septiembre de 2013 recibió 7190 casos, durante este periodo la Dirección de Tecnología de dicha función, adquirió el software de Gestión de Acciones Constitucionales, siendo esta la plataforma central para registrar todos los casos referentes a la vulneración de los derechos constitucionales. En dicho sistema los usuarios internos y externos pueden

encontrar información certificada desde el 20 de octubre de 2008 hasta la presente, sobre los casos resueltos o en proceso de la corte Constitucional.
(Corte Constitucional del Ecuador, 2013)

- **Procuraduría General del Estado:** Tiene como objetivo representar judicialmente al Estado, mediante el asesoramiento legal y la absolución de consultas a todas sus instituciones, controla los actos y contratos que suscriban los organismos del sector público, y concilia o media los conflictos generados mediante los Tribunales de Mediación. (Asamblea Constituyente, 2007)

Durante el periodo de gestión del año 2013, se desarrolló e implementó tecnología informática para la digitalización documental y la automatización de procesos, siendo esta una herramienta informática de nivel gerencial, que permite acceder al 100% de los expedientes judiciales a nivel nacional, permitiendo abrir en tiempo real los textos digitalizados de todos los escritos y providencias de un proceso requerido, además de presentar datos estadísticos sobre resultados. El resultado de la implantación de dicha herramienta se ve reflejado en una reducción en el número de consultas formuladas a la Procuraduría General del Estado, ya que quienes se conectan al sistema de consultas pueden acceder en tiempo real a los pronunciamientos que emite esta Institución. (Procuradoria General del Estado, 2013)

1.2.2 Iniciativa Presidencial: Plan Nacional para el Buen Vivir

El Plan Nacional para el Buen Vivir se constituye como un instrumento guía para el Gobierno Nacional, con el fin de articular su política pública mediante la gestión y la inversión pública, cuya estrategia clave es el cambio de la matriz productiva. Está conformado mediante 12 objetivos, 83 metas, 111 políticas y 1.089 lineamientos estratégicos. Fue elaborado por la SENPLADES, conforme el Decreto Ejecutivo 1577 de febrero de 2009 y presentado por el Presidente de la República Economista Rafael Correa Delgado.

1.2.2.1 Objetivos

Los objetivos nacionales para el Buen Vivir, son doce, los cuales cuentan con políticas, estrategias y metas, estos se encuentran organizados en tres ejes:

1) Cambio en las relaciones de poder para la construcción del poder popular.
2) Derechos, libertades y capacidades para el Buen Vivir.
3) Transformación económica – productiva, a partir del cambio de la matriz productiva.

A continuación se analizará la evolución de algunas de las metas del objetivo 11, el cual trata la política pública para asegurar la soberanía y eficiencia de los sectores estratégicos para la transformación industrial y tecnológica, que en conjunto con el objetivo 10 impulsan el cambio de la matriz productiva, ayudando a que la penetración de las TIC en el territorio ecuatoriano sea viable.

1.2.2.2 Metas para asegurar la transformación industrial y tecnológica

El Plan Nacional para el Buen Vivir en su versión 2013-2017 establece:

> La información y el conocimiento tienen un rol primordial en la construcción de una nueva sociedad, esto ha generado un nuevo impulso del gobierno hacia los territorios digitales. La mayoría de las instituciones públicas y privadas a nivel nacional, no proporcionan servicios ni tramites que permitan acceder a servicios de calidad por medios electrónicos. En el mejor de los casos, se ofertan aplicaciones informativas, cuando el verdadero requerimiento es transaccional. Esta problemática es más grave cuanto más lejos se encuentre la población de las oficinas centrales, en las que se realizan los trámites administrativos y/o la prestación física de estos servicios, lo que acentúa la exclusión social y castiga a la población más alejada de los centros urbanos. (Senplades, 2013)

Para ello a continuación se muestra algunas de las metas planteadas, con sus respectivos indicadores, con el objetivo de lograr la inserción de las tecnologías de la información y comunicaciones.

- **Alcanzar un índice de digitalización de 41,7 para el 2017**

Mide el nivel de adopción y uso de las tecnologías de información y comunicación (TICs) del país, y sus múltiples impactos en el ámbito socio económico (crecimiento económico como: creación de empleo, reducción de la pobreza, innovación entre otros).

El índice mide cuatro estados de desarrollo en términos de la digitalización (limitado, emergente, transicional y avanzado).

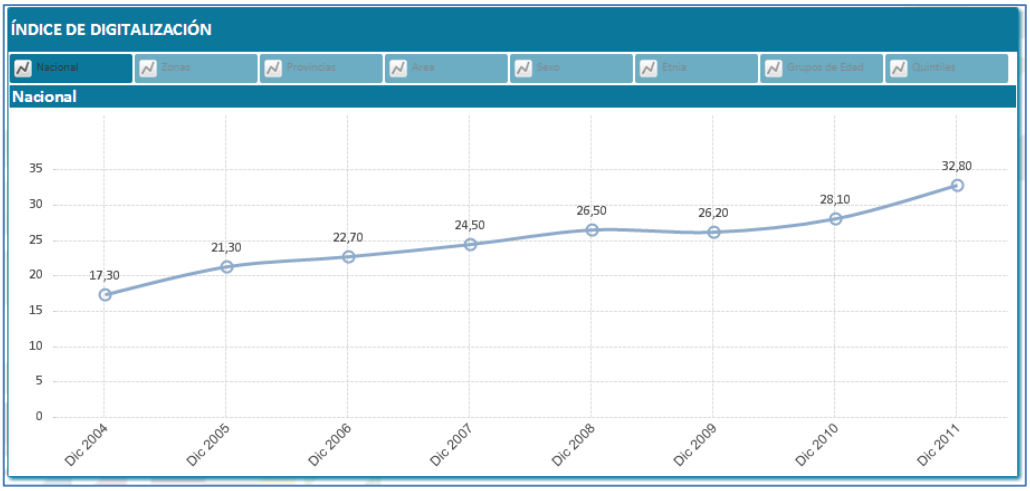

Figura 3: Índice de digitalización.
Fuente: Secretaria Nacional de Planificación y Desarrollo, Senplades 2014.

Tabla 1:

Estados de digitalización

Estado	Rango de valoración
Limitado	0-20
Emergente	21-35
Transaccional	36-50
Avanzado	51-100

Fuente: Secretaria Nacional de Planificación y Desarrollo, Senplades 2014.

De acuerdo a la información presentada se tiene que hasta diciembre del 2011, el índice de digitalización nacional fue de 32,80, lo que indica que el estado es emergente.

- **Disminuir el analfabetismo digital al 17,9%**

Se define como el porcentaje de la población de 15 a 49 años de edad que no utiliza internet, computador o teléfono celular en los últimos doce meses; respecto a la población del mismo grupo etario.

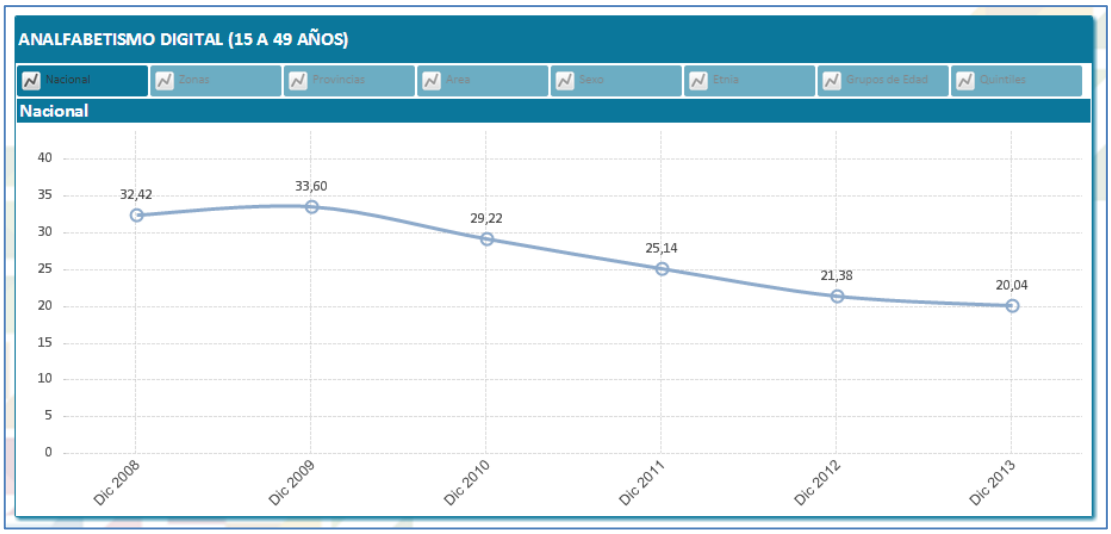

Figura 4: Analfabetismo digital.
Fuente: Secretaria Nacional de Planificación y Desarrollo, Senplades 2014.

Como se puede apreciar en la gráfica, para diciembre de 2013, el porcentaje de la población a nivel nacional que no utilizó internet, computador o teléfono celular en los últimos doce meses es del 20,04%.

- **Aumentar el porcentaje de personas que usan tics al 50%**

Se define como el número de personas mayores de 5 años de edad que utilizan tecnologías de la información y comunicación (TIC´S), expresado como porcentaje del total de personas del mismo rango etario.

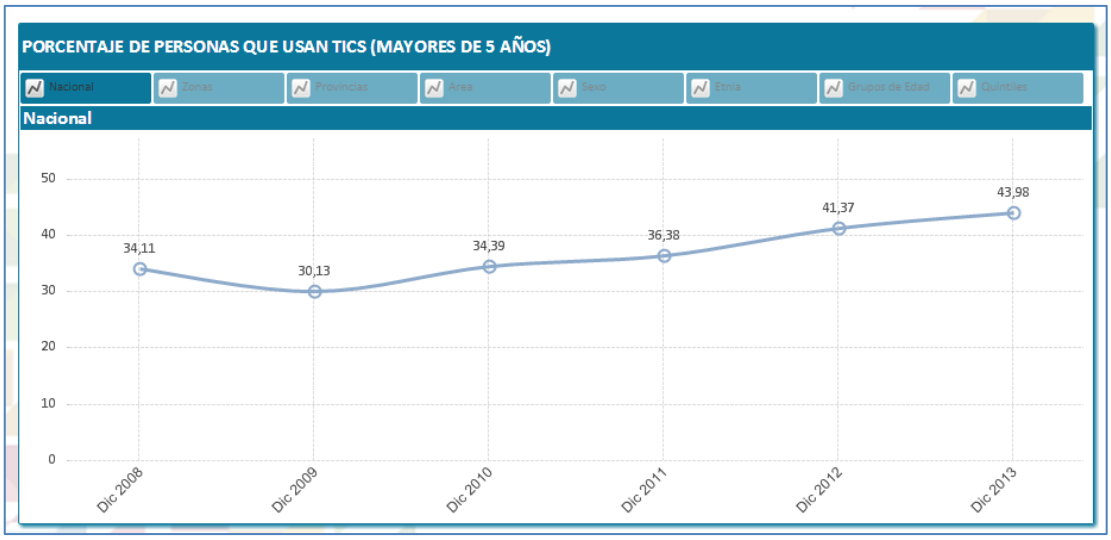

Figura 5: Porcentaje de personas que usan TIC
Fuente: Secretaria Nacional de Planificación y Desarrollo, Senplades 2014.

Para diciembre de 2013, se tiene que el 43,98% de la población a nivel nacional mayor de 5 años, utilizó las tecnologías de la información y comunicación (TIC).

1.2.2.3 Transformación de la Matriz Productiva

La forma cómo se organiza la sociedad para producir determinados bienes y servicios no se limita únicamente a los procesos estrictamente técnicos o económicos, sino que también tiene que ver con todo el conjunto de interacciones entre los distintos actores sociales, que utilizan los recursos que tienen a su disposición para llevar adelante las actividades productivas. A ese conjunto, que incluye los productos, los procesos productivos y las relaciones sociales resultantes de estos procesos, se la denomina matriz productiva. La transformación de la matriz productiva, significa dar paso a un cambio en el patrón de especialización primario exportador a uno que priorice la producción diversificada, ecoeficiente y con un alto valor agregado. (Senplades, 2012)

Los ejes para la transformación de la matriz productiva son:

1. Diversificación productiva basada en el desarrollo de industrias estratégicas como son: la refinería, petroquímica, metalurgia y siderúrgica, así como también estableciendo nuevas actividades en los sectores productivos de: maricultura, biocombustibles, productos forestales de madera, logrando así ampliar la oferta de productos ecuatorianos eliminando la dependencia de producto del exterior.

2. Agregar valor a la producción de todos los sectores, mediante la inclusión de tecnología y la transferencia de conocimiento a los actuales y futuros procesos productivos.

3. Sustitución selectiva de importaciones en bienes y servicios que se produzcan actualmente, y que permitan la sustitución en el corto plazo en industrias como: farmacéutica, tecnología y metalmecánica.

4. Fomento a las exportaciones de productos nuevos, provenientes de actores nuevos como la economía popular y solidaria.

A continuación se muestra una comparación entre el enfoque tradicional y el enfoque moderno de la matriz productiva, orientada desde el punto de vista del desarrollo de software, siendo esta una buena oportunidad para la industria de las TIC.

- **Enfoque tradicional de la Matriz Productiva**

En un enfoque tradicional las compañías extranjeras hacen uso de la mano de obra ecuatoriana para generar productos al extranjero, estos posteriormente son comercializados de vuelta en nuestro país como productos terminados.

Figura 6 : Enfoque tradicional de la Matriz Productiva.

- **Enfoque moderno de la Matriz Productiva**

El enfoque moderno en el cambio de la matriz productiva, se refiere a la elaboración de productos terminados de exportación y de consumo interno, contribuyendo a la generación de plazas de trabajo, así como la mejora de la producción.

Figura 7: Enfoque moderno de la Matriz Productiva.

1.2.3 Plan Nacional de Gobierno Electrónico

De acuerdo a la Organización Mundial de las Naciones Unidas, el Gobierno Electrónico se refiere al uso de las Tecnologías de la Información y Comunicaciones (TIC), por parte de las instituciones de Gobierno, para mejorar cualitativamente los servicios de información que se ofrecen a las ciudadanas y ciudadanos, aumentar la eficiencia y eficacia de la gestión pública, incrementar sustantivamente la transparencia del sector público y la participación ciudadana.

1.2.3.1Objetivos que persigue el Gobierno Electrónico

- Implementar y utilizar las TIC manteniendo pautas, normas, experiencias y buenas prácticas.
- Plantear una nueva forma de gobernar, a través de la toma de decisiones basado en información en línea.
- Gestionar de forma coherente personas, tecnologías, normas, servicios, sistemas y procesos.

1.2.3.2 Actores del Gobierno Electrónico

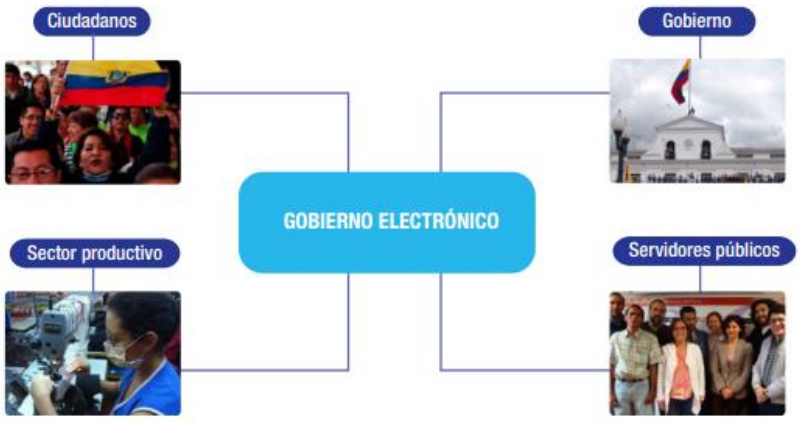

Figura 8: Actores del Gobierno Electrónico.
Fuente: Secretaria Nacional de la Administración Pública, 2014.

- ✓ Los ciudadanos son la razón de ser de la gestión del Gobierno y quienes, de manera individual o colectiva, se benefician del Gobierno Electrónico por ser este un medio de participación e interacción, que permite el adecuado ejercicio de sus derechos y obligaciones conforme al marco Constitucional y normativo vigente. (Secretaria Nacional de la Administración Pública, 2014)

- ✓ El Gobierno entendido como el responsable de administrar el aparato estatal de conformidad con la Constitución y el cuerpo legal vigente. Se beneficiará del Gobierno Electrónico como una plataforma, que fomenta el desarrollo de nuevas formas de relación entre los actores de la sociedad. Adicionalmente este actor hace referencia a otros Gobiernos, con los cuales puede emprenderse estrategias comunes para consolidar el Gobierno Electrónico. (Secretaria Nacional de la Administración Pública, 2014)

- ✓ El Sector Productivo, es el actor que con sus esfuerzos individuales o colectivos, organiza y desarrolla procesos de producción, intercambio, comercialización, financiamiento, y consumo de bienes y servicios; para satisfacer necesidades y generar ingresos. (Secretaria Nacional de la Administración Pública, 2014)

- ✓ Los servidores públicos son el talento humano que presta sus servicios dentro de las instituciones del sector público. El beneficio que el Gobierno Electrónico les brinda, es tener acceso a herramientas que facilitan su trabajo y les permite ofrecer un servicio de mayor calidad. (Secretaria Nacional de la Administración Pública, 2014)

1.2.3.3 Etapas de evolución del Gobierno Electrónico

La Organización de las Naciones Unidas (ONU), ha definido las etapas de evolución en la gestión del Gobierno Electrónico, de acuerdo a la siguiente estructura piramidal:

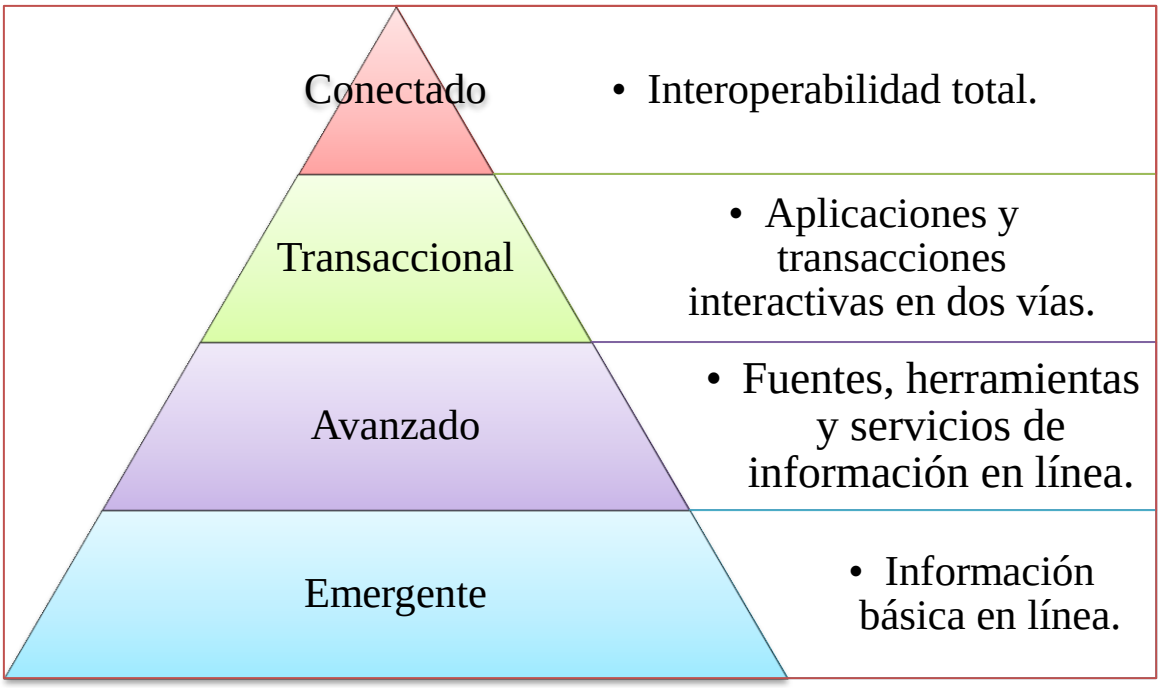

Figura 9: Evolución del Gobierno Electrónico.
Fuente: Naciones Unidas, 2012.

- ✓ **Etapa Emergente:** Durante esta etapa, los gobiernos solo disponen de información básica publicada en el internet, mediante el uso de páginas web que disponen información sobre política pública, gobernanza, legislación, reglamentación, documentación pertinente de trámites y servicios gubernamentales; donde los ciudadanos puedan obtener información en tiempo real.

- ✓ **Etapa Avanzada:** Durante esta etapa, se implementan mejoras a los servicios de información, donde los sitios web gubernamentales, permiten una comunicación unidireccional o en algunos casos bidireccionales entre el gobierno y el ciudadano, a través de aplicaciones multilenguaje permitiendo el envío y recepción de formularios en línea, que incluyen funciones multimedia de audio y vídeo.

- ✓ **Etapa Transaccional:** Durante esta etapa, los sitios web gubernamentales incluyen servicios transaccionales con una comunicación bidireccional entre el ciudadano y el gobierno, los ejemplos que se pueden citar de servicios ofrecidos son: votación electrónica, descarga y carga de formularios, presentación de declaraciones de impuestos en línea, trámites en línea para solicitar certificados, licencias y permisos otorgados por las instituciones públicas.

- ✓ **Etapa Conectada:** Durante la etapa final, la implementación de Gobierno Electrónico, conecta los departamentos y ministerios de manera uniforme, permitiendo que los datos y el conocimiento se transfieran entre los organismos gubernamentales, y las demás instituciones de una forma integrada.

1.2.4 Nivel de desarrollo de las TIC en el Ecuador

Es importante conocer los niveles de acceso de las TIC tanto en hogares, individuos, empresas y también en las instituciones públicas para conocer el grado de desarrollo, en cuanto al uso y presencia de las TIC en los distintos sectores.

1.2.4.1 Incidencia de las TIC a nivel nacional

Como análisis inicial es importante caracterizar la situación actual del desarrollo respecto a las Tecnologías de la Información y Comunicaciones en nuestro país, para ello es necesario conocer el nivel de penetración y acceso, para ello, se muestra a continuación los principales indicadores de penetración y cobertura de las TIC a nivel nacional, que de acuerdo a datos obtenidos en el Ministerio de Telecomunicaciones, se presenta la situación de nuestro país en términos económicos y sociales con respecto al resto de regiones del Mundo, los comparativos se realizan entre los años 2005 y 2010.

Tabla 2:

Caracterización económica y social de las TIC

	Mundo		Europa y Asia Central		Latinoamérica y Caribe		Ecuador		Promedio comparativo	
Indicador	**2005**	**2010**	**2005**	**2010**	**2005**	**2010**	**2005**	**2010**	**Ecuador**	**Mundo**
Población (Millones de personas)	6504	6895	3990	4080	550	589	13	14	**8%**	**5%**
Crecimiento por producto interno bruto PIB (% media anual)	2.8	1.9	6.1	3.2	2.6	3.9	5.6	3.6	**-36%**	**-22%**
Crecimiento PNB per cápita ($ millones)	7099	9071	3711	7734	4427	8574	2620	3850	**47%**	**67%**
Tasa de alfabetización de adultos (% a partir de los 15 años)	82	84	97	98	90	91	84	84	**0%**	**1%**
Matriculación en enseñanza primaria, secundaria y superior (%)	67	73	79	80	81	83	79	82	**4%**	**4%**

Fuente: Ministerio de Telecomunicaciones del Ecuador, 2014.

Como se puede observar en los datos presentados, Ecuador mantiene una similitud respecto a los promedios obtenidos de los indicadores económicos y sociales, sin embargo existe una diferencia mayor en los indicadores de crecimiento PIB y PNB. Así también se obtuvieron indicadores que ayudan a comprender el comportamiento del sector de las TIC en el Ecuador en relación de al resto de regiones, los comparativos se realizan entre los años 2005 y 2010.

Tabla 3:

Comportamiento de las TIC

	Mundo		Europa y Asia Central		Latinoamérica y Caribe		Ecuador		Promedio comparativo	
Indicador	**2005**	**2010**	**2005**	**2010**	**2005**	**2010**	**2005**	**2010**	**Ecuador**	**Mundo**
Suscriptores a telefonía fija por cada 100 habitantes	19.4	17.2	24	25.1	17.6	18.5	12.5	14.4	**15%**	**0%**
Suscriptores a telefonía móvil por cada 100 habitantes	34	78.2	61.6	132.5	43.1	107.2	46.5	102.2	**120%**	**129%**
Suscriptores a banda ancha fija por cada 100 habitantes	3.44	7.75	1.1	10.42	1.5	7.66	0.2	1.37	**585%**	**328%**
Porcentaje de Hogares con computadores	27.3	36.2	27.8	44.9	16.4	37.9	17.9	27	**51%**	**66%**
Porcentaje de Hogares con acceso a Internet	18.8	30.3	19.9	37	9.9	30.3	2.5	11.5	**360%**	**101%**

Fuente: Ministerio de Telecomunicaciones del Ecuador, 2014.

Respecto al nivel de penetración de las TIC en nuestro país, se puede apreciar que tenemos una clara evolución con respecto al acceso al internet, telefonía fija y móvil con respecto al resto de regiones en el mundo.

1.2.4.2 Incidencia de las TIC a nivel empresarial

Es importante conocer la penetración del uso de las TIC en las MIPYMES; para ello se presenta los resultados de la medición de indicadores a través de una investigación de mercado realizada por el Ministerio de Telecomunicaciones en el 2012, donde se aplicó a 7.750 establecimientos segmentados por tipo de actividad (comercio, servicio, manufactura e información/comunicación) y tipo de establecimiento (microempresa, pequeña empresa y mediana empresa), en la ciudades de: Ibarra, Santo Domingo, Quito, Ambato, Riobamba, Manta-Portoviejo, Guayaquil, Machala, Cuenca y Loja.

Tabla 4:

Penetración de las TIC a nivel empresarial

	Micro Empresa	Pequeña Empresa	Mediana Empresa	Media Total
Porcentaje de empresas que utilizan computadoras	42.9%	71.6%	90.2%	**68.2%**
Porcentaje de empresas que utilizan internet	72.4%	81.9%	92.5%	**82.3%**
Porcentaje de empresas con presencia en internet	9.2%	22.8%	50.2%	**27.4%**
Porcentaje de empresas que utilizan el internet para: Servicios bancarios/ Banca Electrónica	51.1%	68.5%	78.2%	**65.9%**

Fuente: Ministerio de Telecomunicaciones del Ecuador, 2014.

Tabla 4:

(Continuación)

	Micro Empresa	Pequeña Empresa	Mediana Empresa	Media Total
Porcentaje de empresas que utilizan el internet para: Capacitación de personal	13.9%	17.1%	24.2%	**18.4%**
Porcentaje de empresas que utilizan el internet para: Enviar o recibir correos	85.9%	92.1%	94.3%	**90.8%**
Porcentaje de empresas que utilizan el internet para: Interactuar con sitios gubernamentales	41.8%	56.3%	66.7%	**54.9%**
Porcentaje de empresas que utilizan el internet para: Obtener información de bienes y servicios	74.3%	82.7%	84.7%	**80.6%**
Porcentaje de empresas que utilizan el internet para: Proveer servicios a clientes	53.1%	43.8%	35.2%	**44.0%**

Fuente: Ministerio de Telecomunicaciones del Ecuador, 2014.

De acuerdo a la información presentada se puede concluir que el nivel de acceso a las TIC en el sector de las MIPYMES, se encuentra alto para el uso interno de ellas, sin embargo al momento de tener presencia en internet, interacción gubernamental,

capacitación u ofrecer servicios en línea, los indicadores muestran un bajo nivel de penetración.

1.2.4.3 Incidencia de las TIC en las instituciones públicas

En la investigación realizada en el año 2013 por la Subsecretaría de Fomento a la Sociedad de la Información y Gobierno en Línea del Ministerio de Telecomunicaciones, mediante una encuesta a las instituciones públicas del país, se diagnosticó el nivel de penetración de las TIC.

A continuación se presentan los resultados de la investigación realizada en el año 2013, en donde se miden seis parámetros, que sirvieron para determinar la penetración de las TIC en las instituciones públicas.

- ✓ **Niveles de cultura digital:** Representa las distintas formas y medios de información, basados en tendencias tecnológicas, las cuales son adoptadas por el personal de las instituciones de acuerdo a la evolución de las TIC.

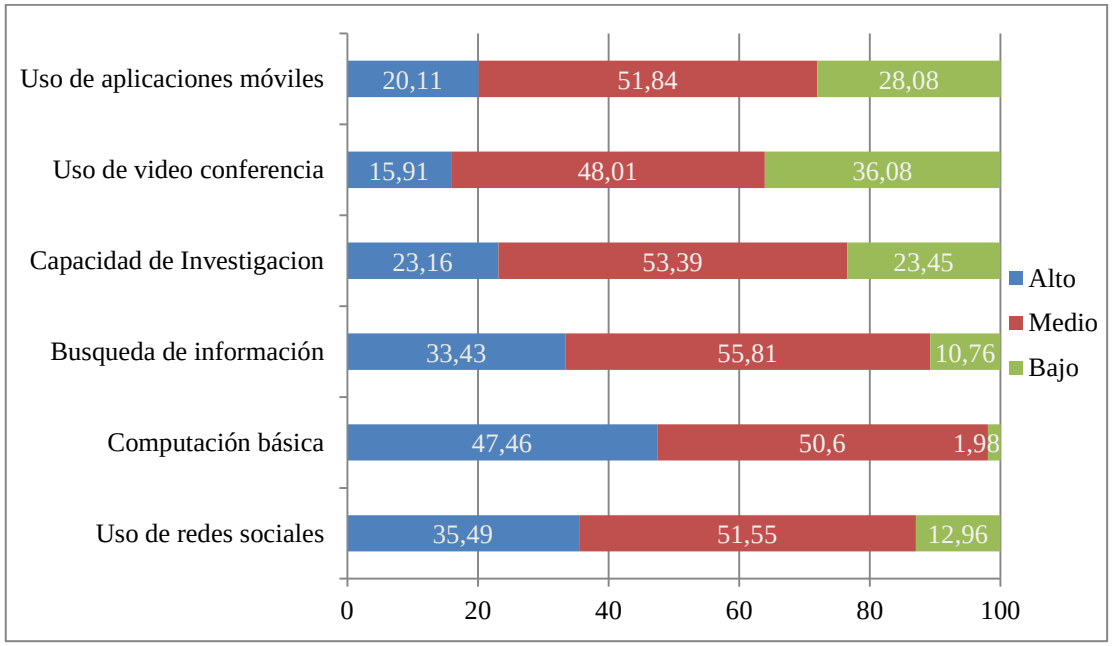

Figura 10: Nivel de cultura digital.
Fuente: Ministerio de Telecomunicaciones del Ecuador, 2014.

Como resultado de esta evaluación se determina que las destrezas para manejar las TIC son catalogadas como *media*, destacándose el uso del internet para la investigación y búsqueda de información, además para el uso rutinario de las actividades diarias, tanto en computadores como en dispositivos móviles.

- ✓ **Capacitación en el uso diario de las tecnologías de la información y comunicación:** Representa los conocimientos y habilidades sobre las tecnologías de la información y el uso de herramientas ofimáticas básicas.

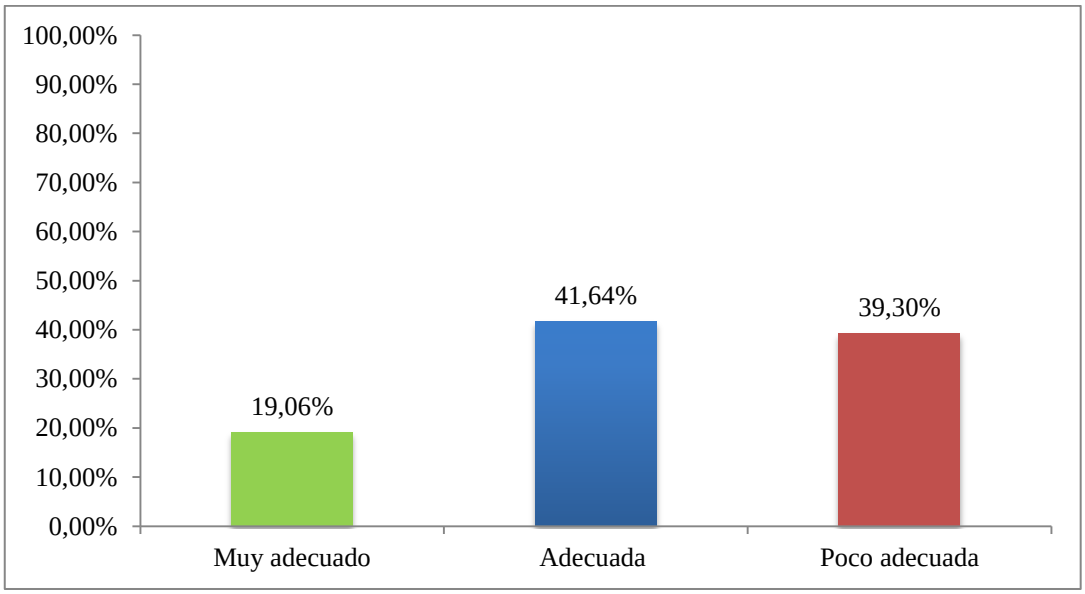

Figura 11: Capacitación en el uso diario de las Tecnologías de la Información y Comunicación.
Fuente: Ministerio de Telecomunicaciones del Ecuador, 2014.

La capacitación para el uso diario de herramientas de tecnologías de la información y comunicación dentro de los funcionarios públicos, puede ser catalogada como *adecuada*, sin embargo, no se debe descuidar el porcentaje alto de funcionarios que contestaron como *poco adecuada*.

- ✓ **Las instituciones públicas proveen formularios electrónicos para interactuar con la ciudadanía:** Representa la interacción entre la ciudadanía y las instituciones, mediante el uso de tecnologías de la información.

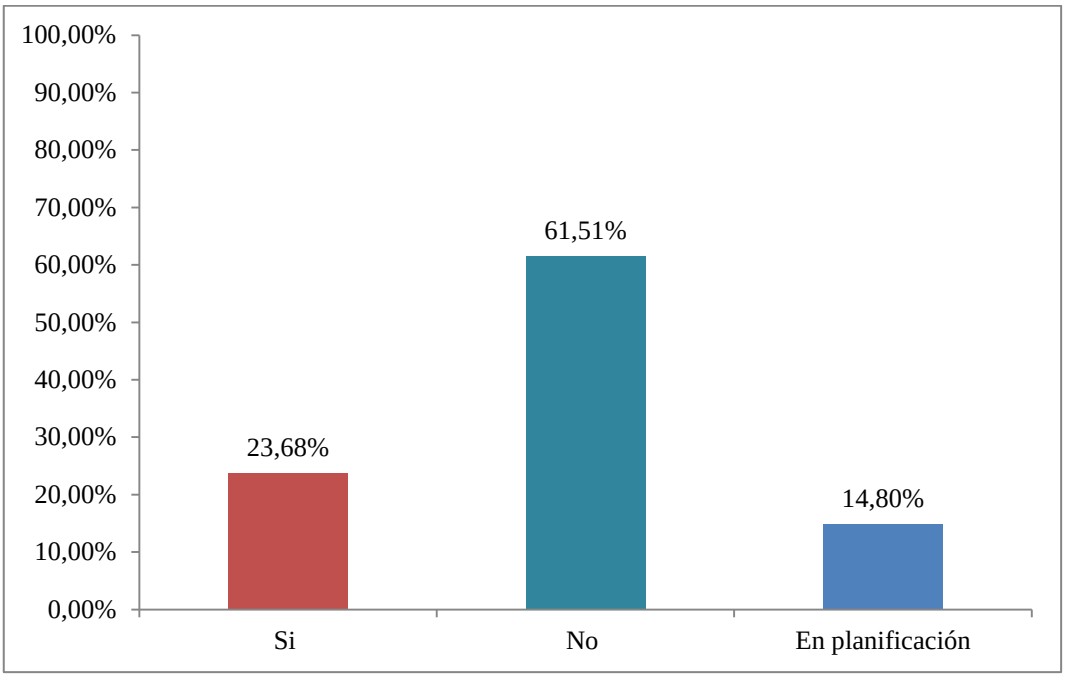

Figura 12: Uso de formularios electrónicos para la interacción con la ciudadanía.
Fuente: Ministerio de Telecomunicaciones del Ecuador, 2014.

Es muy importante analizar el nivel de interacción entre la ciudadanía y la función pública, siendo esta interacción uno de los pilares fundamentales del gobierno electrónico, donde se articula la comunicación a la ciudadanía en temas concernientes a leyes, políticas, planes, etc., además permite a los ciudadanos opinar sobre temas específicos. Las encuestas nos revela que aproximadamente el 76% de la instituciones públicas *n*o ofrecen medios electrónicos de comunicación con la ciudadanía.

- ✓ **Implementación de proyectos en tecnologías de la información y comunicación para la mejora de la productividad:** Representa el grado de penetración de las TIC en las instituciones, con la finalidad de mejorar la productividad.

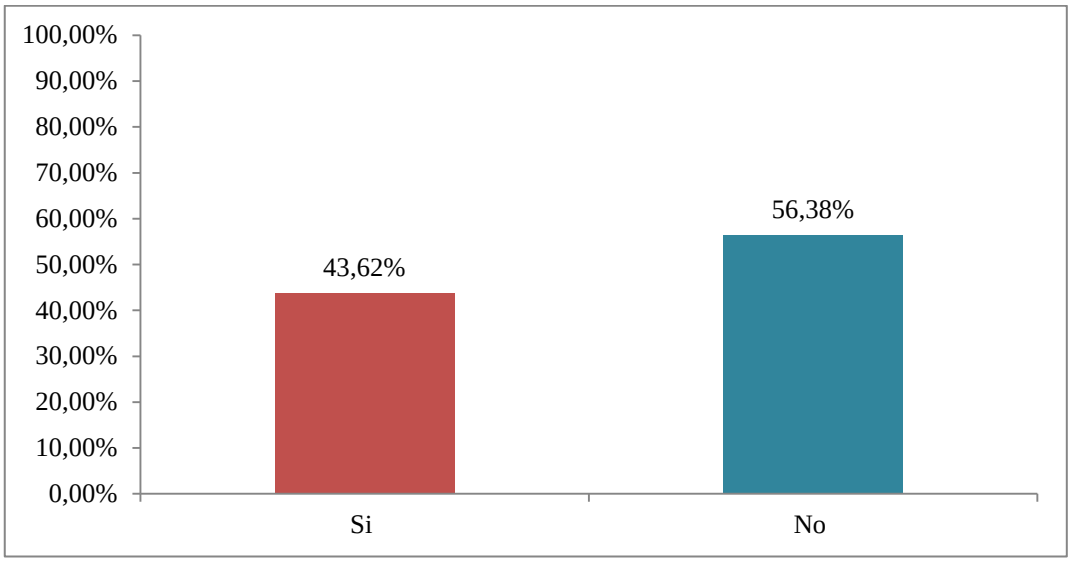

Figura 13: Implementación de proyectos en TIC para la mejora de la productividad.
Fuente: Ministerio de Telecomunicaciones del Ecuador, 2014.

Son conocidos los beneficios que ofrecen las TIC relacionadas con la eficiencia laboral, por lo tanto deben ser consideradas como mecanismos para mejorar los procesos de las instituciones públicas. Los resultados de la encuesta identifican que el 56% de las instituciones públicas, no cuentan con proyectos en TIC para mejorar la productividad institucional.

- ✓ **Conocimiento sobre los beneficios de gobierno electrónico:** Representa el grado de conocimiento de los funcionarios, respecto al mejoramiento en los servicios que ofrece el gobierno electrónico.

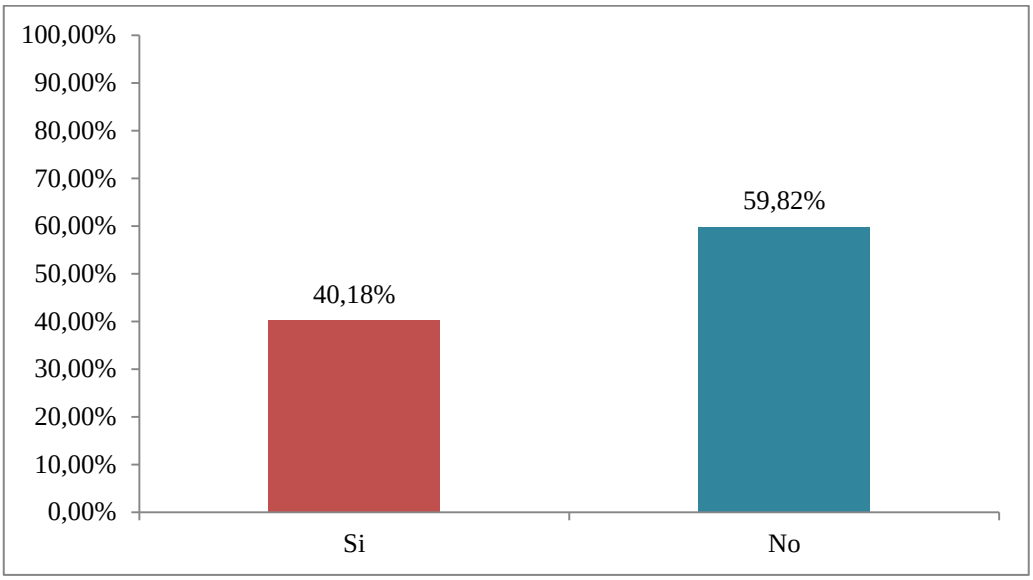

Figura 14: Conocimiento sobre los beneficios de gobierno electrónico.
Fuente: Ministerio de Telecomunicaciones del Ecuador, 2014.

Los resultados de la encuesta muestran, que el 60% de los funcionarios *no* conoce los beneficios atribuidos a la implementación del gobierno electrónico, el cual es un indicativo de que el sector público no conoce los beneficios provenientes de la innovación tecnológica, para el ofrecimiento y mejoramiento de servicios.

- ✓ **Implementación de gobierno electrónico:** Representa el uso de las TIC por parte de las instituciones gubernamentales, con el objetivo de mejorar cualitativamente los servicios a usuarios internos y externos.

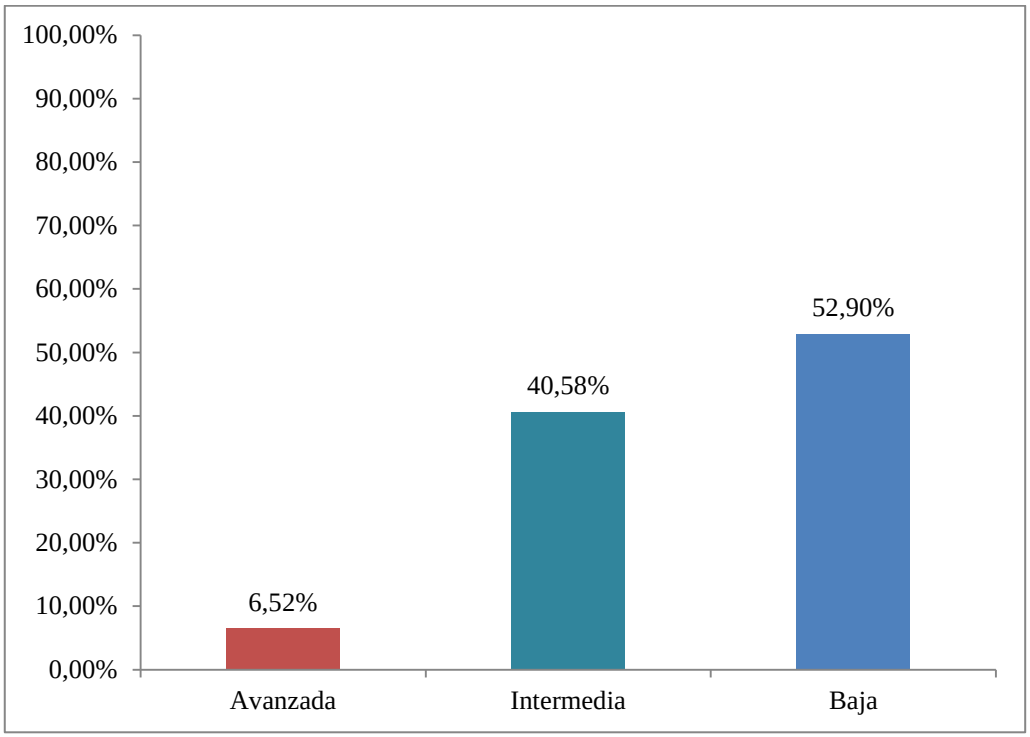

Figura 15: Implementación del Gobierno Electrónico.
Fuente: Ministerio de Telecomunicaciones del Ecuador, 2014.

En general el estado de la implementación del gobierno electrónico de acuerdo a la investigación llevada a cabo por el Ministerio de Telecomunicaciones, la ubican en su mayoría como *intermedia*; donde solo el 6% de las entidades públicas son consideradas con un estado de implementación de gobierno electrónico *avanzada*.

1.3 Marco Jurídico de las Políticas Públicas de las TIC

El propósito de este punto es caracterizar el marco jurídico que opera en el Ecuador, respecto a la regulación publica sobre las TIC. Existen Leyes, Acuerdos Internacionales, y Reglamentos, Decretos Ejecutivos, Resoluciones y Acuerdos Ministeriales, que tienen validez jurídica y que influyen directa e indirectamente sobre las políticas públicas de las TIC.

- ✓ **Leyes:**
    a. Constitución Política del Ecuador.
    b. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
    c. Ley de Gobierno Electrónico.
    d. Ley Orgánica de Transparencia y Acceso a la información Pública.
    e. Ley del Sistema Nacional de Registro de Datos Públicos.
    f. Código Orgánico Integral Penal.
    g. Entre otras leyes, normas o decretos cuya materia trate sobre la gestión de activos de información.

- ✓ **Convenios Internacionales:**

    a. Convenio Internacional de Telecomunicaciones.
    b. Constitución Internacional de Telecomunicaciones.
    c. Constitución de la Organización Internacional de Telecomunicaciones por Satélite.
    d. Normas que regulan el proceso de integración y liberalización del comercio de Servicios de Telecomunicaciones en la Comunidad Andina.
    e. Convención Interamericana sobre Radiocomunicaciones.

- ✓ **Acuerdos Ministeriales:**

    a. Acuerdo N° 804 y 837: La Creación de la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación.
    b. Acuerdo N° 166: Uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000, para la Gestión de la Seguridad de la Información.

1.3.1 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

En el año 2002 el Congreso Nacional de la República del Ecuador considera que, el uso de sistemas de información y de redes electrónicas, han adquirido importancia para el desarrollo del comercio y la producción, tanto para el sector público como para el sector privado, siendo necesario impulsar el acceso de las población a estos servicios, para fomentar el desarrollo del comercio, educación y cultura. Siendo así, es indispensable que el Estado Ecuatoriano cuente con herramientas jurídicas que le permitan el uso de los servicios electrónicos, incluido el comercio electrónico y acceder con mayor facilidad a la compleja red de los negocios internacionales.

El objetivo de la ley es: regular los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas. Los mensajes de datos están considerados como: la información que ha sido generada, enviada, recibida, almacenada o comunicada a través de medios electrónicos.

De acuerdo a la Ley de Comercio Electrónico una firma electrónica son: los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.

1.3.2 Acuerdo Interministerial N° 166. Uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000

Es importante mantener políticas claras que en conjunto con estrategias, normas, procesos y procedimientos mantengan la seguridad de la información que se genera y almacena en los diferentes medios electrónicos, en las entidades de la Administración Pública Central, Institucional y que dependan de la Función Ejecutiva, siendo esta la razón por la cual se crea el acuerdo interministerial N° 166, que dispone: a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información. Las Entidades dispondrán de un plazo de 18 meses para a la implementación a partir del 19 de septiembre de 2013.

Como primer paso las entidades deberán designar al interior de su institución un Oficial de Seguridad de la Información, el mismo que deberá ser comunicado a la Secretaria Nacional de la Administración Pública.

La Secretaria Nacional de la Administración Pública, será quien coordine y de seguimiento a la implementación del Sistema de Gestión de Seguridad de la Información, así también deberá realizar de forma ordinaria una revisión anual al Sistema de Gestión.

Es responsabilidad de la autoridad de cada institución, mantener la documentación de la implementación del Sistema de Gestión de Seguridad de la Información de manera organizada y registrada, de acuerdo a los procedimientos que establezca la Secretaria Nacional de la Administración Pública.

1.3.3 Esquema Gubernamental de Seguridad de la Información (EGSI)

Los crecientes avances de la tecnología de la información han causado que el gobierno ecuatoriano preste una mayor atención a la protección de sus activos de información, con el fin minimizar los riesgos que conllevan las vulnerabilidades en

los sistemas de información, generando así confianza en la ciudadanía y a nivel interno de la instituciones.

Entre los meses de julio y agosto de 2011, la Secretaria Nacional de Administración Publica emite los Acuerdos Ministeriales N° 804 y N° 837, en donde se establece la Comisión para la Seguridad Informática y de las Tecnologías de la información y Comunicación.

Dicha comisión determinó tras un análisis de la situación de la gestión de la seguridad de la información en las instituciones públicas, la necesidad de aplicar normas y procedimientos para asegurar la información e incorporar a los procesos de gestión una cultura de seguridad.

En septiembre de 2013, la Comisión para la Seguridad y de las Tecnologías de la Información y Comunicación da a conocer el Esquema Gubernamental de Seguridad de la Información (EGSI), el cual se encuentra basado en la norma técnica ecuatoriana INEN ISO/IEC 27002 para la Gestión de la Seguridad de la Información, el mismo que está dirigido para las Instituciones de Administración Pública Central. Este esquema determina un conjunto de directrices prioritarias para la Gestión de la Seguridad de la Información.

Para ello la Secretaria Nacional de la Administración Pública, a través del EGSI determina las siguientes directrices, para la Gestión de la Seguridad de la Información:

- Política de Seguridad de la Información.
- Organización de la Seguridad de la Información.
- Gestión de los Activos.
- Seguridad de los Recursos Humanos.
- Seguridad Física y del Entorno.
- Gestión de Comunicaciones y Operaciones.
- Control de Acceso.

- Adquisición, Desarrollo y Mantenimientos de Sistemas de información.
- Gestión de los Incidentes de la Seguridad de la Información.
- Gestión de la continuidad del negocio.
- Cumplimiento normativo.

1.4 Seguridad de la información

En Ecuador se empezaron a registrar delitos informáticos en el año 2009; éstos a la fecha viven su apogeo, siendo cada día más común los ataques a servicios financieros, robo de cuentas bancarias, clonación de tarjetas e identidades, daño de la imagen corporativa, robo, alteración y espionaje a la información de las organizaciones, trayendo como resultado pérdidas económicas y desconfianza entre los usuarios. Estadísticas obtenidas en la fiscalía del Ecuador muestran la evolución de los casos de delitos informáticos, existiendo registros durante el período 2009 - 2011de un total de 3100 denuncias, sin embargo sólo en el 2012 se registraron 3500 denuncias, esto significa un incremento del 70%.

Las organizaciones ecuatorianas se enfrentan cada vez más a riesgos e inseguridades procedentes de una gran variedad de orígenes, que pueden dañar de forma importante su información y pueden poner en peligro la continuidad del negocio. En muchos de los casos, se encargan la elaboración de sus portales o sistemas de información a terceros, descuidando el manteamiento y actualización de los mismos, siendo el tema de seguridad algo no incluido en la lista de sus prioridades.

La seguridad de la información desempeña un papel importante en el desarrollo de las tecnologías de la información, así como de los servicios de Internet. Implementar sistemas de gestión de seguridad y proteger las infraestructuras de la información críticas, es esencial para lograr la seguridad y el bienestar económico de cada país. Conseguir un servicio de Internet más seguro y proteger a los usuarios, se ha convertido en parte integrante del desarrollo de nuevos servicios, así como de la política gubernamental.

La Superintendencia de Telecomunicaciones, como Organismo Técnico de Control en sus objetivos, destaca el compromiso de combatir el fraude en el sector de las

telecomunicaciones, ya que el rápido desarrollo de las tecnologías de la información y de las comunicaciones (TIC) resulta en un potencial desafío e incluso amenaza a la privacidad personal.

1.4.1 Antecedentes de fallas en la seguridad de la información en instituciones públicas

En las instituciones públicas del Ecuador se han registrado una serie de incidentes de seguridad en los sistemas de información, causando graves perjuicios económicos y generando desconfianza en la población. La principal causa se debe a la ausencia o incumplimiento de controles, normas o políticas para proteger la información.

A continuación se citan algunos casos conocidos de incidentes de seguridad en instituciones públicas:

- Ministerio del Ambiente - año 2012: Al menos 5.4 millones de dólares fueron sustraídos por funcionarios de la Dirección Financiera, debido a un mal manejo de las contraseñas.

- Ministerio de Salud/Finanzas - año 2012: Se registraron transferencias ilícitas de más de 3 millones de dólares, debido a una falla contable en el sistema de administración financiera *E-Sigef*.

- Consejo Nacional Electoral - año 2012: Miles de ciudadanos denunciaron haber sido incluidos en registros electorales sin su autorización, este ilícito fue realizado por el mundialmente conocido delito de compra de bases de datos.

- Municipalidad de Riobamba - año 2013: Funcionarios del Municipio detectaron transferencias ilícitas por 13 millones de dólares, debido a un mal manejo de las contraseñas.

(Ministerio de Finanzas, 2014)

1.4.2 Delitos contra la seguridad de los activos de los sistemas de información y comunicación

En febrero de 2014, la Asamblea Nacional de la República del Ecuador hace público el nuevo Código Orgánico Integral Penal, el cual fue reformado, su antecesor fue codificado en octubre 1971 y ha sufrido un sin número de reformas hasta mayo del 2010.

Siendo así el nuevo código penal ahora tipifica los delitos en contra de las TIC en los artículos 229-234:

- Revelación ilegal de base de datos.
- Intercepción ilegal de datos.
- Transferencia electrónica de activo patrimonial.
- Ataque a la integridad de los sistemas informáticos.
- Delitos contra la información pública reservada legalmente.

1.4.2.1 Revelación ilegal de base de datos

Las personas que revelen para beneficio propio o de terceros, la información registrada en ficheros, archivos, bases de datos o medios semejantes a través de medios electrónicos o de telecomunicaciones, voluntaria e intencionalmente, será sancionada con pena privativa de libertad de uno a cinco años, dependiendo si el infractor pertenece al sector público o al sector de la banca. (Ministerio de Justicia del Ecuador, 2014)

1.4.2.2 Interceptación ilegal de datos

La persona que sin orden judicial previa, para beneficio propio o de terceros, intercepte, escuche, desvíe, grabe u observe mensajes de datos con la finalidad de obtener información registrada o disponible o que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes de datos, con el objetivo de inducir a las

víctimas a ingresar a una dirección o sitio de internet diferente a la que quiere acceder, siendo el fin almacenar de manera ilícita la información. Aduanalmente, quien comercialice o copie información almacenada en las tarjetas de crédito, débito o pago, así como las personas que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados para permitir dichos actos ilícitos, serán privados de libertad de tres a cinco años. (Ministerio de Justicia del Ecuador, 2014)

1.4.2.3 Transferencia electrónica de activo patrimonial

La persona que con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero o que proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona, serán privados de libertad de tres a cinco años. (Ministerio de Justicia del Ecuador, 2014)

1.4.2.4 Ataque a la integridad de sistemas de información

La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Cometa la infracción sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la

seguridad ciudadana. Será sancionada con pena privativa de libertad de tres a siete años. (Ministerio de Justicia del Ecuador, 2014)

1.4.2.5 Delitos contra la información pública reservada legalmente

La persona que destruya o inutilice información clasificada de conformidad con la Ley. Siendo servidor público, utilice cualquier medio electrónico o informático para obtener este tipo de información. Revele información reservada, la cual pueda comprometer gravemente la seguridad del Estado. Será sancionada con pena privativa de libertad de tres a diez años. (Ministerio de Justicia del Ecuador, 2014)

1.4.2.6 Acceso no consentido a un sistema de información

La persona que sin autorización acceda en todo o en parte a un sistema de información, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años. (Ministerio de Justicia del Ecuador, 2014)

2. FUNDAMENTO TEÓRICO

El propósito del presente capítulo es analizar los fundamentos teóricos, alcances y objetivos de la Norma ISO/IEC 27001, que tiene estricta relación con el Acuerdo Interministerial N° 166 y el Esquema Gubernamental de Seguridad de la Información, mismos que deben aplicarse en las Instituciones de Administración Pública Central, los cuales hacen referencia a la implementación obligatoria de un sistema de gestión de la seguridad de la información.

2.1 Sistema de Gestión de la Seguridad de la Información (SGSI)

Un sistema de gestión de la seguridad de la información sirve para garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por parte de la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (Instituto Ecuatoriano de Normalización, 2012)

Por tanto dicho sistema de gestión, podría considerarse, por analogía con la norma ISO 9001, como el sistema de calidad para la seguridad de la información.
Para la presente investigación, se entiende por información todo aquel conjunto de datos sometidos a un procesamiento y que posean valor para la organización, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración. (Iso27000.es, 2014)

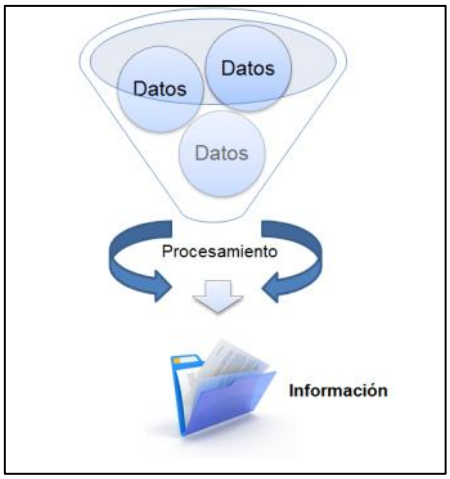

Figura 16: Transformación de la información.

Durante esta investigación definiremos que la seguridad de la información, consiste en la preservación de su confidencialidad, integridad, disponibilidad y no repudio, así como de los sistemas implicados en su tratamiento, dentro de la organización. (Iso27000.es, 2014)

• Confidencialidad: La información no debe estar disponible, ni ser revelada a individuos, entidades o procesos no autorizados.

• Integridad: La información debe mantener la exactitud con la cual fue generada, previniendo las modificaciones no autorizadas.

• Disponibilidad: El acceso y utilización de la información, por parte de los usuarios entidades o procesos autorizados cuando lo requieran.

• No repudio: O irrenunciabilidad, permite probar la partición de las partes en una comunicación.

La información en conjunto con sus procedimientos y sistemas que hagan uso de ella, es uno de los activos más importantes de una organización. La confidencialidad, integridad y disponibilidad de información pueden llegar a ser esenciales para salvaguardar los niveles de competitividad, rentabilidad e imagen corporativa, necesarias para lograr los objetivos de la organización. (IT360.es, 2014)

Los activos están considerados como toda información o sistema de información (hardware, software, documentación, etc.), que tenga valor para la organización. (IT360.es, 2014)

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo.

Asegurar un nivel de protección total es prácticamente imposible, incluso disponiendo de recursos ilimitados. El propósito de gestionar la seguridad de la información es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por parte de la organización, adaptándose a los cambios que se produzcan en el entorno. (Instituto Ecuatoriano de Normalización, 2011)

2.1.1 Normas para un Sistema de Gestión de la Seguridad de la Información

Este conjunto de normas, tienen como propósito la creación y mantenimiento de un Sistema de Gestión de la Seguridad de la Información, proporcionando un marco de gestión de la seguridad de la información, utilizable por cualquier tipo de organización, pública o privada, grande o pequeña; fue desarrollado por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission). (Iso27000.es, 2014)

2.1.1.1 Origen

En el año 1901, el Comité de Ingeniería de normas de Londres, funda la primera entidad de normalización a nivel mundial, BSI (British Standards Institution), que es responsable de la publicación de importantes normas como:

- ✓ 1979 Publicación BS 5750 - en la actualidad ISO 9001.
- ✓ 1992 Publicación BS 7750 - en la actualidad ISO 14001.
- ✓ 1995 Publicación BS 7799 - en la actualidad ISO 27001.

- ✓ 1996 Publicación BS 8800 - en la actualidad OHSAS 18001.

La norma BS 7799 1-2 de BSI aparece por primera vez en 1995, con el objetivo de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de esta noma es una guía de buenas prácticas, para la que no se establece un esquema de certificación. En la segunda parte publicada por primera vez en 1998, se establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable.

En el año 2005 y con alrededor de 1700 empresas certificadas en BS7799-2, la Organización Internacional de Normalización ISO, publica el estándar ISO 27001:2005 y la guía de buenas prácticas toma el nombre de la ISO 27002:2005. (Ramírez Castro & Ortiz Bayona, 2011)

2.1.1.2 Familia de normas

- ✓ **ISO/IEC 27000**: Sistema de gestión de seguridad de la información. Descripción general y vocabulario.

- ✓ **ISO/IEC 27001**: Sistema de gestión de seguridad de la información. Requisitos.

- ✓ **ISO/IEC 27002:** Código de prácticas para la gestión de la seguridad de la información.

- ✓ **ISO/IEC 27003:** Guía de implementación del sistema de gestión de la seguridad de la información.

- ✓ **ISO/IEC 27004:** Gestión de la seguridad de la información. Métricas e indicadores.

- ✓ **ISO/IEC 27005:** Gestión de riesgo de la seguridad de la información.

- ✓ **ISO/IEC 27006:** Requisitos para organizaciones que proveen la auditoria y certificación de los sistemas de gestión de la seguridad de la información.

- ✓ **ISO/IEC 27007:** Directrices para la auditoría de los sistemas de gestión de la seguridad de la información.

- ✓ **ISO/IEC 27011:** Directrices para la gestión de la seguridad de la información para organizaciones de telecomunicaciones, basada en la norma ISO/IEC 27002.

- ✓ **ISO/IEC 27799:** Gestión de la seguridad de la información para la salud, basada en la norma ISO/IEC 27002.

- ✓ **ISO/IEC 27035:** Gestión de incidentes de seguridad de la información.

De todo el conjunto de normas que hacen parte del SGSI, la única certificable es la norma ISO/IEC 27001, la misma que especifica todos los requisitos necesarios para el establecimiento de los sistemas de gestión de seguridad de la información, con el apoyo conjunto del resto de normas del SGSI. (IT360.es, 2014)

A continuación se muestra un diagrama de interacción entre las diferentes normas:

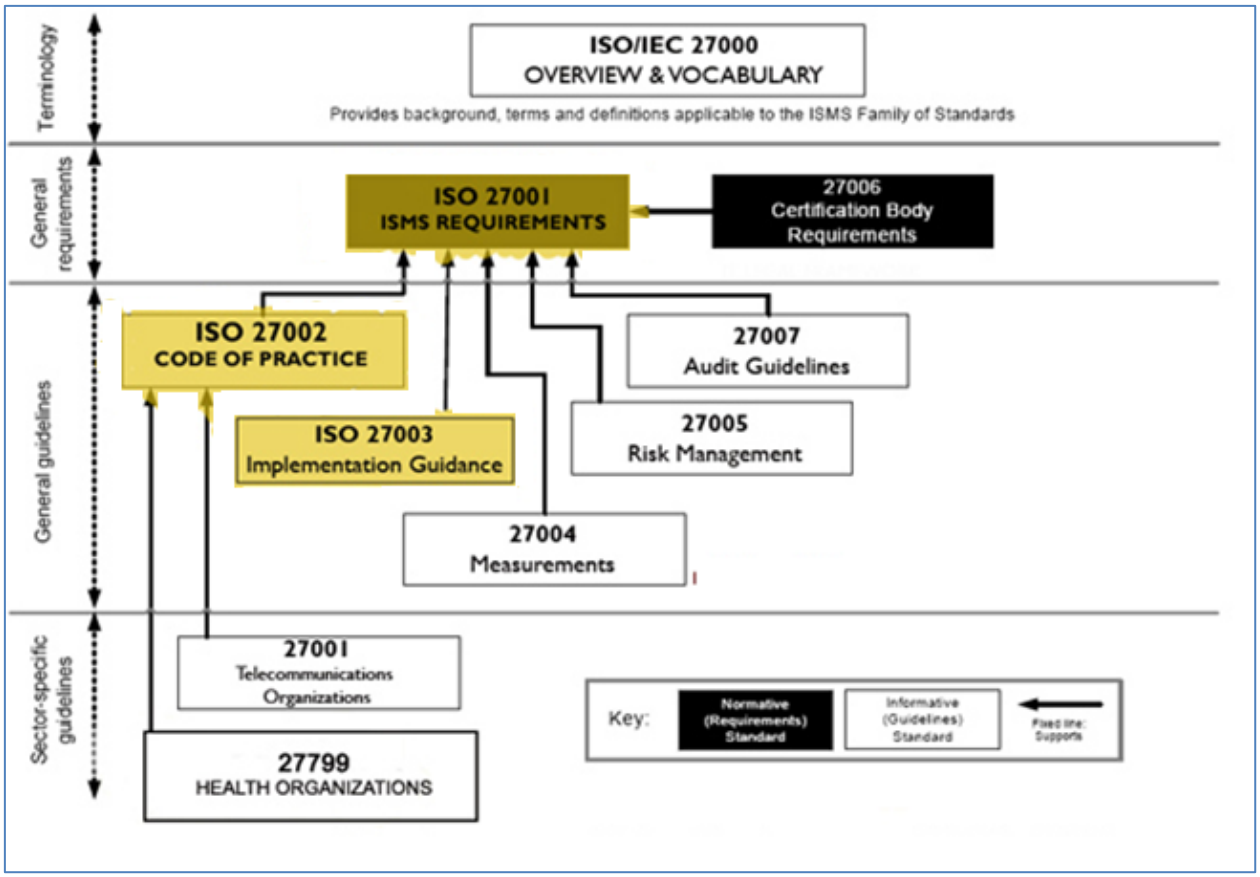

Figura 17: Relación entre la familia de normas ISO/IEC 27000.
Fuente: IT Audit & Innovation.

2.2 Norma NTE INEN–ISO/IEC 27001:2011

En el año 2011 el Instituto Ecuatoriano de Normalización, realiza una traducción idéntica de la Norma Internacional ISO/IEC 27001:2005, la cual se adopta para el Ecuador como NTE INEN –ISO/IEC 27001:2011.

Esta norma proporciona los requisitos de un modelo certificable para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de la Seguridad de la Información (SGSI). La adopción de esta norma deber ser fruto de una decisión estratégica tomada por la alta dirección de las organizaciones. El diseño y la implementación del SGSI, así como sus requisitos de seguridad, procesos, tamaño y estructura, se ajustará a las necesidades de cada organización. (Instituto Ecuatoriano de Normalización, 2011)

La norma NTE INEN–ISO/IEC 27001:2011 se encuentra diseñada para coexistir de manera integrada y consistente con las normas ISO/IEC 9001 (Sistema de gestión de la calidad) e ISO/IEC 14001 (Sistema de gestión Ambiental).

De acuerdo a la norma NTE INEN–ISO/IEC 27001:2011, un proceso se define por: cualquier actividad que utiliza y se gestiona de modo que permite la transformación de unos elementos de entrada en unos elementos de salida. La aplicación de un conjunto de procesos en una organización, junto a la identificación de estos y sus interacciones y su gestión, pueden calificarse de enfoque por proceso.

La norma NTE INEN–ISO/IEC 27001:2011 implementa el modelo Planear, Hacer, Verificar y Actuar (PHVA o ciclo de Deming), para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora del SGSI.

Es importante tener claro la definición de las siguientes etapas durante un sistema de gestión de seguridad de la información, de acuerdo a la norma NTE INEN–ISO/IEC 27001:2011:

- Planificar: Identificar los requisitos de seguridad de la información, y la necesidad de establecer una política de seguridad de la información junto a sus objetivos.

- Hacer: Implementar y operar los controles para administrar los riesgos de seguridad de la información.

- Verificar: Supervisar y revisar el rendimiento y la eficacia del SGSI.

- Actuar: Asegurar la mejora continua del SGSI.

A continuación se muestra el ciclo de vida del SGSI, que implementa un enfoque basado en proceso de acuerdo al modelo PHVA.

Figura 18: Ciclo de vida del SGSI
Fuente: ISOTools – Webinar.

Para cumplir con el objetivo de la norma NTE INEN–ISO/IEC 27001:2011, esta ha sido desarrollada de forma metodología con cláusulas y anexos, donde se incluyen los objetivos de control y controles.

En la siguiente tabla se muestra su estructura:

Tabla 5:

Estructura de la Norma ISO 27001

Introducción.	-	-	-
Objeto.	1	-	-
Referencias Normativas.	2	-	-
Términos y Definiciones.	3	-	-
Sistema de Gestión de Seguridad de la Información.	4	4.1 Requisitos Generales.	-
		4.2 Establecer y Gestionar el SGSI.	4.2.1 Establecer el SGSI.
			4.2.2 Implementar y operar el SGSI.
			4.2.3 Monitorear y revisar el SGSI.
			4.2.4 Mantener y mejorar el SGSI.
		4.3 Documentar.	4.3.1 Generalidades.
			4.3.2 Controlar documentos.
			4.3.3 Controlar los registros.
Responsabilidad de la Dirección	**5**	5.1 Compromiso de la dirección.	-
		5.2 Gestionar los recursos.	5.2.1 Provisión de recursos.
			5.2.2 Capacitación y entrenamiento.
Auditorías Internas del SGSI	**6**	-	-
Revisión por la Dirección del SGSI	**7**	7.1 Generalidades.	-
		7.2 Elementos de entrada para revisión.	-
		7.3 Resultados de la revisión.	-

Tabla 5:

(Continuación)

Mejora del SGSI	**8**	8.1 Mejoramiento continuo.	-
		8.2 Acción correctiva.	-
		8.3 Acción preventiva.	-
Anexos	**-**	Anexo A Normativo: Objetivos de control y controles. Anexo B Informativo. Anexo C Informativo.	-
Bibliografía	**-**	-	-

La presente norma hace referencia explícita al código de buenas prácticas para la gestión de la seguridad de la información ISO/IEC 27002. En el año 2011, la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación desarrolló el Esquema Gubernamental de Seguridad de la Información (EGSI), que se encuentra basado en la norma ISO/IEC 27002.

Como se había mencionado anteriormente el objetivo de los sistemas de gestión de seguridad de la información es preservar la disponibilidad, confidencialidad, integridad y el no repudio de los activos de información. En la siguiente figura se puede ver como los controles planteados por la norma NTE INEN –ISO/IEC 27001:2011, están dirigidos a gestionar la Seguridad de la Información.

A continuación se realiza un análisis de la presente norma, utilizando como referencia el Esquema Gubernamental de Seguridad de la Información (Secretaría Nacional de la Administracion Pública , 2013), con el objetivo de generar la metodología de evaluación que permitan determinar el nivel de calidad de la seguridad de la información en el sector público.

2.2.1 Sistema de gestión de la seguridad de la información

Las Instituciones de la Administración Pública Central y que dependen de la Función Ejecutiva, de acuerdo al decreto No. 166, se encuentran obligadas a crear, implementar, operar, supervisar, mantener y mejorar un SGSI, el mismo que debe estar plenamente documentado.

2.2.1.1 Creación y gestión del SGSI

Para la creación y gestión del SGSI en las instituciones, se considera el Esquema Gubernamental de Seguridad de la Información EGSI, el cual hace referencia a la operación, riesgos, controles, auditorías internas y externas, planes de continuidad, entre otros, cuyo objetivo es determinar los activos a proteger.

La Secretaría Nacional de la Administración Pública (SNAP) con fecha 19 de Septiembre del 2013, emite el Acuerdo 166, documento en el cual se establece que las entidades de la Administración Pública que dependen de la Función Ejecutiva deben implementar de forma obligatoria las normas NTE INEN-ISO/ IEC 27000, para la gestión de la Seguridad de la información.
El SNAP, solicita a las entidades públicas, la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), que está basado en la norma INEN ISO/IEC 27002, cuyo plazo es hasta marzo de 2014 para las directrices señaladas como prioritarias, y hasta marzo de 2015 para el resto de directrices. (Secretaría Nacional de la Administracion Pública , 2013)

2.2.1.2 Planificación para la creación del SGSI

Las instituciones deben seguir las siguientes fases para la creación del SGSI de acuerdo a la norma NTE INEN–ISO/IEC 27001:2011:

a. Definición del alcance y límites del SGSI.
b. Definición de la política del SGSI.
c. Definición del enfoque de la evaluación de riesgos.

d. Identificación de los riesgos.
e. Análisis y valoración de los riesgos.
f. Identificación y evaluación de las opciones para el tratamiento de los riesgos.
g. Selección de los objetivos de control para el tratamiento de riesgos
h. Obtención de la aprobación de los riesgos residuales por parte de la dirección.
i. Autorización por parte de la dirección para implementar y operar el SGSI.
j. Elaboración de la declaración de aplicabilidad.

a. Alcance y límites del SGSI

La definición del alcance del SGSI es una de las fases más importantes dentro de este proceso, para ello en el Acuerdo Interministerial No. 166, se establece que cada institución implementará el EGSI de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de seguridad de la información.

Cabe recalcar que el alcance del SGSI, puede abarcar a toda la institución, parte de ella, un proceso o un sistema de información. Un punto que es importante tenerlo en cuenta durante la definición del alcance es que, cualquier exclusión de la misma debe ser plenamente justificada.

b. Política del SGSI

La política define el marco para establecer los objetivos y el rumbo del SGSI, para ello hay que tener en cuenta la Constitución, leyes y demás normativa legal propia de la institución. En el Esquema Gubernamental de la Seguridad de la Información se define la siguiente política de seguridad de la información como referencia:

> Las entidades de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera.

Dicha política podrá ser tomada por las distintas instituciones públicas como base, la cual puede ser ampliada o adaptada a la realidad de la institución.

c. Enfoque de evaluación de riesgos

El definir el enfoque para la evaluación de riesgo, es importante para que la seguridad de la información se gestione con éxito. Existen algunas metodologías que pueden satisfacer las necesidades de las instituciones, para ello la presente norma propone el análisis de diferentes metodologías que se pueden encontrar en la Norma ISO/IEC TR 13335-3 *Directrices para la gestión de la seguridad de TI*.

Sin embargo en referencia al Artículo 7 del Acuerdo Interministerial No. 166, establece que:

> Las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos de su institución, en base a la norma INEN ISO/IEC 27005 "Gestión del Riesgo en la Seguridad de la Información".

El marco de trabajo que la norma NTE INEN-ISO/ IEC 27001 establece para la evaluación de riesgos son los siguientes:

- ✓ Definir la metodología de evaluación de riesgo.
- ✓ Definir el criterio para la aceptación de riesgo.
- ✓ Especificar de manera documentada las circunstancias por las cuales la institución está dispuesta a aceptar los riesgos.
- ✓ Definir los niveles de riesgo aceptables.
- ✓ Cubrir a todos los controles que forman parte del SGSI.
- ✓ La evaluación de riesgos deben generar resultados comparables y reproducibles.

d. Identificación, análisis y evaluación de los riesgos

La Norma INEN ISO/IEC 27005 *Gestión del Riesgo en la Seguridad de la Información*, proporciona directrices para la gestión del riesgo en la seguridad de la información en las instituciones, dando soporte particular a los requisitos de un sistema de gestión de seguridad de la información SGSI, de acuerdo a la norma ISO/IEC 27001. (Instituto Colombiano de Normas Técnicas, 2009)

Dicha metodología inicia con tres pasos para gestionar el riesgo de seguridad de la información:

1. Identificación de los activos a proteger.
2. Estimación o análisis del impacto por la ocurrencia de riesgos sobre los activos.
3. Evaluación sobre los riesgos, para determinar la priorización y objetos de control.

En la figura que se muestra a continuación se observa la metodología para la gestión del riesgo en la seguridad de la información de acuerdo a Norma INEN ISO/IEC 27005:

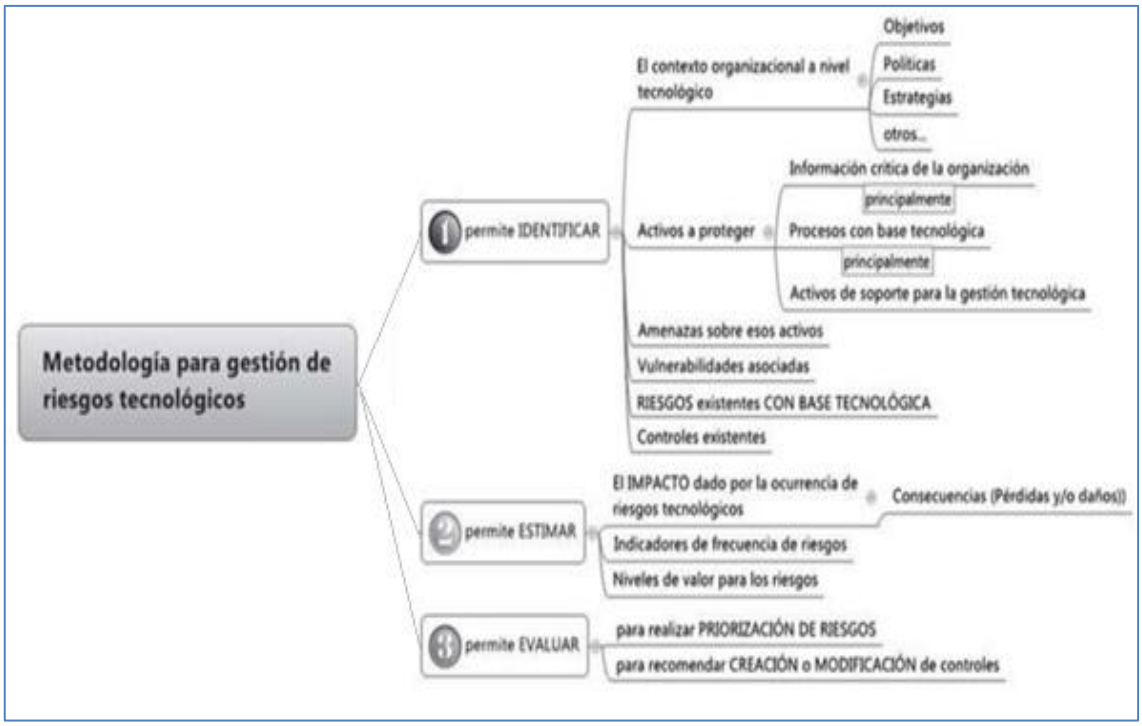

Figura 19: Metodología para gestión de riesgos tecnológicos.
Fuente: Ramírez Castro, Alexandra; Ortiz Bayona, Zulima, 2011.

e. Identificación de activos a proteger

Los activos de información hacen referencia a todos los elementos que contienen, mantienen o guardan la información, el análisis y la evaluación de los riesgos gira alrededor de los activos identificados, dentro del contexto de la presente norma un activo de información es cualquier cosa que tiene valor para la institución.

De acuerdo al Esquema Gubernamental de Seguridad de la Información, los activos de información se clasifican en las siguientes categorías:

- Activos primarios (datos, manuales, reglamentos, entre otros).
- Activos de soporte de hardware (computadoras, medios magnéticos, entre otros).
- Activos de soporte de software (sistemas operativos, software de servicio, software ofimático, entre otros).
- Activos de soporte de redes (interfaces de comunicación, switchs, ruteadoes, cortafuegos, entre otros).

- Estructura organizacional (objetivos, políticas, estrategias, organigrama, entre otros).

Es fundamental asignar los activos o grupos de ellos a una persona que actuará como responsable, este tendrá las siguientes funciones:

- Elaborar el inventario de los activos que se encuentre a su cargo.
- Delegar tareas rutinarias.
- Administrar la información.
- Elaborar las reglas para el uso aceptable.
- Clasificar, documentar y mantener actualizada la información.
- Tasación de los activos.

Los información referente a los activos deberá ser actualiza con una periodicidad no mayor a seis meses. (Secretaría Nacional de la Administracion Pública , 2013)

- ✓ **Identificación de amenazas**

Las amenazas son consideradas como cualquier evento que puede provocar daños en los activos de información, produciendo a la empresa pérdidas materiales o financieras. Una vez identificadas las amenazas, se debe evaluar su posibilidad de ocurrencia.
Estos eventos que causan las amenazas en los activos de información se las clasifican a continuación:

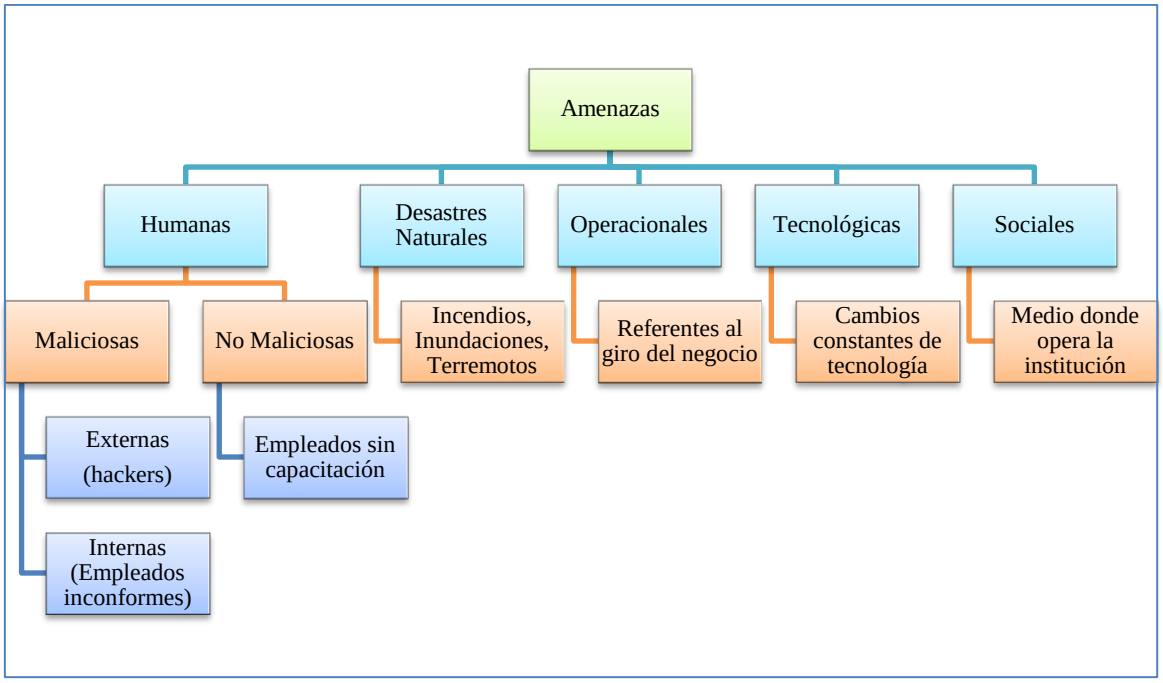

Figura 20: Clasificación de amenazas.

Para que una amenaza cause daño a algún activo de información, primero debe explotar una o más vulnerabilidades.

- ✓ **Identificación de vulnerabilidades**

Las vulnerabilidades son conocidas como debilidades que pueden ser explotadas por una o más amenazas. Estas pueden provenir por debilidades encontradas en el diseño físico, organizacional, personal, hardware, software o en la información que maneja la organización. Evaluar las vulnerabilidades, es el examen de las debilidades que pueden ser explotadas por las amenazas identificadas.

De acuerdo al Esquema Gubernamental de Seguridad de la Información, las vulnerabilidades se clasifican en las siguientes categorías:

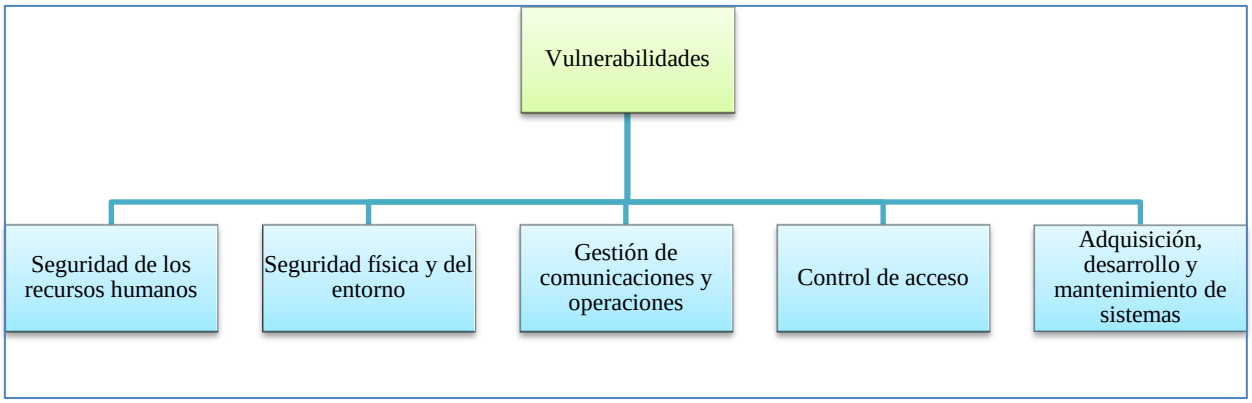

Figura 21: Clasificación de vulnerabilidades.

- ✓ **Riesgos existentes**

El riesgo es considerado como la posibilidad de que una amenaza se aproveche de las vulnerabilidades de un activo o grupo de activos, y por tanto cause daño a la organización. Para llegar a determinar los riesgos se deben plantear los escenarios, mediante los cuales se puedan explotar una determinada vulnerabilidad o grupo de vulnerabilidades.

- ✓ **Identificación de controles existentes**

Como parte final de este proceso de identificación de los activos de información, se debe comprobar si existen controles para el tratamiento de los riesgos. Una vez inventariados estos deben ser verificados para garantizar la fiabilidad del control. La efectividad de los controles es medida en base a que debe reducir la probabilidad de ocurrencia de la amenaza, o aumentar la dificultad de explotar una vulnerabilidad.

En el siguiente gráfico se detalla la interacción que existe entre los diferentes actores: amenazas, vulnerabilidades, activos, controles y riesgos.

Figura 22: Diagrama de interacción de riesgos.
Fuente: Portal de ISO 27001 en Español

- ✓ **Estimación del riesgo**

Las consecuencias tras la explotación de una amenaza por medio de una vulnerabilidad o grupo de ellas, deberán ser evaluadas para medir el impacto en la institución. Dicha evaluación se relaciona directamente con la tasación de los activos, ya que en base a este se obtiene el impacto en el negocio.

Un incidente en la seguridad de la información puede afectar a más de un activo, esto dependerá de la relación entre los activos, vulnerabilidades y amenazas. Las consecuencias de dichos incidentes se pueden expresar en términos financieros, técnicos, humanos u otros criterios relevantes para la institución.

Una vez identificados los diferentes escenarios de incidentes, es obligación establecer la probabilidad de ocurrencia y las consecuencias en el negocio. El resultado de la estimación del riesgo es la combinación de la probabilidad de un incidente y sus consecuencias.

- ✓ **Evaluación del riesgo**

Finalizada la estimación del riesgo, se debe determinar cuáles son los más significativos, para esta determinación algunos autores establecen los niveles de riesgos de acuerdo a su importancia, y los clasifican en:

- Impacto económico del riesgo.
- Tiempo de recuperación ante un incidente en la institución.
- Posibilidad real de ocurrencia.
- Posibilidad de interrumpir las actividades.
- Otros niveles que la institución determine pertinentes para la evaluación del riesgo.

f. Identificación y evaluación de las opciones para el tratamiento de los riesgos

De acuerdo a la norma NTE ISO/IEC 27005:2009, se propone cuatro opciones para la identificación y evaluación del tratamiento del riesgo.

1. Reducción del riesgo: Tiene por objetivo disminuir el nivel de riesgo identificado, mediante la implementación de controles a la interna de las instituciones, reduciendo así el impacto y la probabilidad de ocurrencia de daños sobre los activos de información.

2. La transferencia de riesgos a terceros: Consiste en transferir el riesgo a una parte externa de la institución, por ejemplo: a una aseguradora, que será la responsable de asumir las consecuencias en caso de existir un incidente sobre el activo de información.

3. Evitar el riesgo: Consiste en evitar la actividad o acción que produce riesgos, por ejemplo, si la institución determina que un equipo de comunicaciones genera un riesgo alto para ella, la forma de evitarlos podría ser parar el uso del mismo o cambiarlo, asumiendo los riesgos relacionados con la actividad o acción.

4. Aceptación del riesgo: Cuando los costos de implementación de un control, sobrepasa el valor del activo de información que se desea proteger o cuando el nivel del riesgo es muy bajo, la institución debe asumir los daños provocados en caso de existir un incidente.

g. Obtención de la aprobación de los riesgos residuales por parte de la dirección

Tras la implementación de los diferentes controles para el tratamiento de los riesgos, siempre existirá un remanente de esos mismos riegos, ya que es prácticamente imposible asegurar un nivel de protección total, incluso disponiendo de recursos ilimitados. El propósito de gestionar el tratamiento de los riesgos es garantizar que estos sean conocidos, asumidos, gestionados y minimizados por parte de las instituciones, adaptándose a los cambios que se produzcan en el entorno.

Para la presente investigación se define al riesgo residual como al riesgo que queda, tras la implementación de un plan de tratamiento de riesgos. Es necesario que la dirección de la institución esté en pleno conocimientos de cuáles son los riesgos residuales.

2.2.1.3 Implementación y operación del SGSI

Finalizado la etapa de la planificación del Sistema de Gestión de la Seguridad de la Información, se tiene como resultado el plan de tratamiento de riesgos sobre los activos identificados; de aquí en adelante es obligación de la dirección asignar los recursos necesarios, establecer las funciones, responsabilidades al personal y dar inicio a la implementación de los controles seleccionados en el plan de tratamiento de riesgos.

Es obligación de la institución definir los métodos de medición de la eficacia de los controles implementados, esto permite a la dirección y personal responsable determinar hasta qué punto los controles cumplen los objetivos de control planificados. La creación de programas de capacitación y concientización es obligatoria dentro del proceso de gestión del SGSI. Por último, es deber de la

institución actuar de forma proactiva en la detección de eventos o incidentes de seguridad.

Continuando con el ciclo del SGSI, nos encontramos en la fase de verificación (PH**V**A), para ello la institución debe:

- Ejecutar procedimientos de supervisión y revisión al SGSI.
- Revisar regularmente la efectividad del SGSI.
- Medir la efectividad de los controles.
- Revisar periódicamente los planes y opciones de tratamientos de riegos.
- Realizar auditorías internas.
- Realizar revisiones por parte de la dirección del SGSI, para asegurar que el ámbito de aplicación es el correcto e identificar que existan procesos de mejora al SGSI.
- Verificar que los planes de seguridad se encuentren actualizados, concluido el proceso de supervisión y revisión.
- Registrar los incidentes que pudieran afectar al funcionamiento del SGSI.

2.2.1.4 Mantenimiento y mejora del SGSI

Para finalizar el ciclo de gestión del SGSI, se debe implementar las mejoras identificadas al SGSI, tomando acciones correctivas y preventivas en materia de seguridad de la información, creando planes de comunicación de las acciones tomadas, que involucren a todas las partes interesadas en la institución, y por último se debe asegurar que las acciones tomadas alcancen los objetivos previstos.

En la siguiente figura se muestra el ciclo completo para crear, implementar, operar, supervisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información.

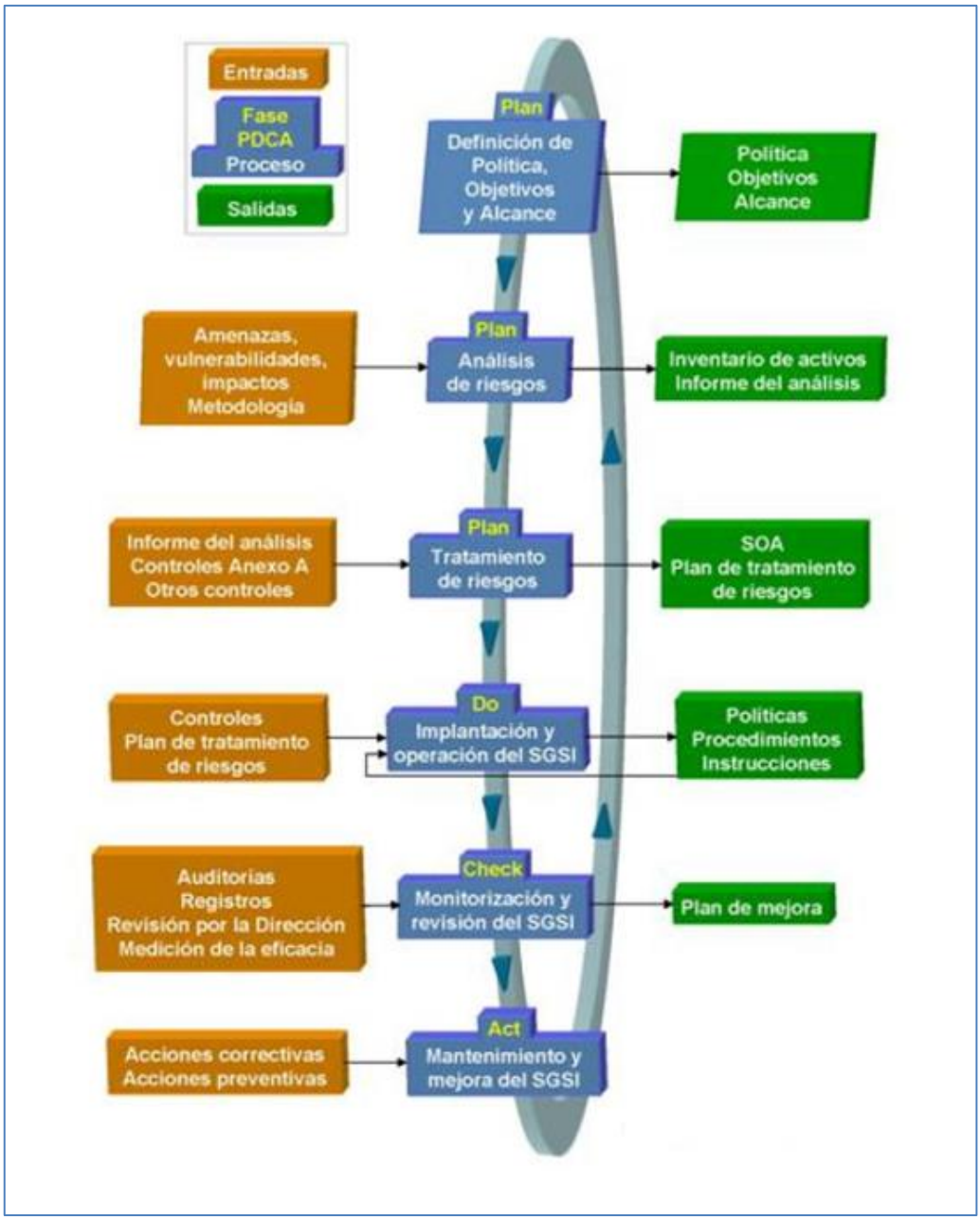

Figura 23: Modelo de implementación del SGSI.
Fuente: Portal de ISO 27001 en Español.

2.2.2 Anexo A (normativo) objetivos de control y controles

Los controles son los medios que se utilizan para gestionar el riesgo dentro una institución, el alcance de estos dentro del SGSI incluyen la política, objetivos de control, controles, procesos y procedimientos siendo la naturaleza de estos administrativa, técnica, de gestión o legales.

El Anexo A presenta un listado completo de controles agrupados en once objetivos de control. Dicho anexo proporciona una referencia, por lo tanto no son exhaustivas, la institución puede considerar que son necesarios objetivos y controles adicionales. Estos controles son los mínimos que se deberán aplicar, o justificar su no aplicación, los 11 objetivos adjuntos al Anexo A son:

1. Política de seguridad de la información: Expectativas de la organización referente a la gestión de la seguridad de la información.

2. Organización de la seguridad de la información: Estructura institucional donde se delegan responsables para la gestión de la seguridad de la información.

3. Gestión de los activos: Mantener un inventario de los activos de información.

4. Seguridad de los recursos humanos: Plantear los procedimientos necesarios para asegurar que los recursos humanos nuevos o actuales, comprendan la importancia de la seguridad de la información.

5. Seguridad física y del entorno: Establece la necesidad de proteger las áreas y equipos dentro de la institución.

6. Gestión de comunicaciones y operaciones: Se plantean los objetos de control para mantener la integridad, confidencialidad, disponibilidad y no repudio en las operaciones de procesamiento de información.

7. Control de acceso: Se establece los objetivos de control para monitorear y controlar los accesos (físicos o lógicos) a los activos de información.

8. Adquisición, desarrollo y mantenimientos de sistemas de información: Se planean los controles necesarios para incluir seguridad en los sistemas de información en todas sus etapas de desarrollo.

9. Gestión de los incidentes de la seguridad de la información: Establece que los incidentes en seguridad de la información deben ser gestionados y comunicados.

10. Gestión de la continuidad del negocio: Se plantean objetivos de control para evitar la interrupción del negocio.

11. Cumplimiento normativo: Toda acción mantenida o realizada como parte del proceso de implementación o gestión de la norma ISO/IEC 27001, debe concordar con los requisitos jurídicos internos y externos.

Figura 24: Objetivos de control para la protección de los activos de información.

Como se puede observar en el gráfico anterior, la finalidad de los 11 objetivos de control es asegurar que la información responda a los 4 parámetros de seguridad: disponibilidad, integridad, confidencialidad y no repudio.

3. DESARROLLO DE LA METODOLOGÍA DE EVALUACIÓN

El propósito del presente capítulo es desarrollar una metodología de evaluación, que permita determinar el grado con el cual es gestionado la seguridad de la información en Instituciones Públicas, dicha metodología es desarrollada en base a los parámetros de la norma NTE INEN-ISO/IEC 27001:2011.

3.1 Metodología de Evaluación

La metodología desarrollada durante la presente investigación es del tipo cualitativa, ya que se busca entender el nivel de calidad de la gestión en lo que respecta a la seguridad de la información en Instituciones Públicas. Para ello se analizó la norma NTE INEN-ISO/IEC 27001:2011, tomando como punto de referencia los objetivos de control y controles, adicionalmente se establecieron los parámetros básicos con los cuales se pueden medir y posicionar la gestión de la seguridad de la información en las instituciones públicas.

Estos parámetros son cuantificados a través de un modelo de evaluación, el cual está compuesto por variables e indicadores, y se lo ejecuta a través de una guía de entrevista y una guía de observación. Como parte de esta metodología se incorporó un modelo de madurez, que permite determinar cuantitativamente aspectos cualitativos objetos de la medición, permitiendo así posicionar a la organización dentro de un grado o nivel de calidad de gestión de la seguridad de la información.

3.1.1 Selección de variables

Los objetivos de control son los puntos críticos que se utilizan para evaluar la gestión de seguridad de la información dentro una institución, estos se dividen en once ítems los cuales se utilizaron como variables en el modelo de evaluación desarrollado.

A continuación se presentan las once variables utilizadas en el modelo:

1. **Política de seguridad**: Esta variable mide las directrices proporcionadas por parte de la dirección de la institución con respecto a la seguridad de la información de acuerdo al giro del negocio, con la legislación y normativas aplicables, adicionalmente se mide si dichas directrices están siendo distribuidas, socializadas, revisadas, medidas y mejoradas.

2. **Organización de la seguridad de la información**: Esta variable mide como está siendo gestionada la seguridad de la información dentro de la organización como con terceros, para ello se verifica el compromiso de las autoridades a través de la asignación de recursos, la coordinación entre los diferentes departamentos, la existencia de acuerdos de confidencialidad, que exista una revisión independiente de la seguridad de la información, entre otros.

3. **Gestión de los activos**: Esta variable mide si se están protegiendo y administrando adecuadamente los activos, así como, si la clasificación y protección de la información es la adecuada.

4. **Seguridad de los recursos humanos:** Esta variable busca medir si los procesos previo, durante y al finalizar el empleo con los funcionarios y/o contratistas son los adecuados para reducir el riesgo de robo, fraude o uso indebido de recursos.

5. **Seguridad física y ambiental:** Esta variable mide la gestión para prevenir los accesos físicos no autorizados, daños provocados por el hombre y daños provocados por desastres naturales, con el objetivo de evitar pérdidas, daños, robos que pongan en peligro los activos de la institución.

6. **Gestión de comunicaciones y operaciones**: Esta variable mide como está siendo gestionado el funcionamiento y operación de los recursos de tratamiento de la información, incluyendo controles a la provisión de

servicios, el intercambio de información, respaldo de la información, la gestión de almacenamiento y la supervisión de dichos procedimientos, siendo el objetivo primordial minimizar el riesgo de fallo en los sistemas y comunicaciones para proteger la integridad del software y de la información.

7. **Control de acceso:** Esta variable mide la gestión del acceso a la información por parte de los actores involucrados, así como la responsabilidad de los actores al manipular la información, esto a través de controles en las comunicaciones y en los sistemas de información.

8. **Adquisición, desarrollo y mantenimientos de sistemas de información:** Esta variable mide el tratamiento que se da a los sistemas de información cuando los mismos son adquiridos, desarrollados y/o actualizados, en donde se establecen controles para proteger la confidencialidad, autenticidad e integridad de la información que estos procesan.

9. **Gestión de los incidentes de la seguridad:** Esta variable mide la capacidad de gestión de la institución ante eventos de seguridad de la información por medio de la designación de responsabilidades y mecanismos de comunicación de eventos de seguridad, con el objetivo de que exista una oportuna toma de acciones correctivas.

10. **Gestión de la continuidad del negocio:** Esta variable busca medir el plan de contingencia que contrarreste posibles interrupciones de las actividades de la institución y procesos críticos de la misma, derivados de fallos importantes o catastróficos de los sistemas de información, así como su oportuna reanudación.

11. **Cumplimiento:** Esta variable mide el cumplimento de los requisitos legales, el cumplimiento de las políticas y normas de seguridad de la institución, así como las consideraciones sobre la auditoria a los sistemas

de información, con el objetivo de asegurar la correcta aplicación del sistema de gestión de seguridad de la información.

Dichas variables agrupan procesos determinados dentro de las áreas administrativas, áreas técnicas, áreas de gestión - planificación y área legal en la organización y estas permiten desglosar una serie de indicadores que responden a controles determinados en la norma NTE INEN-ISO/IEC 27001:2011.

3.1.2 Selección de indicadores

Los controles representan lineamientos que permiten gestionar los procesos de seguridad para la información con el objetivo de minimizar el riesgo ante posibles eventos de seguridad dentro de la organización. Los presentes controles representan los indicadores en el modelo de evaluación planteado para medir la gestión de seguridad de la información.
Dichos indicadores fueron planteados de forma agrupada para que permitan cuantificar a las variables mencionadas anteriormente y como están siendo gestionadas dentro de la organización.

A continuación se presentan los 81 indicadores planteados y su clasificación con respecto a cada variable:

Tabla 6:

Indicadores

Variable	Indicadores
Política de Seguridad.	Política de Seguridad.
	Distribución, Publicación y Conocimiento de la Política.
	Revisión a la Política.
	Medición de Política de Seguridad.
	Mejora de la Política de Seguridad.
Organización de la Seguridad de la Información.	Compromiso de la dirección.
	Coordinación y Responsabilidad de la seguridad de la información.
	Autorización de nuevos recursos para el tratamiento de la información.
	Acuerdo de Confidencialidad.
	Contacto con Autoridades y Grupos de Interés Especializados.
	Revisión independiente de la Seguridad de Información.
	Identificación de los riesgos y controles a la seguridad por el acceso de terceros.
	Tratamiento de la Seguridad en contratos con terceros.
	Tratamiento de la Seguridad con los ciudadanos.
Gestión de Activos y Clasificación de la Información.	Inventario de Activos.
	Propiedad de los activos.
	Reglamentos de Uso de activos.
	Directriz de clasificación.
Seguridad en Recursos Humanos.	Funciones, Responsabilidades.
	Investigación de antecedentes.
	Términos y Condiciones Contractuales.
	Responsabilidad de la dirección.
	Capacitación en seguridad de la información.
	Proceso disciplinario.
	Cese del empleo o cambio de puesto de trabajo.
Seguridad Física y Ambiental.	Perímetros y controles de seguridad física.
	Protección de las áreas críticas de activos de información contra amenazas externar y de origen ambiental.
	Trabajo en áreas seguras.
	Áreas de acceso público.
	Instalaciones de suministro y cableado.
	Mantenimiento de equipos.
	Seguridad de los equipos fuera de la organización.
	Reutilización o retiro seguro de equipos.
	Transporte de los activos de información propiedad de la organización.

Tabla 6:

(Continuación)

Variable	Indicadores
Gestión de Comunicaciones y Operaciones.	Documentación de procedimientos de operación.
	Control de cambios en activos.
	Separación de tareas.
	Separación de recursos.
	Provisión y supervisión de servicios prestados por terceros.
	Gestión del cambio en los servicios prestados por terceros.
	Gestión de capacidad de los recursos de tratamiento de la información.
	Aceptación de sistemas.
	Protección contra el código malicioso y descargable.
	Copias de seguridad.
	Controles de red.
	Seguridad de los servicios de red.
	Manipulación de los soportes.
	Intercambio de la información.
	Supervisión del tratamiento de la información.
Control de Acceso.	Políticas de Control de Accesos.
	Gestión de acceso de usuario.
	Responsabilidades de usuario.
	Uso de servicios de red.
	Autentificación de conexiones remotas.
	Identificación de equipos en redes.
	Protección de puertos de diagnóstico y configuración.
	Separación de redes.
	Control de Conexiones de redes inter organizacionales.
	Encaminamiento (routing) de red.
	Control de acceso y gestión de sistemas operativos.
	Política de uso Equipos portátiles o móviles.
	Política de Teletrabajo.
Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.	Especificación de requisitos de seguridad en los sistemas de información
	Tratamiento de las aplicaciones.
	Cifrado de contraseñas.
	Seguridad de los archivos de sistema.
	Control de cambios en aplicativos.
	Revisión técnica de aplicaciones tras cambios en el sistema operativo.
	Control de paquetes de software.
	Fugas de información.
	Control de desarrollo de sistemas externo.
	Control de vulnerabilidades.

Tabla 6:

(Continuación)

Variable	Indicadores
Gestión de incidentes de seguridad.	Notificación de eventos y puntos débiles de seguridad.
	Responsabilidad y procedimientos ante eventos de seguridad.
	Valoración de incidentes de seguridad.
	Recopilación de evidencias.
Gestión de la continuidad del negocio.	Plan de continuidad del negocio.
	Mantenimiento del plan de continuidad del negocio.
Cumplimiento normativo.	Cumplimiento de requisitos legales.
	Cumplimiento de política y normas de seguridad y Cumplimiento Técnico.
	Auditoria de los sistemas de información.

Los indicadores anteriormente expuestos fueron sometidos a un análisis para determinar el nivel de madurez que aportan a la gestión de la variable.

3.1.3 Modelo de madurez

El modelo de madurez utilizado en la presente metodología fue elaborado por el CMMI, que es el acrónimo de *Integración de Modelos de Madurez de Capacidades* (Capability Maturity Model Integration) y hace referencia a modelos con las mejores prácticas que ayudan a las organizaciones a evaluar, controlar y mejorar sus procesos. Fueron desarrollados por equipos de trabajo formados por especialistas de la industria, con el apoyo de once gobiernos (Colombia, Reino Unido, Qatar, Sudáfrica, Malasia, Tailandia, Estados Unidos, Bulgaria, Kenia, China y Vietnam) y el Software Engineering Institute (SEI) que posteriormente transfirió los derechos al CMMI Institute para su operación y comercialización. (Software Engineering Institute, 2010)

Dichos modelos sirven para conocer la madurez de los procesos y su aplicabilidad en varias áreas incluida la de las Tecnologías de la Información y Comunicaciones, el mismo sirve para develar la capacidad de las organizaciones y para que las mismas implementen estrategias para la mejora. CMMI contienen los elementos

esenciales para la evaluación, control y mejora de procesos. Estos elementos se basan en los conceptos para la mejora de procesos junto a los principios de control estadístico de la calidad desarrollados por Crosby, Deming, Juran y Humphrey. (Software Engineering Institute, 2010)

Luego de la publicación de la Constitución de la República del Ecuador en el año 2008, hubo dos visiones que marcaron el direccionamiento estratégico del Gobierno en funciones, siendo estas la recuperación del estado y la planificación. Como una acción direccionada a conseguir los cambios que la sociedad necesitaba. Surge ante ello el programa Gobierno por Resultados (GPR), con el objetivo de implementar una metodología de gestión gubernamental por resultados. El GPR busca aplicar e instaurar una metodología de planificación y gestión gubernamental para resultados, que permita la gestión de mapas estratégicos, objetivos, indicadores, metas, proyectos y procesos, esto mediante el uso de herramientas informáticas.
(Corporación EKOS, 2013)

La Secretaria Nacional de Administración Pública en el año 2010, aplicó una metodología sustentada con las mejores prácticas internacionalmente reconocidas, midiendo la administración de procesos con una escala de madurez institucional de administración de procesos similar a la utilizada en la presente metodología.

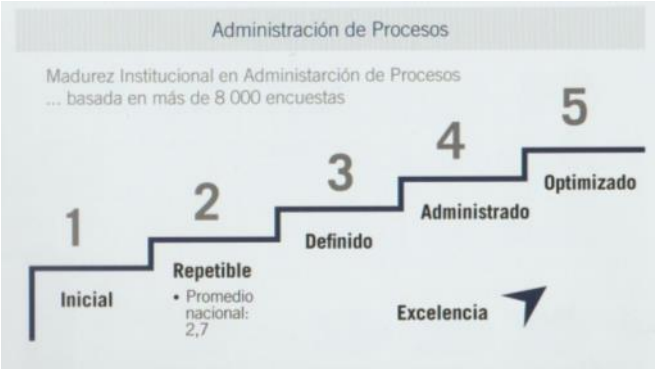

Figura 25: Madurez Institucional de Administración de Procesos.
Fuente: Gobierno por Resultados.

Los niveles de madurez se refieren a la consecución de la mejora de procesos de una organización en múltiples áreas.. Los cinco niveles de madurez se numeran del 1 al 5. (Software Engineering Institute, 2010)

Figura 26: Niveles de madurez.
Fuente: Estándares de Calidad de Software CMMI.

De acuerdo al CMMI Institute, un nivel de madurez se define como una plataforma evolutiva definida para la mejora de procesos de la organización.

A continuación se describen los conceptos de los cinco niveles de madurez:

- **Nivel de madurez 1: Inicial**

En el nivel de madurez 1, los procesos son generalmente ad hoc y caóticos. La organización generalmente no proporciona un entorno estable para dar soporte a los procesos. El éxito en estas organizaciones depende de la competencia y la heroicidad del personal de la organización, y no del uso de procesos probados. (Software Engineering Institute, 2010)

- **Nivel de madurez 2: Gestionado**

En el nivel de madurez 2, se garantiza que los procesos se planifican y ejecutan de acuerdo con las políticas; se emplea personal calificado que dispone de recursos adecuados para producir resultados controlados; se involucra a las partes interesadas relevantes; se monitorizan, controlan y revisan; y se evalúan en cuanto a

la adherencia a sus descripciones de proceso. La disciplina de proceso reflejada por el nivel de madurez 2, ayuda a asegurar que las prácticas existentes se mantengan durante periodos bajo presión. (Software Engineering Institute, 2010)

- **Nivel de madurez 3: Definido**

En el nivel de madurez 3, los procesos están bien caracterizados y comprendidos, y se describen en estándares, procedimientos, herramientas y métodos. El conjunto de procesos estándar de la organización, que es la base del nivel de madurez 3, se establece y se mejora a lo largo del tiempo. Estos procesos estándar se utilizan para establecer la integridad en toda la organización. (Software Engineering Institute, 2010)

- **Nivel de madurez 4: Gestionado cuantitativamente**

En el nivel de madurez 4, la organización establece objetivos cuantitativos para la calidad y el rendimiento del proceso, y los utilizan como criterios en la gestión. Los objetivos cuantitativos se basan en las necesidades del cliente y la organización. La calidad y el rendimiento del proceso se interpretan en términos estadísticos. (Software Engineering Institute, 2010)

- **Nivel de madurez 5: En optimización**

En el nivel de madurez 5, una organización mejora continuamente sus procesos basándose en una comprensión cuantitativa de sus objetivos de negocio y necesidades de rendimiento. La organización utiliza un enfoque cuantitativo para comprender la variación inherente en el proceso, y las causas de los resultados del proceso. El nivel de madurez 5 se centra en mejorar continuamente el rendimiento de los procesos, mediante mejoras incrementales e innovadoras de proceso y de tecnología. (Software Engineering Institute, 2010)

3.1.4 Agrupación de Indicadores según la escala de madurez

Se ubica dentro de los niveles antes descritos a los indicadores planteados para cada variable, de acuerdo a la criticidad y análisis de cada uno de ellos, junto a una posterior validación del modelo durante la investigación de campo realizada.

Se plantea que para que exista gestión de la seguridad de la información, los procesos dentro de las instituciones deben ser definidos y caracterizados (nivel tres), con el objetivo de tener una línea base para la agrupación de los indicadores. A partir de esta línea base se agrupa a todos los indicadores en tres niveles de madurez (tres, cuatro y cinco), como se muestra a continuación:

- **Agrupación de indicadores en el nivel de madurez tres (definido)**

Los siguientes indicadores fueron agrupados en el nivel de madurez tres, ya que se determinó que los mismos forman parte base para iniciar una gestión de la seguridad de la información. Las características de los mismos permiten situar a las instituciones en un nivel de madurez dentro de la escala de cero a tres; donde cero representa la no existencia del indicador y tres representa que el indicador se encuentra definido y caracterizado.

Tabla 7:

Indicadores nivel de madurez tres

Variable	Madurez Indicado	Inidcadores
Politica de Seguridad	3	Politica de Seguridad
	3	Distribución,Publicación y
	3	Revisión a la Politica
Organización de la seguridad de la información	3	Compromiso de la dirección
	3	Coordinacion y Responsabilidad de la
	3	Acuerdo de Confidencialidad
	3	Identificación de los riesgos y controles
	3	Tratamiento de la Seguridad en
	3	Tratamiento de la Seguridad con los
Gestion de Activos y	3	Reglamentos de Uso de activos
Seguridad en Recursos Humanos	3	Funciones, Reponsabilidades
	3	Investigación de antecedentes
	3	Terminos y Condiciones Contractuales
	3	Capacitación en seguridad de la
	3	Cese del empleo o cambio de puesto de
Seguridad física y ambiental	3	Trabajo en areas seguras
	3	Mantenimiento de equipos
	3	Transporte de los activos de información
Gestion de Comunicaciones y Operaciones	3	Documentacion de procedimientos de
	3	Separación de tareas
	3	Copias de seguridad
	3	Seguridad de los servicios de red
	3	Manipulación de los soportes
Control de Accceso	3	Políticas de Control de Accesos
	3	Responsabilidades de usuario
	3	Separación de redes
	3	Politica de uso Equipos portatiles o
	3	Política de Teletrabajo
Adquisición, desarrollo y mantenimiento de Gestión de Cumplimiento	3	Especificación de requisitos de
	3	Cifrado de contraseñas
	3	Revisión tecnica de aplicaciones tras
	3	Responsabilidad y procedimientos ante
	3	Auditoria de los sistemas de información

- **Agrupación de indicadores en el nivel de madurez cuatro (gestionado).**

Los indicadores que se muestran a continuación fueron agrupados en el nivel de madurez cuatro, debido a que los mismos permiten establecer lineamientos precisos para que las instituciones administren de una forma ordenada la seguridad de la información, basados en datos que permiten medir, controlar procesos y tomar decisiones sobre la calidad de gestión de la seguridad de la información en base a resultados reales. Las características de los mencionados indicadores permiten situar a las instituciones en un nivel de madurez dentro de la escala de cero a

cuatro; donde cero representa la no existencia del indicador y cuatro representa que el indicador es gestionado.

Tabla 8:

Indicadores nivel de madurez cuatro

Variable	Madurez Indicado	Inidcadores
Politica de Seguridad	4	Medicion de Politica de Seguridad
Organización de la seguridad de la información	4	Autorizacion de nuevos recursos para el
	4	Revisión independiente de la seguridad
Gestion de Activos y clasificacion de la informacion	4	Propiedad de los activos
	4	Directriz de clasificacion
Seguridad en Recursos Humanos	4	Proceso disciplinario
Seguridad física y ambiental	4	Areas de acceso publico
	4	Instalaciones de suministro y cableado
	4	Reutilizacion o retiro seguro de equipos
Gestion de Comunicaciones y Operaciones	4	Control de cambios en activos
	4	Separación de recuros
	4	Provisión y supervición de de servicios
	4	Gestion del cambio en los servicios
	4	Protección contra el codigo malicioso y
	4	Intercambio de la información
	4	Uso de servicios de red
Control de Accceso	4	Autentificación de conecciones remotas
	4	Identificación de equipos en redes
	4	Control de Conecciones de redes
	4	Control de acceso y gestión de sistemas
	4	Tratamiento de las aplicaciones
Adquisición, desarrollo y mantenimiento de los sistemas de información	4	Seguridad de los archivos de sistema
	4	Control de cambios en aplicativos
	4	Control de paquetes de software
	4	Control de desarrollo de sistemas
Gestión de incidentes de seguridad	4	Notificación de eventos y puntos debiles
	4	Valoración de incidentes de seguridad
Gestión de la continuidad del negocio	4	Plan de continuidad de negocio
Cumplimiento	4	Cumplimiento de requisitos legales

- **Agrupación de indicadores en el nivel de madurez cinco (optimizado)**

Los siguientes indicadores pertenecen al nivel de madurez cinco, los mismos que permiten a la institución mantener el rendimiento de los procesos en mejora continua, estableciendo una gestión de la calidad de la seguridad de la información incremental e innovadora en los procesos y tecnologías de la información y comunicaciones, asociados a los activos de la institución. Las características de los

presentes indicadores permiten situar a las instituciones en un nivel de madurez dentro de la escala de cero a cinco; donde cero representa la no existencia del indicador y cuatro representa que el indicador es optimizado.

Tabla 9:

Indicadores nivel de madurez cinco

Variable	Madurez Indicado	Inidcadores
Politica de Seguridad	5	Mejora de la Politica de Seguridad
Organización de la seguridad de la	5	Contacto con Autoridades y Grupos de
Gestion de Activos y clasificacion de la	5	Inventario de Activos
Seguridad en Recursos Humanos	5	Responsabilidad de la dirección
Seguridad física y ambiental	5	Perimetros y controles de seguridad
	5	Protección de las áreas criticas de activos
	5	Seguridad de los equipos fuera de la
Gestion de Comunicaciones y Operaciones	5	Gestión de capacidad de los recuros de
	5	Aceptación de sistemas
	5	Controles de red
	5	Supervisión del tratamiento de la
Control de Accceso	5	Gestion de acceso de usuario
	5	Proteccion de puertos de diganóstico y
	5	Encaminamiento (routing) de red
Adquisición, desarrollo y mantenimiento de los sistemas de información	5	Fugas de información
	5	Control de vulnerabilidades
Gestión de incidentes de seguridad	5	Recoplación de evidencias
Gestión de la continuidad del negocio	5	Mantenimiento del plan de continuidad
Cumplimiento	5	Cumplimiento de política y normas de

3.1.5 Cuantificación de indicadores según la escala de madurez

Una vez definido el nivel de madurez para cada indicador, se establece la necesidad de la cuantificación (evaluación) del mismo. Esto se lo realiza tomando como base la guía de buenas prácticas de apoyo a los controles especificadas en la norma NTE INEN ISO/IEC 27002:2009, dicha norma propone un conjunto de actividades para cumplir con los controles establecidos, estas actividades fueron analizadas con el fin de determinar el aporte al nivel de madurez de cada indicador. Durante este análisis se generaron interrogantes junto a un conjunto de respuestas que permiten alcanzar un grado de madurez dependiendo de las respuestas seleccionadas, dichas interrogantes y conjuntos de respuestas se generaron a partir las actividades planteadas, para cumplir cada control en las normas NTE INEN ISO/IEC 27001:2011 y NTE INEN ISO/IEC 27002:2009.

La forma en la que se llevó a cabo la valoración de cada respuesta, se la fijó en base a su aporte al nivel de madurez de cada indicador. Este aporte fue determinado de acuerdo a la importancia que cada una ellas desempeña dentro del indicador.

A continuación se muestra un ejemplo de la cuantificación de un indicador extraído del modelo desarrollado en la presente investigación.

Tabla 10:

Cuantificación Indicador

Variable	Madurez Indicador	Indicador	Interrogantes	Respuestas		Valoración
Política de Seguridad	3	Distribución, Publicación y Conocimiento de la Política	¿Usted recibió la Política de seguridad de la información de la organización?	NO		-
				Si	A través de inducción ☑	0.50
					Físicamente /digitalmente ☑	0.50
			¿Conoce usted la Política de Seguridad?	NO		
				Si	Poco ○	0.50
					Completa ◉	1.00
			¿Se evidencia la publicación de la Política?	NO		
				Si	☑	1.00

Como se puede apreciar la variable seleccionada es la *Política de Seguridad*, el indicador es la *Distribución, Publicación y Conocimiento de la Política*, el mismo que pertenece al nivel tres de madurez. Se muestran tres interrogantes junto a un conjunto de respuestas, las mismas que están valoradas para alcanzar un nivel de madurez en el rango de cero a tres; dicho conjunto de respuestas son de selección múltiple o de selección única, la misma lógica se aplica para todos los indicadores propuestos. El modelo completo se lo puede apreciar en el anexo 1.

3.1.6 Cuantificación del nivel de madurez de la variable

Para cuantificar el nivel de madurez de las once variables propuestas, utilizamos como base los cinco niveles de madurez propuestos por el CMMI Institute, con el fin de desarrollar un rango de cuantificación que permita situar a las variables en el nivel de madurez correspondiente. A continuación se presenta la tabla de rangos utilizada:

Tabla 11:

Rango de niveles de madurez

Rango		Nivel	Descripción
5	5.99	5	Optimizado.
4	4.99	4	Gestionado Cuantitativamente.
3	3.99	3	Definido en procedimientos.
2	2.99	2	Gestionada.
1	1.99	1	Existencia.
0	0.99	0	No existencia.

Como se puede apreciar en la tabla se añadió un nivel de madurez cero, debido a que durante la validación del modelo, se evidenció que en las instituciones ciertos indicadores no alcanzan al nivel uno de existencia propuesto por el CMMI Institute. Con este antecedente se determina que el número de niveles que utiliza la presente metodología es de seis.

La cuantificación de cada variable se la realizó con la siguiente fórmula:

$Nm = 6$ → Niveles de madurez.

$\sum Nmi$→ Sumatoria de la cuantificación de los indicadores pertenecientes a la variable.

$\sum Sio$→ Sumatoria de las respuestas obtenidas por los indicadores pertenecientes a la variable.

$$Nivel\ de\ madurez\ variable = \frac{\sum Sio * Nm}{\sum Nmi}$$

Tras aplicar la fórmula planteada se obtiene un valor, que ubicado en la tabla de rangos se consigue el nivel de madurez de la variable.

3.1.7 Cuantificación del nivel de madurez de la organización

Para cuantificar el nivel de madurez de la organización se utiliza los resultados de los niveles de madurez de las once variables propuestas, junto a una ponderación de aportación de cada variable al nivel de madurez de la organización. A continuación se muestra la ponderación de cada una de las variables:

Tabla 12:

Ponderación Variables

	Variable	Ponderación Variable
1	Política de seguridad	3,60
2	Organización de la seguridad de la información	3,44
3	Gestión de activos y clasificación de la información	4,00
4	Seguridad en recursos humanos	3,43
5	Seguridad física y ambiental	4,00
6	Gestión de comunicaciones y operaciones	3,93
7	Control de acceso	3,85
8	Adquisición, desarrollo y mantenimiento de los sistemas de información	3,90
9	Gestión de incidentes de seguridad	4,00
10	Gestión de la continuidad del negocio	4,50
11	Cumplimiento	4,00

Como se puede apreciar en el cuadro anterior se asigna a las once variables los valores ponderados, los mismos que provienen del promedio del nivel de madurez de sus indicadores.

A continuación se muestra como obtener el valor ponderado de una de las variables.

Tabla 13:

Ejemplo para obtener el valor de ponderación de una variable

Variable	Madurez Indicador	Indicadores
Política de Seguridad	3	Política de Seguridad
	3	Distribución, Publicación y Conocimiento de la Política
	3	Revisión a la Política
	4	Medición de la Política de Seguridad
	5	Mejora de la Política de Seguridad
Promedio **Ponderación variable**	3,60 **3,60**	

El objetivo es obtener el nivel de aportación de cada variable al nivel de madurez de la organización. Una vez determinados estos valores para cada variable, se aplica un promedio ponderado entre el resultado de madurez de cada variable y su ponderación respectiva; como resultado se obtiene el nivel de madurez de la organización en base a la aportación de cada una de sus variables.

3.1.8 Técnicas y herramientas

Para la presente investigación se utilizó como técnica la entrevista en las distintas áreas involucradas en la gestión de seguridad en las instituciones, para lo cual se tomó el modelo basado en la metodología anteriormente descrita, que permite evaluar el nivel de madurez de las once variables planteadas. Esta evaluación se la realizó mediante dos instrumentos: guía de entrevista y guía de observación, las mismas que agrupan a todas las interrogantes y conjuntos de respuestas para realizar el levantamiento de los datos de una manera eficiente en las organizaciones. Dichas guías se las puede apreciar en el anexo 2.

3.1.9 Fuentes de información

Se identifican como fuentes de información a diferentes funcionarios dentro de los departamentos en las instituciones públicas, con el objetivo de relacionar las once variables establecidas en la presente metodología, dicho relacionamiento busca direccionar de forma exacta el levantamiento de los datos necesarios en los distintos departamentos o unidades organizacionales responsables de la información. A continuación se muestra la relación variable/departamento.

Tabla 14:

Cruce de variables con las unidades organizacionales

N°	Variable	Departamentos o Unidades Organizacionales				
		Planificación	**TIC**	**Recursos Humanos**	**Legal**	**Administrativa -Logística**
1	Política de seguridad	**X**		**X**		
2	Organización de la seguridad de la información	**X**	**X**	**X**	**X**	
3	Gestión de activos y clasificación de la información	**X**				**X**
4	Seguridad en recursos humanos	**X**		**X**	**X**	
5	Seguridad física y ambiental		**X**			**X**
6	Gestión de comunicaciones y operaciones		**X**			
7	Control de acceso	**X**	**X**	**X**		
8	Adquisición, desarrollo y mantenimiento de los sistemas de información	**X**	**X**			

Tabla 14:

(Continuación)

N°	Variable	Departamentos o Unidades Organizacionales				
		Planificación	**TIC**	**Recursos Humanos**	**Legal**	**Administrativa -Logística**
9	Gestión de incidentes de seguridad de la información		**X**			
10	Gestión de la continuidad del negocio	**X**				
11	Cumplimiento	**X**			**X**	

Como se puede apreciar en la tabla anterior, se identificaron cinco departamentos que son los responsables de los procesos que gestionan la seguridad de la información y por ende la calidad de la misma.

4. APLICACIÓN DE LA METODOLOGÍA

Propuesta la metodología en el capítulo anterior, nos enfocamos en ubicar instituciones del sector público que permitan levantar la información necesaria para validar la metodología planteada y determinar el grado con la cual es gestionada la seguridad de la información con respecto a la norma NTE INEN ISO/IEC 27001:2011.

Debido a la criticidad de la información solicitada, fueron pocas las instituciones del sector público que dieron apertura para este análisis, llegándose a ejecutar la investigación de campo en tres instituciones del sector público, que tienen un alcance a nivel nacional.

El proceso formal que se siguió con las tres instituciones públicas anteriormente mencionadas, inició con una carta enviada por parte de la Pontificia Universidad Católica del Ecuador, dirigida a los directivos de cada institución, en donde se explica el motivo de la investigación, el alcance de la misma y la solicitud para realizar la investigación de campo. Con dos instituciones públicas se firmaron un acuerdo de confidencialidad, para asegurar que la información entregada al investigador, va a ser utilizada exclusivamente para la investigación en curso y con fines académicos, adicionalmente por la criticidad de la información obtenida y por los posibles resultados de la calidad de gestión de la seguridad de la información que se obtengan durante la presente investigación, los nombres de las instituciones, directivos encargados y datos organizacionales, no serán revelados para proteger la confidencialidad de las instituciones, así como la seguridad de las mismas, para ello estas serán identificadas como Caso uno, Caso dos y Caso tres.

Como aporte a las instituciones públicas evaluadas los resultados obtenidos, así como las conclusiones y recomendaciones generales emitidas en base a los mismos, van a ser entregados a cada una de ellas para su análisis y de ser el caso para fines de mejoramiento.

En las tres instituciones públicas seleccionadas para la presente investigación, se ejecuta y la metodología desarrollada, con el objetivo de obtener el nivel de madurez con respecto a la calidad de gestión de la seguridad de la información basado en la norma NTE INEN

ISO/IEC 27001:2011, los resultados y comparativas de las diferentes variables se analizan en la modalidad de casos.

4.1 Investigación de campo

A continuación se detallan las fases seguidas para ejecutar la investigación de campo, con el objetivo de aplicar la metodología desarrollada en el capítulo anterior.

4.1.1 Contacto con las instituciones

El primer paso fue establecer contacto con instituciones del sector público de la ciudad de Quito, específicamente con los departamentos encargados de gestionar la seguridad de la información. Para esto se establecieron una serie de reuniones en las cuales se exponía la presente investigación y la necesidad de obtener datos de las instituciones. Debido a la criticidad de los datos a solicitar se pidió al investigador seguir un proceso formal para la aprobación por parte de los directivos, obteniendo la autorización en tres de ellas. Cabe mencionar que las aprobaciones fueron dadas gracias a que se mantenía una relación directa con los directivos de las instituciones y en las otras instituciones se dieron largas y no se autorizó la investigación.

4.1.2 Exposición y aceptación del modelo

Una vez que se obtuvieron las autorizaciones necesarias con las instituciones, se planificó una reunión con los Oficiales de Seguridad de la Información de cada una de ellas, dichos oficiales son los responsables de planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones con el fin de mejorar la seguridad de la información, siendo su objetivo fundamental mantener la confidencialidad, integridad y disponibilidad de la información, por tanto ellos son los encargados de conducir junto al investigador la ejecución de la investigación de campo. En las reuniones planificadas con cada Oficial de Seguridad de la Información se expone la metodología planteada en la presente investigación, en donde los tres funcionarios tuvieron una duda en común antes de aceptar la metodología:

¿Qué diferencia hay con el modelo planteado VS un análisis GAP (brechas)?

Para responder está interrogante partimos del concepto de un análisis GAP o de brechas, el cual se basa en comparar el estado de la situación actual y el estado esperado o ideal, en este caso el estado esperado para las instituciones públicas es completar la implementación del EGSI en los plazos estipulados, por lo tanto el resultado de un análisis GAP es un índice de cumplimiento. En cambio el objetivo de la presente metodología es determinar la calidad de la gestión de la seguridad de la información a través de índices que ubican en niveles de madurez a cada una de las once variables definidas, siendo el resultado de la metodología planteada, la determinación del nivel madurez organizacional en referencia a la gestión de la seguridad de la información.

Una vez que los Oficiales de Seguridad de Información estuvieron de acuerdo con la metodología planteada, se planificaron reuniones con los funcionarios encargados de entregar la información al investigador.

4.1.3 Ejecución de la metodología

La investigación de campo en las instituciones tomó alrededor de 3 días laborables en cada uno de ellas, en periodos de tiempos distintos ya que se dependía de la disponibilidad de los horarios de los funcionarios públicos. Durante la investigación de campo el 90% de la información se obtuvo del Departamento de Planificación y del Departamento de Tecnologías de la Información y Comunicaciones (TIC). La ejecución de la metodología en un inicio se ejecuta en un ambiente en donde los responsables de entregar la información sienten que es una auditoria externa de cumplimiento e inmediatamente intentan justificar sus acciones con documentos y/o registros de descargo, sin embargo que se les explica que no es necesario disponer de estas pruebas de descargo argumentando el investigador que es una investigación del tipo cualitativa, en donde se intenta conocer la calidad de gestión de la seguridad de la información a través de acciones cotidianas. A partir de este punto la recolección de datos con cada funcionario se vuelve dinámica, incluso llegando los

funcionarios a sugerir mejoras o cambios al modelo que estaba siendo ejecutado y tomando nota de potenciales buenas practicas.

Una vez realizada la investigación de campo, se determinó que la valoración planteada a cada indicador correspondía a la realidad medida, puesto que la cuantificación de la importancia de los indicadores que aportan a la variables en el modelo planteado fueron definidos en base a los controles que la norma NTE INEN –ISO/IEC 27001:2011 solicita para gestionar de manera adecuada la seguridad de la información.

4.1.4 Entrega de resultados

Los resultados obtenidos fueron presentados a las instituciones públicas para su correspondiente análisis, siendo el objetivo obtener una retroalimentación con respecto a la información entregada. En las reuniones mantenidas se analizaron los resultados junto al oficial de seguridad de la información y se determina que el resultado obtenido corresponde a la realidad respecto a la gestión de seguridad de la información, validando de esta manera el modelo planteado por la presente investigación. Adicionalmente se advierte que en dos de las tres instituciones objeto de la presente investigación el estado implementación y gestión de la norma NTE INEN –ISO/IEC 27001:2011, se aplican a todos los procesos relacionados con la seguridad de la información en la institución, y en la otra institución solo aplican la implementación de la norma en procesos críticos previamente determinados. Esto se debe a que las primeras instituciones se encuentran normadas por la Secretaria de Administración Publica, la misma que tiene plazos y alcances establecidos para la implementación de la norma a nivel de todas las instituciones públicas dependientes del gobierno central. La institución restante aun siendo publica no es dependiente del gobierno central, por tanto implementa la norma de forma proactiva debido y en base a la criticidad de la información que administra.

4.2 Caso Uno

En el presente caso se analiza a una empresa pública de dependencia municipal encargada de la gestión y suministro de servicios básicos en el Distrito Metropolitano de la Ciudad de Quito, la empresa municipal fue creada en al año de 1960 y en la actualidad tiene una penetración del 98.2% del servicio ofrecido en la población del distrito metropolitano, y es un referente en la gestión y calidad del servicio a nivel nacional. Está conformado por más de 2000 servidores municipales públicos y dispone de un sistema integrado de gestión que incluye Calidad, Ambiente, Seguridad y Salud Ocupacional.

En diciembre del 2013 de forma proactiva esta institución toma la decisión de iniciar el proceso de implementación de la norma NTE INEN ISO/IEC 27001:2011´, la cual gestionara la seguridad de la información. Para junio del 2014, la alta dirección de la empresa aprueba y publica la política de seguridad de la información, comprometiéndose a asignar los recursos administrativos y económicos necesarios para la aplicación de la misma. A la fecha de inicio de la presente investigación ya existe un sin número de controles y avances en la implementación de la norma, por lo que el objetivo será conocer cuan madura es la organización en relación a la gestión de la seguridad de la información, para lo cual se analiza los resultados de las once variables propuestas por la metodología.

Se planificaron reuniones con las personas encargadas de cada departamento en la oficina matriz ubicada en Quito, para el levantamiento de los datos de acuerdo a la metodología establecida, esta investigación tomo 3 días laborables, en periodos de tiempos distintos, ya que dependíamos de la disponibilidad de horarios de los servidores municipales públicos.

4.2.1 Variable 1: Política de seguridad

Los resultados obtenidos respecto a la política de seguridad se muestran a continuación:

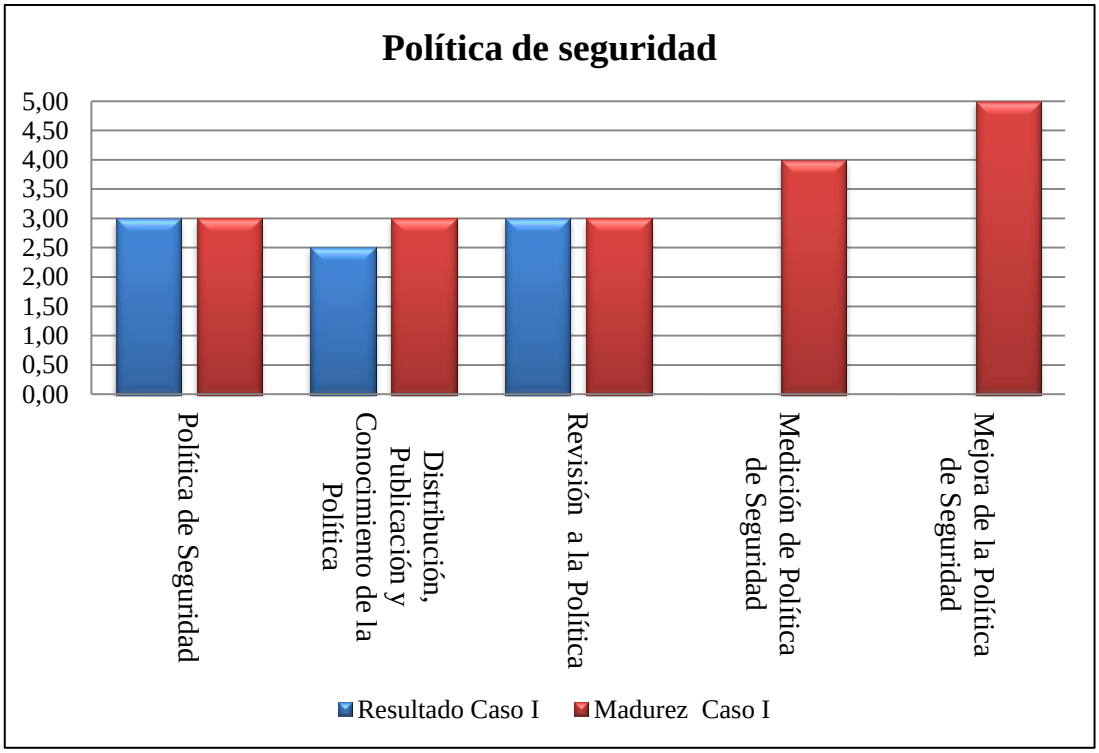

Figura 27: Política de seguridad - Caso 1.

- ✓ **Política de seguridad (3/3):** De acuerdo a la madurez propuesta para cada indicador, los resultados obtenidos nos indican que la institución dispone de una política de seguridad de la información documentada, situándola en el punto óptimo de escala de madurez.

- ✓ **Distribución, publicación y conocimiento de la política (2,5/3):** Se pudo evidenciar que la misma está siendo distribuida y publicada, sin embargo los funcionarios de la institución no disponen de un conocimiento completo.

- ✓ **Revisión de la política (3/3):** La institución se encuentra realizando revisiones de forma proactiva y planificada a la política de seguridad de la información, con el objetivo de ajustar nuevas normativas que permitan gestionar la seguridad de la

información en toda la institución durante el proceso de implementación que se está ejecutando.

- ✓ **Medición de la política (0/4) y mejora de la política de seguridad (0/4):** Durante la investigación de campo se determinó que la institución no dispone de indicadores de gestión de la política de seguridad de la información, ni tampoco que exista planes de mejora de la misma, esto se debe a que la implementación de la norma se encuentra en proceso.

- ✓ **Estado de madurez de la variable política de seguridad:** El estado de madurez obtenida en esta variable es de 2,83 que la sitúa dentro de la escala de madurez en el nivel dos, lo cual indica que está siendo *Gestionada.*

4.2.2 Variable 2: Organización de la seguridad de la información

Los resultados obtenidos respecto a la organización de la seguridad de la información se muestran a continuación:

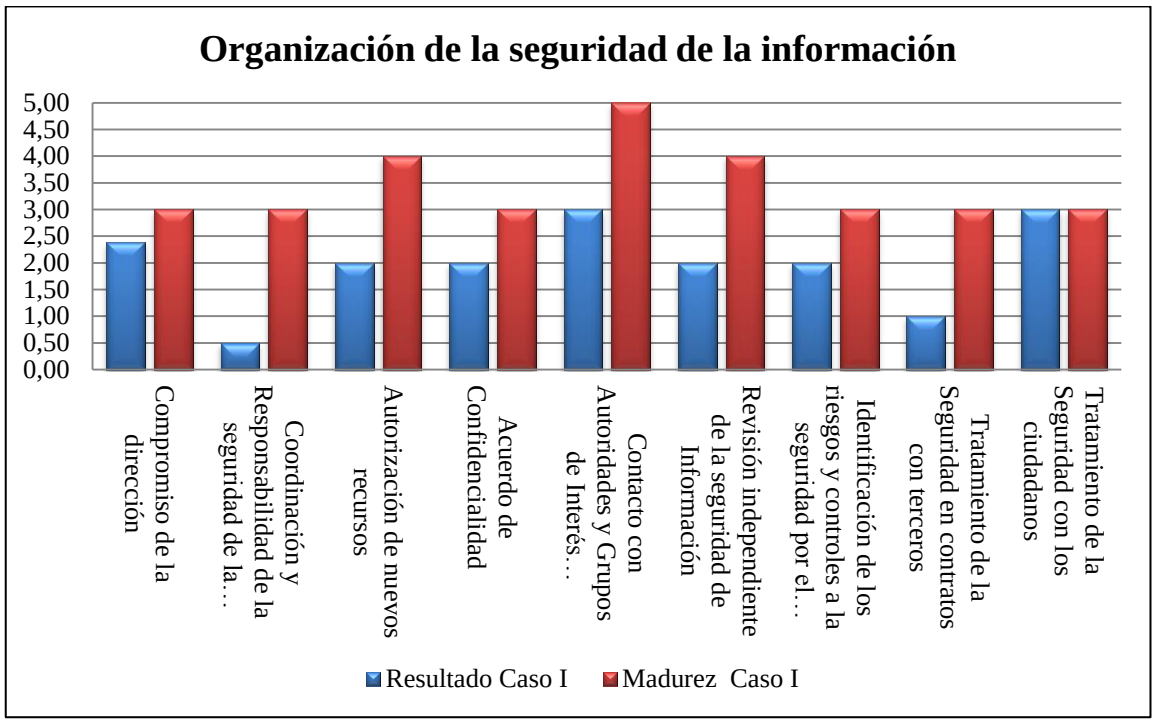

Figura 28: Organización de la seguridad de la información - Caso 1.

- ✓ **Compromiso de la dirección (2,5/3):** Como se puede apreciar existe un compromiso por parte de la dirección a través de acuerdos formales y asignación de recursos, sin embargo no llega a su tope óptimo, ya que las responsabilidades referentes a la seguridad de la información se encuentran en un proceso de definición.

- ✓ **Coordinación y responsabilidad de la seguridad de la información (0,5/3):** Ya que la asignación de responsabilidades se encuentran en un proceso de definición, es evidente que la coordinación de las actividades referentes a la seguridad de la información entre los diferentes departamentos se encuentra en un nivel de madurez bajo.

- ✓ **Autorización de nuevos recursos (2/4):** La institución dispone de un procedimiento para autorizar el uso de nuevos recursos de tratamiento de la información, sin embargo el mismo se encuentra siendo implementado, por lo que su nivel de madurez no es el óptimo.

- ✓ **Acuerdos de confidencialidad (2/3):** La institución dispone de acuerdos de confidencialidad con todos los actores involucrados, los cuales no han sido revisados desde su firma.

- ✓ **Contacto con autoridades y grupos de interés especializados (2/4):** La institución mantiene contacto con profesionales o entidades especializadas en el área de seguridad de la información, sin embargo la institución no mantiene contacto con autoridades competentes para tratar temas relacionados con la seguridad de la información.

- ✓ **Revisión independiente de la seguridad de información (2/4):** Debido a que la implementación de la norma se encuentra en marcha, sólo se han realizado auditorias de seguridad externas a los procesos críticos que afectan a la seguridad de la información.

- ✓ **Identificación de los riesgos y controles a la seguridad por el acceso de terceros (2/3):** La institución ha identificado los riesgos provenientes por el acceso a la información por parte de terceros, para lo cual ha implementado controles de acceso lógico a la información, sin embargo no dispone de controles de acceso a los dispositivos que utilizan terceros para acceder a la información.

- ✓ **Tratamiento de la seguridad en contratos con terceros (1/3):** Las cláusulas contractuales de confidencialidad se incluyen dentro de los contratos con terceros, sin embargo no se toma en cuenta cláusulas sobre la disponibilidad e integridad de la información que pueda ser afectada.

- ✓ **Tratamiento de la seguridad con los ciudadanos (3/3):** Se evidencia que la institución identifica a los ciudadanos y define los perfiles de acceso a la información, por lo que logra un nivel óptimo en la aportación a la madurez de la variable.

- ✓ **Estado de madurez de la variable - organización de la seguridad de la información:** El estado de madurez obtenida en esta variable es de 3,46 que la sitúa dentro de la escala de madurez en el nivel tres, lo cual indica que dispone de procesos *Definidos.*

4.2.3 Variable 3: Gestión de activos y clasificación de la información

Los resultados obtenidos respecto a la gestión de los activos y la clasificación de la información se muestran a continuación:

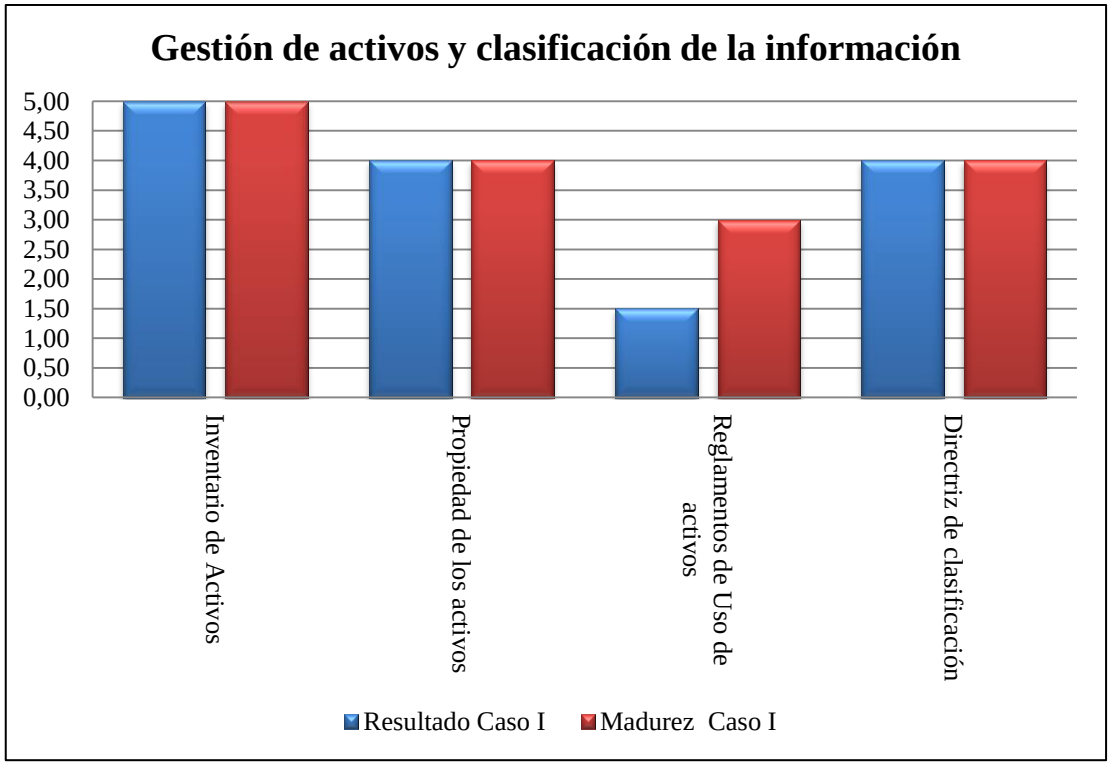

Figura 29: Gestión de activos y clasificación de la información – Caso 1.

- ✓ **Inventario de activos (5/5) - Propiedad de los activos (4/4) - reglamento de uso de activos (1,5/3):** Como se puede apreciar en la institución se mantiene un control óptimo sobre el inventario de los activos, están claramente definidas las propiedad de cada uno de ellos, sin embargo los reglamentos del uso de dichos activos se encuentran documentados y en proceso de sociabilización.

- ✓ **Directriz de clasificación (4/4):** Se puede evidenciar que la institución dispone de directrices de clasificación de la información definida e implementada.

- ✓ **Estado de madurez de la variable - gestión de activos y clasificación de la información:** El estado de madurez obtenida en esta variable es de 5,44 que la sitúa dentro de la escala de madurez en el nivel cinco, lo cual indica que dispone de procesos en *Optimización.*

4.2.4 Variable 4: Seguridad en recursos humanos

Los resultados obtenidos respecto a la seguridad en recursos humanos se muestran a continuación:

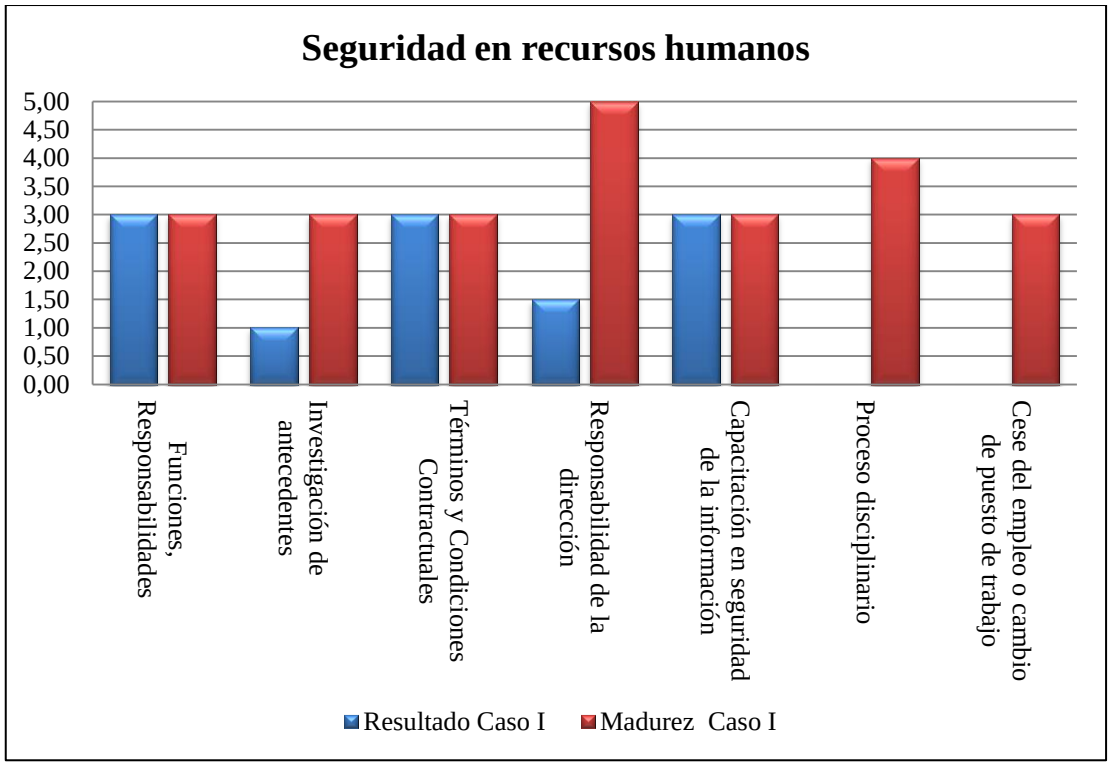

Figura 30: Seguridad en recursos humanos - Caso 1.

.

- ✓ **Funciones y responsabilidades (3/3) – investigación de antecedentes (1/3):** Como se puede apreciar la institución mantiene definidas las funciones y responsabilidades previas al empleo de un actor, sin embargo se denota una falta de investigación de los antecedentes previo al empleo, la institución solo verifica los antecedentes laborales y no está tomando en cuenta antecedentes penales y conductuales.

- ✓ **Términos y condiciones contractuales (3/3):** Referente a los términos y condiciones contractuales con los actores involucrados, se puede determinar que la institución está incluyendo cláusulas que precautelan la confidencialidad, integridad y disponibilidad de la información que manejarán los actores.

- ✓ **Responsabilidad de la dirección (1,50/5):** Al estar la institución en un proceso de implementación de la norma, el sistema de gestión de seguridad no dispone de suficientes indicadores para que la dirección pueda tomar decisiones o acciones de mejora, al momento la dirección sólo dispone de informes generales del cumplimiento de políticas y procedimientos.

- ✓ **Capacitación en seguridad de la información (3/3):** La institución al momento está en el punto más alto referente a la capacitación de los actores involucrados en temas relacionados con la seguridad de la información, siendo esta periódica y constante.

- ✓ **Proceso disciplinario (0/4):** El departamento de recursos humanos informó que no tiene definido un proceso disciplinario, en el caso de que uno de sus actores provoque un evento de seguridad.

- ✓ **Cese de empleo o cambio de puesto de trabajo (0/4):** El departamento de recursos humanos también informó que no dispone de un procedimiento formal para cuando uno de los funcionarios cese o cambie de puestos de trabajo, es decir, dicho procedimiento carece de responsables para recibir las funciones de los funcionarios salientes, y la devolución de los activos se la realiza de manera verbal.

- ✓ **Estado de madurez de la variable seguridad en recursos humanos:** El estado de madurez obtenida en esta variable es de 2,88 que la sitúa dentro de la escala de madurez en el nivel dos, lo cual indica que dispone de procesos *Definidos.*

4.2.5 Variable 5: Seguridad física y ambiental

Los resultados obtenidos respecto a la seguridad física y ambiental se muestran a continuación:

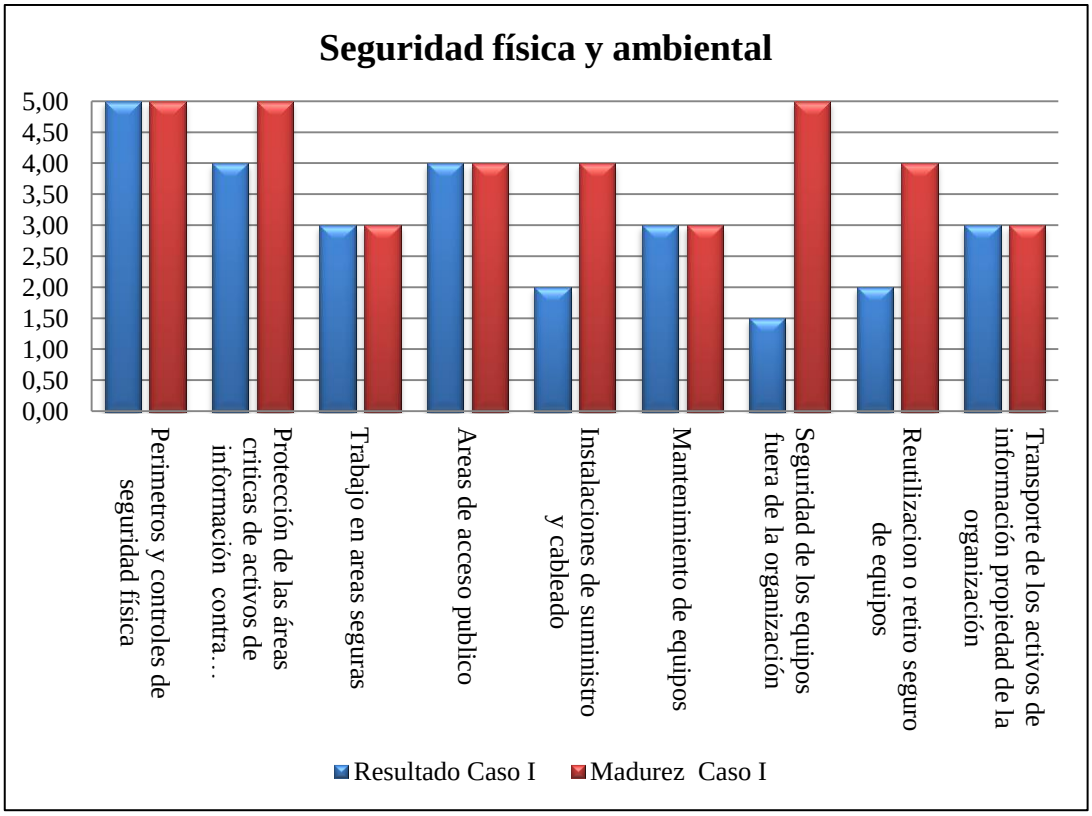

Figura 31: Seguridad física y ambiental - Caso 1.

- ✓ **Perímetros y controles de seguridad física (5/5):** Como se puede apreciar en el gráfico, en la institución se mantiene un control óptimo de los perímetros de las instalaciones así como controles de seguridad física de las instalaciones.

- ✓ **Protección de las áreas críticas de activos de información contra amenazas externas y de origen ambiental (4/5):** Con respecto a la protección de las áreas críticas de tratamiento de la información, estas cuentan con los controles necesarios para asegurar la información, sin embargo se pudo evidenciar que en dichas áreas críticas no disponen de sensores anti-shock para precautelar la integridad de la información en caso de movimientos telúricos.

- ✓ **Trabajo en áreas seguras (3/3):** El trabajo en áreas seguras esta normado por un documento de política de seguridad industrial, el mismo que se encuentra implementado para proteger a las personas y zonas críticas (área de servidores) de posibles incidentes de seguridad.

- ✓ **Áreas de acceso público (4/4):** Se puede evidenciar que desde las áreas de acceso público hacia las privadas de la institución, se encuentran debidamente protegidas por sistemas de seguridad (puestos de vigilancia, controles de acceso físicos y lógicos) implementados para el efecto.

- ✓ **Instalaciones de suministro y cableado (2/4):** La institución dispone de una fuente alterna de energía, en caso de fallas de la misma asegura la disponibilidad de la información, sin embargo cuenta con cableado estructurado que no ha recibido el mantenimiento debido de acuerdo a los cambios físicos realizados en la institución, por lo que podría permitir fallas en la seguridad de la información. Dicha condición no permite al indicador llegar a un nivel óptimo.

- ✓ **Mantenimiento de equipos (3/3):** Como se aprecia en el grafico la institución cuenta con un plan preventivo para los equipos, el mismo que siendo llevado de una forma proactiva permite llegar al nivel óptimo de madurez de este indicador.

- ✓ **Seguridad de los equipos fuera de la organización (1,5/5):** En la seguridad física de los equipos fuera de las áreas seguras de la institución, se evidencia que se los protegen por medio de contraseñas, sin embargo no se utiliza encriptación de datos para proteger la confidencialidad de los mismos, y también si los equipos son robados no disponen de un proceso de trazabilidad que permita recuperar o ubicar los equipos.

- ✓ **Reutilización o retiro seguro de equipos (2/4):** Con respecto a la reutilización o retiro seguro de equipos, en este indicador se mide la forma en la que se destruye los datos de equipos que van a ser reutilizados. Se verificó que la institución realiza este proceso con técnicas estándar y no con técnicas seguras, esto podría permitir la recuperación indeseada de datos afectando la confidencialidad de los mismos, por lo cual se obtiene un nivel de madurez medio.

- ✓ **Transporte de los activos de información propiedad de la organización (3/3):** La institución dispone de un proceso claramente definido e implementando para el transporte de los activos de la información propiedad de la institución.

- ✓ **Estado de madurez de la variable seguridad física y ambiental:** El estado de madurez obtenida en esta variable es de 4,58 que la sitúa dentro de la escala de madurez nivel cuatro, lo cual indica que dispone de procesos *Gestionados Cuantitativamente.*

4.2.6 Variable 6: Gestión de comunicaciones y operaciones

Los resultados obtenidos respecto a la gestión de comunicaciones y operaciones se muestran a continuación:

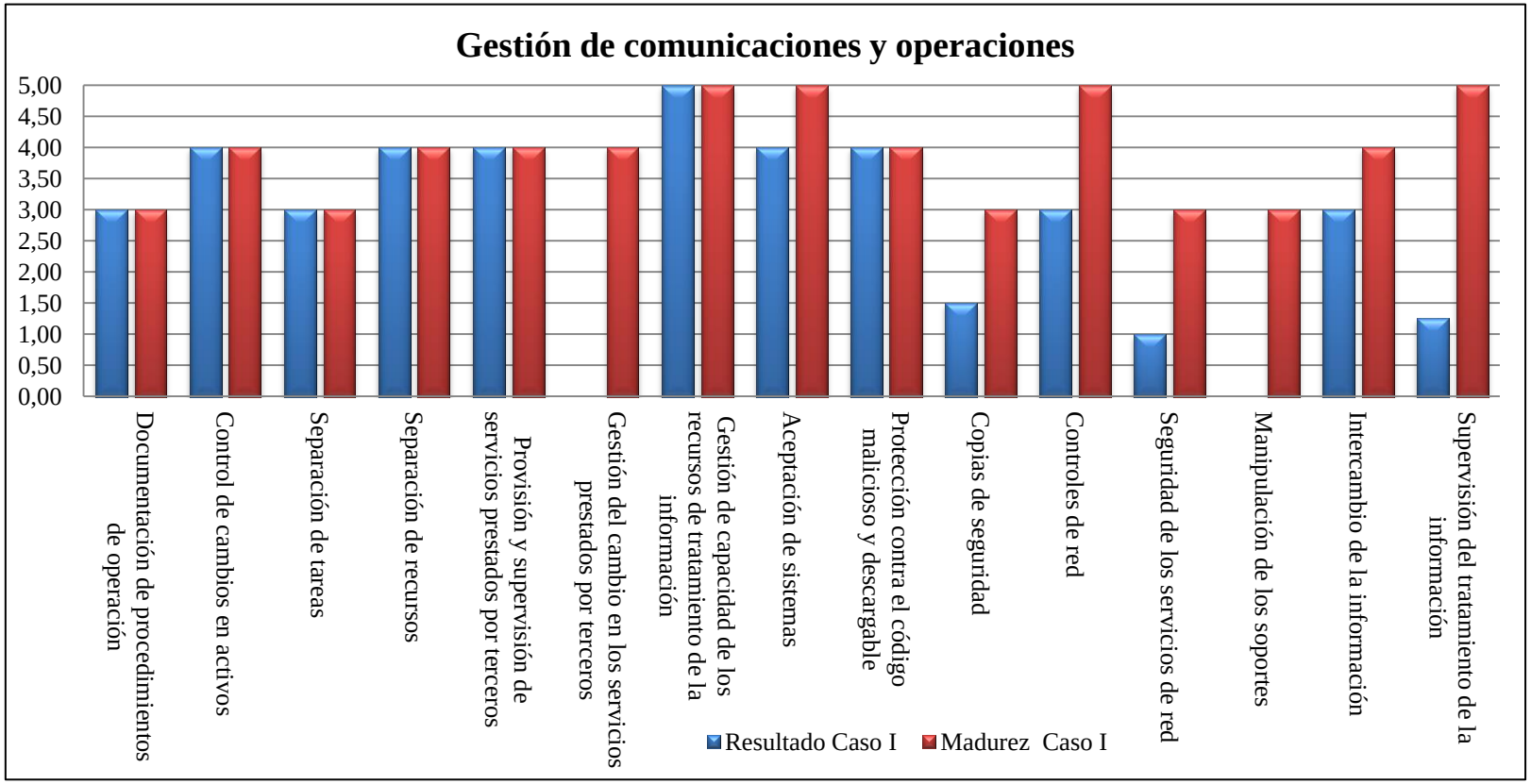

Figura 32: Gestión de comunicaciones y operaciones - Caso 1.

- ✓ **Documentación de procedimientos de operación (3/3):** Como se puede apreciar la institución mantiene de manera documentada los manuales de operación de los distintos sistemas de información, dichos manuales se encuentran a disposición de los usuarios y se los mantienen actualizados.

- ✓ **Control de cambios en activos (4/4):** Cualquier cambio realizado sobre los activos de información, responden a un procedimiento formal en el cual dichos cambios son documentados y se lleva un registro de versionamiento sobre los mismos.

- ✓ **Separación de tareas (3/3):** Dentro de la institución se tienen claramente identificadas las tareas y responsabilidades para el tratamiento de la información, dichas responsabilidades recaen sobre funcionarios como el administrador de base de datos, el administrador de infraestructura, el jefe del área de desarrollo, etc.

- ✓ **Separación de recursos (4/4):** Dentro del departamento que maneja la infraestructura de la institución, se pudo evidenciar que los recursos de tratamiento de la información se encuentran separados en diferentes ambientes, los mismos que son: producción, desarrollo, pruebas y capacitación.

- ✓ **Provisión y supervisión de servicios prestados por terceros (4/4):** La institución cuando adquiere servicios prestados por terceros, dispone de un procedimiento para validar periódicamente que dichos servicios cumplen con las expectativas requeridas, en este procedimiento se encuentran acuerdos de calidad de servicios, auditoras planificadas, etc.

- ✓ **Gestión del cambio en los servicios prestados por terceros (0/4):** Un punto desfavorable durante la gestión de los servicios prestados por terceros, es que si existe algún cambio en la provisión del servicio y el mismo es aceptado por la institución, no consta ningún procedimiento para verificar si dicho cambio afecta a la política o controles de seguridad de la información, debido a la inexistencia de la gestión el indicador es nulo.

- ✓ **Gestión de capacidad de los recursos de tratamiento de la información (5/5):** La institución dispone de una planificación anual en donde se proyecta los futuros incrementos de recursos para el tratamiento de la información, permitiendo así garantizar el rendimiento requerido por los sistemas de información.

- ✓ **Aceptación de sistemas (4/5):** El procedimiento de aceptación de nuevos sistemas de información o modificaciones a los existentes realizados por terceros, se los realiza a través de los Términos y Referencias (TDR) del proyecto, adicionalmente este procedimiento incluye fases de pruebas durante el desarrollo o modificación de los sistemas y una fase adicional de pruebas previas a la aceptación de los nuevos sistemas de información. La debilidad encontrada en este procedimiento es que los temas relacionados con la actualización o mejoras futuras de dichos sistemas, no están siendo contemplados, razón por la cual el indicador no llega a su punto óptimo.

- ✓ **Protección contra el código malicioso y descargable (4/4):** La protección para las terminales de los usuarios en la institución está siendo gestionada de manera correcta, ya que disponen de un sistema del tipo EndPoint, que controla todo lo relacionado con virus, malware, y spam. Los usuarios están en constante capacitación para reconocer y evitar riesgos provenientes del internet. Por otro lado, los usuarios de los terminales tienen una estricta restricción que nos les permite instalar o ejecutar software no autorizado.

- ✓ **Copias de seguridad (1,5/3):** El departamento encargado del área de infraestructura supo indicar que disponen de un procedimiento formal para realizar copias de seguridad de la información, sin embargo el procedimiento para probar si dichas copias de seguridad son cien por ciento funcionales, se encuentra en proceso de desarrollo, por lo que el indicador no llega a su punto óptimo.

- ✓ **Controles de red (3/5):** Las redes de comunicaciones en la institución se encuentran gestionadas por el administrador de red, con la ayuda de hardware especializado para el control de la misma, sin embargo una tarea importante como el monitoreo del tráfico de la red no está siendo implementado dentro de la gestión, por tanto el indicador no llega a su punto óptimo.

- ✓ **Seguridad de los servicios de red (1/3):** Los servicios de red tales como telefonía ip, correo electrónico, sistemas de información, etc., que expone la institución a los actores involucrados, se encuentran identificados y documentados, sin embargo los requisitos relacionados a la seguridad de cada servicio no se encuentran identificados ni documentados, razón por la cual el indicador no llega su punto óptimo.

- ✓ **Manipulación de los soportes (0/3):** La institución se encuentra desarrollando los mecanismos para gestionar la manipulación de soportes de almacenamiento en todas las terminales de usuario, al momento los usuarios pueden insertar memorias flash, cdrom, etc., sin ninguna restricción, por tanto la evaluación del indicador es nula.

- ✓ **Intercambio de la información (3/4):** La institución dispone de procedimientos formales para entregar o intercambiar información con los actores involucrados, dicho procedimiento incluye formularios de solicitud de información y uso de protocolos seguros para el intercambio electrónico (mail) de la información. La causa por la cual el indicador no llega a su punto óptimo, es porque durante el transporte de la información sea física o lógica, no se utilizan medidas de encriptación para protegerla.

- ✓ **Supervisión del tratamiento de la información (1,25/5):** La supervisión del tratamiento de la información, se encuentra realizada en forma parcial, existiendo algunas deficiencias que se encuentran en proceso de implementación, las actividades que actualmente realiza la institución son: registrar las actividades que los usuarios realizan con la información y mantener un histórico de las mismas. La principal deficiencia es que dichos registros no están siendo auditados ni supervisados, razón por la cual el indicador no llega a su punto óptimo.

- ✓ **Estado de madurez de la variable gestión de comunicaciones y operaciones:** El estado de madurez obtenida en esta variable es de 4,14 que la sitúa dentro de la escala de madurez en el nivel cuatro, lo cual indica que dispone de procesos *Gestionados Cuantitativamente.*

4.2.7 Variable 7: Control de accesos

Los resultados obtenidos respecto a los controles de acceso se muestran a continuación:

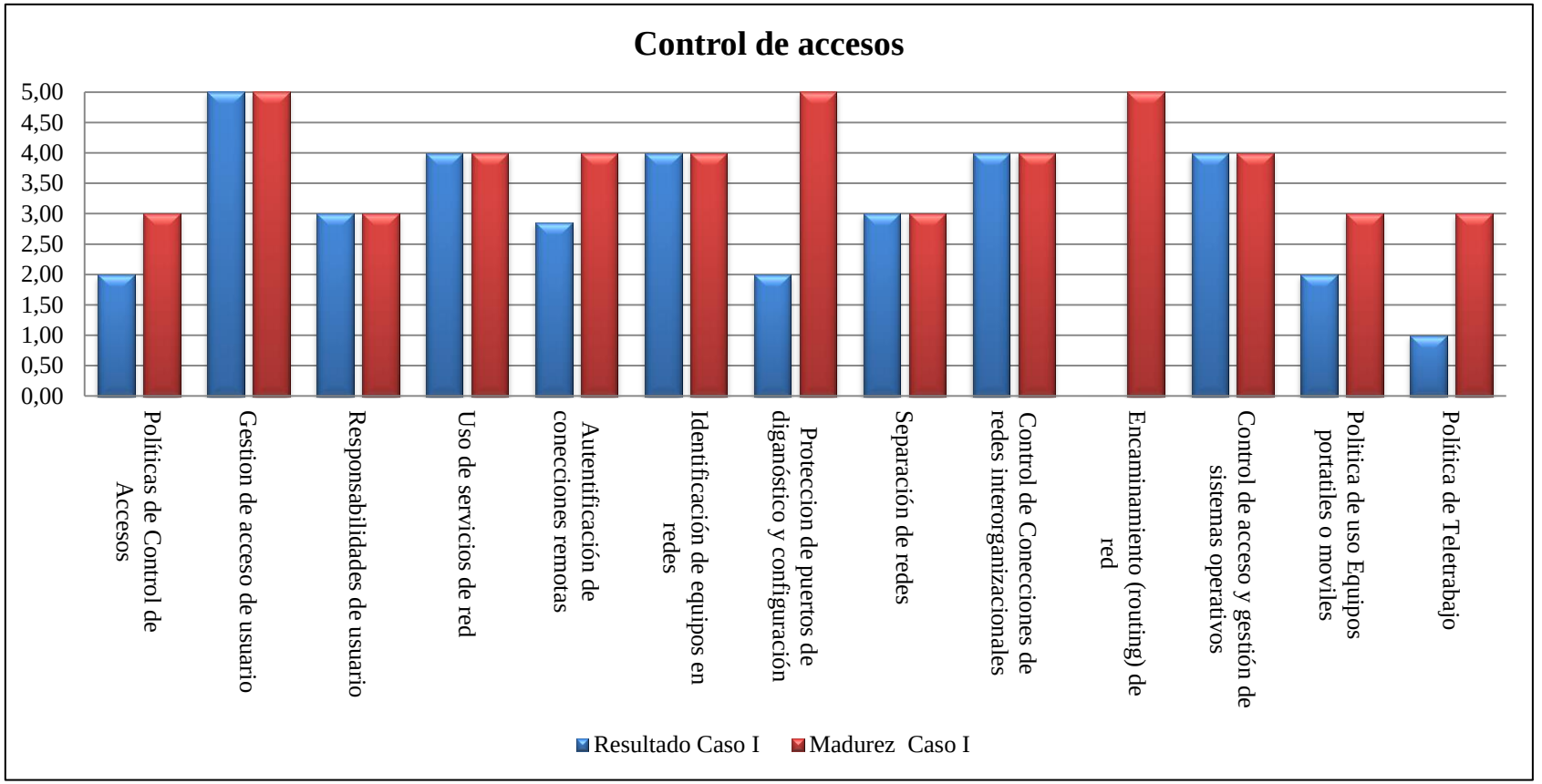

Figura 33: Control de accesos - Caso 1.

- ✓ **Políticas de control de accesos (2/3):** La institución está desarrollando una política formal de control de accesos para normar los mismos, la falta de un documento formal de política, no le permite llegar a un nivel óptimo al indicador.

- ✓ **Gestión de acceso de usuario (5/5):** Como se aprecia en el gráfico la institución mantiene gestionado e implementado todos los objetivos de control solicitados por la norma NTE/ISO-27001:2011, para prevenir el acceso no autorizado a los sistemas de información.

- ✓ **Responsabilidades de usuario (3/3):** Se determina que las responsabilidades de los usuarios con respecto a la seguridad referente al acceso a la información, están siendo cumplidas a cabalidad, las mismas fueron corroboradas con técnicas de observación que permiten situar a este indicador en el nivel óptimo.

- ✓ **Uso de servicios de red (4/4):** Se verifica que en el uso de los servicios de red, la institución dispone de reglas que norman el acceso a los servicios autorizados a los usuarios, con este control y gestión se sitúa el indicador en un nivel óptimo.

- ✓ **Autentificación de conexiones remotas (2,86/4):** Se determinó que la institución cuenta con métodos seguros de autentificación de conexiones remotas (conexiones seguras remotas VPN, envío/recepción de correos smtps/pop3s, administración de dispositivos ssh, encriptación wpa2 en conexiones inalámbricas), sin embargo existen aspectos desatendidos que podrían comprometer la confidencialidad, integridad y disponibilidad de la información (Uso de HTTPS para aplicativos, Transferencia de archivos por FTPS).

- ✓ **Identificación de equipos en redes (4/4):** La institución tiene claramente definido el proceso de autentificación de los equipos en las distintas redes a las que los usuarios tienen acceso, así como su segmentación de acuerdo a la criticidad o a la actividad realizada.

- ✓ **Protección de puertos de diagnóstico y configuración (2/5):** Se dispone de un inventario de puertos de diagnóstico y configuración, sin embargo no existen controles para dar un seguimiento a los mismos.

- ✓ **Separación de redes (3/3):** La institución dispone de un proceso claro y definido para la separación de las redes (vlans) por grupos de servicios o usuarios.

- ✓ **Control de conexiones de redes inter-organizacionales (4/4):** También disponen de un proceso definido para restringir a los usuarios el acceso a las conexiones a redes entre organizaciones interministeriales, reflejando un control claro en este aspecto.

- ✓ **Encaminamiento (routing) de red (0/5):** Con respecto a las rutas de encaminamiento (tracert o routing) que siguen los flujos de información en la organización, no se dispone de un proceso para el control del mismo, por lo que el indicador refleja un nivel inexistente de control.

- ✓ **Control de acceso y gestión de sistemas operativos (4/4):** La institución cuenta con una solución integral (tipo Active Directory o LDAP) que abarca la administración de los usuarios, permisos de sistema operativos y límites de sesión, indicando un claro control de acceso y gestión de los sistemas operativos.

- ✓ **Política de uso equipos portátiles o móviles (2/3):** La institución se encuentra en la etapa de desarrollo de una política formal que incluye medidas de seguridad para la utilización de equipos portátiles o móviles, ya que aún no se encuentra implementada el nivel de madurez de este indicador, está por debajo del nivel óptimo.

- ✓ **Política de teletrabajo (1/3):** No existe una política formal que describa los procedimientos y actividades a controlar con respecto al teletrabajo, sin embargo existe un procedimiento verbal para solicitar la autorización y acceso por medio de redes privadas virtuales seguras, pero no se lleva un control de las actividades realizadas dentro de la misma.

- ✓ **Estado de madurez de la variable control de accesos:** El estado de madurez obtenida en esta variable es de 4,42 que la sitúa dentro de la escala de madurez nivel cuatro, lo cual indica que dispone de procesos *Gestionados Cuantitativamente.*

4.2.8 Variable 8: Adquisición, desarrollo y mantenimiento de los sistemas de información.

Los resultados obtenidos respecto a la adquisición, desarrollo y mantenimiento de los sistemas de información se muestran a continuación:

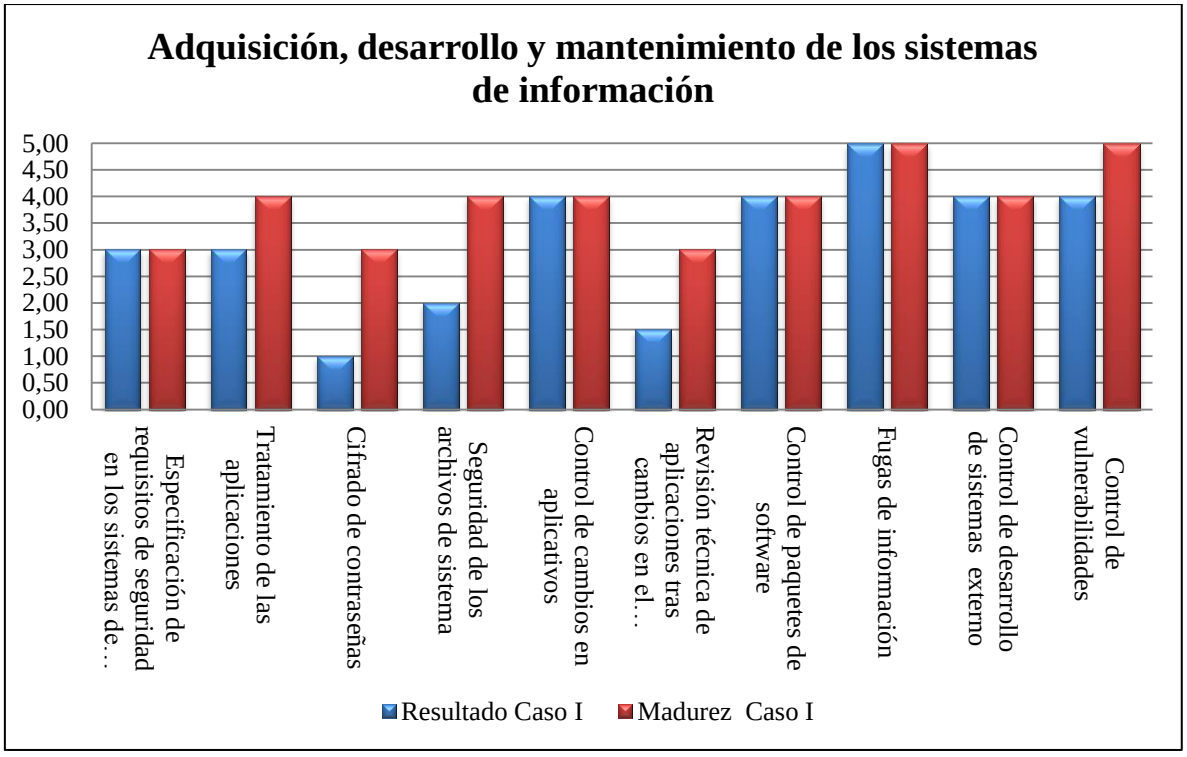

Figura 34: Adquisición, desarrollo y mantenimiento de los sistemas de información - Caso 1.

- ✓ **Especificación de requisitos de seguridad en los sistemas de información (3/3):** Todo nuevo sistema de información o modificación a los existentes, disponen de requisitos de controles de seguridad que se especifican en los términos de referencia (TDR) desarrollados para cada proyecto.

- ✓ **Tratamiento de las aplicaciones (3/4):** La institución dispone de algunos procedimientos para validar que los datos que procesan los sistemas de información sean los adecuados, sin embargo por temas técnicos, a nivel interno de la institución no se cifran las comunicaciones lo cual permitiría comprometer la confidencialidad de la información transmitida entre las terminales y los servidores de la organización, por tanto la madurez del indicador no alcanza su nivel óptimo.

- ✓ **Cifrado de contraseñas (1/3):** El departamento de desarrollo de sistemas de la institución supo indicar que utilizan métodos estándar para cifrar las contraseñas de los usuarios, el nivel óptimo de este indicador se alcanza cuando se aplican métodos avanzados de seguridad en la encriptación de contraseñas para precautelar la identidad de los usuarios.

- ✓ **Seguridad de los archivos de sistemas (2/4):** La gestión de seguridad referente a los archivos de los sistemas de información es llevada a cabo mediante procedimientos de control durante instalación o modificación de cualquier software que afecte al mismo, a su vez el acceso al código fuente de dichos sistemas de información es protegido celosamente. El punto débil durante la gestión de estos archivos de información es que cuando alguien solicita una copia de estos, no existe un procedimiento para verificar que datos son entregados, por esta razón el indicador no llega a su nivel de madurez óptimo.

- ✓ **Control de cambios en aplicativos (4/4):** Una de las fortalezas que se mencionó anteriormente es que la organización mantiene un control de cambios sobre los activos de información de la institución, siendo los sistemas de información parte de dichos activos, el procedimiento para el control de modificaciones y versionamiento se encuentra implementado.

- ✓ **Revisión técnica de aplicaciones tras cambios en el sistema operativo (1,50/3):** Es común que los recursos de soporte (servidores o sistemas operativos) para el tratamiento de los sistemas de información tengan que ser actualizados sea por razones de seguridad o rendimiento, para ello la institución no dispone de un procedimiento formal para validar que tras dicha actualización los sistemas de

información funcionen con normalidad, al momento el procedimiento es Ad-Hoc, razón por la cual no se llega al nivel de madurez óptimo planteado por el indicador.

- ✓ **Control de paquetes de software (4/4):** Al existir medios y controles tecnológicos para gestionar la instalación y modificación del software en las terminales de toda la institución, está dispone de una hegemonía en el software que utilizan los distintos usuarios de la organización.

- ✓ **Fugas de información (4/4):** La institución ha identificado las potenciales situaciones donde puede ocurrir fugas de información, para ello ha implementado reglas y procedimientos formales para el tratamiento de la información.

- ✓ **Control de desarrollo de sistemas externo (4/4):** Se evidencia que la institución dispone registros de control y supervisión del software que se desarrolla externamente.

- ✓ **Control de vulnerabilidades (4/5):** Un punto importante dentro la gestión de la seguridad en los sistemas de información, es conocer las vulnerabilidades asociadas a cada uno de ellos. La institución para identificar las vulnerabilidades asociadas a sus sistemas de información ha contratado los servicios de consultoría para el análisis de vulnerabilidades, sin embargo el indicador no llega a su punto óptimo de madurez, ya que la institución a nivel interno no dispone de un procedimiento para detectar vulnerabilidades en su sistema de información.

- ✓ **Estado de madurez de la variable adquisición, desarrollo y mantenimiento de los sistemas de información:** El estado de madurez obtenida en esta variable es de 4,85 que la sitúa dentro de la escala de madurez en el nivel cuatro, lo cual indica que dispone de procesos *Gestionados Cuantitativamente.*

4.2.9 Variable 9: Gestión de incidentes de seguridad

Los resultados obtenidos respecto a la gestión de incidentes de seguridad se muestran a continuación:

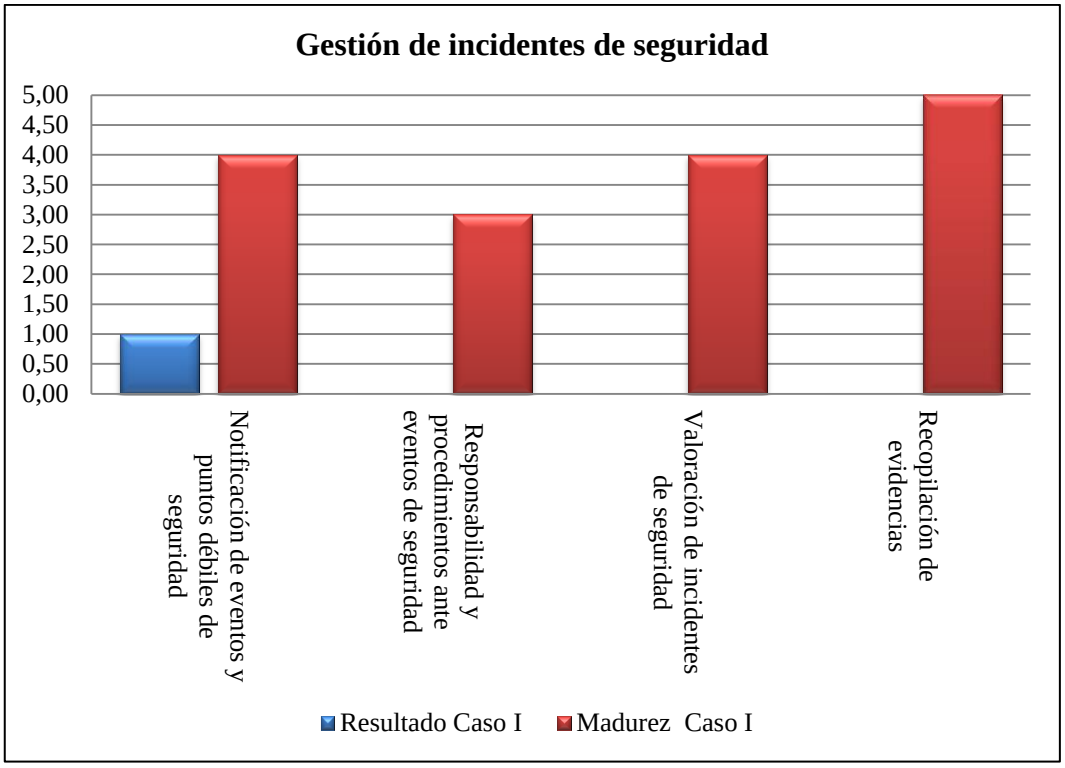

Figura 35: Gestión de incidentes de seguridad - Caso 1.

- ✓ **Notificación de eventos y puntos débiles de seguridad (1/4) - responsabilidad y procedimientos ante eventos de seguridad (0/3) - valoración de incidentes de seguridad (0/4) - recopilación de evidencias (0/5):** Se pudo evidenciar que con respecto a la variable gestión de incidentes de seguridad, si bien los usuarios se encuentran alertados y capacitados para que se notifique cualquier anomalía o evento de seguridad que consideren su ocurrencia, no existe por parte de la organización un procedimiento formal para la notificación de eventos de seguridad, así como no disponen de un mecanismo para cuantificar un incidente de seguridad, ni tampoco se recopila evidencia por personal capacitado o personal externo (forense o perito informático), que sustenten un evento de seguridad con el objetivo de tomar acciones civiles o penales.

- ✓ **Estado de madurez de la variable gestión de incidentes de seguridad:** Esto sitúa a los indicadores en un nivel bajo o nulo, y por ende a la variable en un estado de madurez de 0,38 que la sitúa dentro de la escala de madurez nivel cero, lo cual indica que *No dispone de procesos o controles.*

4.2.10 Variable 10: Gestión de la continuidad del negocio.

Los resultados obtenidos respecto a la gestión de la continuidad del negocio se muestran a continuación:

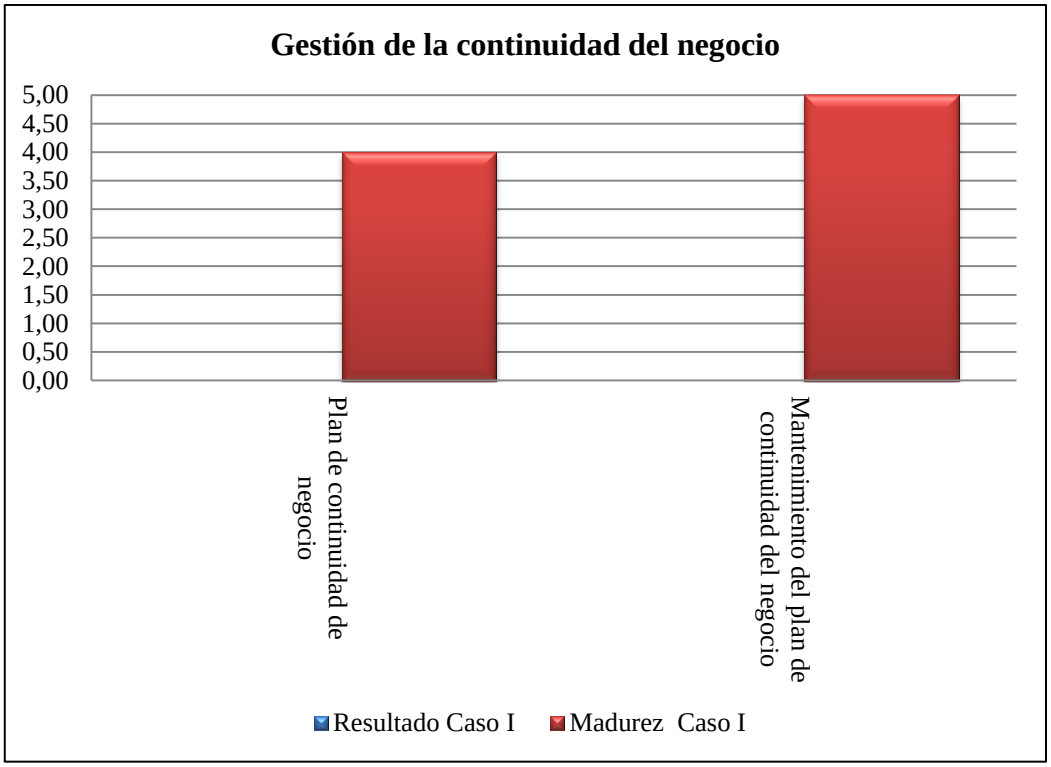

Figura 36: Gestión de la continuidad del negocio - Caso 1.

- ✓ **Plan de continuidad de negocio (0/4) - Mantenimiento del plan de continuidad del negocio (0/5):** Como se puede apreciar en el gráfico la Institución no cuenta con un plan de continuidad de negocio, así como no tiene identificado y evaluados los riesgos que pueden causar las interrupciones del servicio, esta variable desatendida podría ocasionar que se afecte la disponibilidad de la información a todos los actores involucrados con la institución.

- ✓ **Estado de madurez de la variable gestión de la continuidad del negocio:** El estado de madurez obtenida en esta variable es de 0,00 que la sitúa dentro de la escala de madurez nivel cero, lo cual indica que *No dispone de procesos o controles*.

4.2.11 Variable 11: Cumplimiento

Los resultados obtenidos respecto al cumplimiento se muestran a continuación:

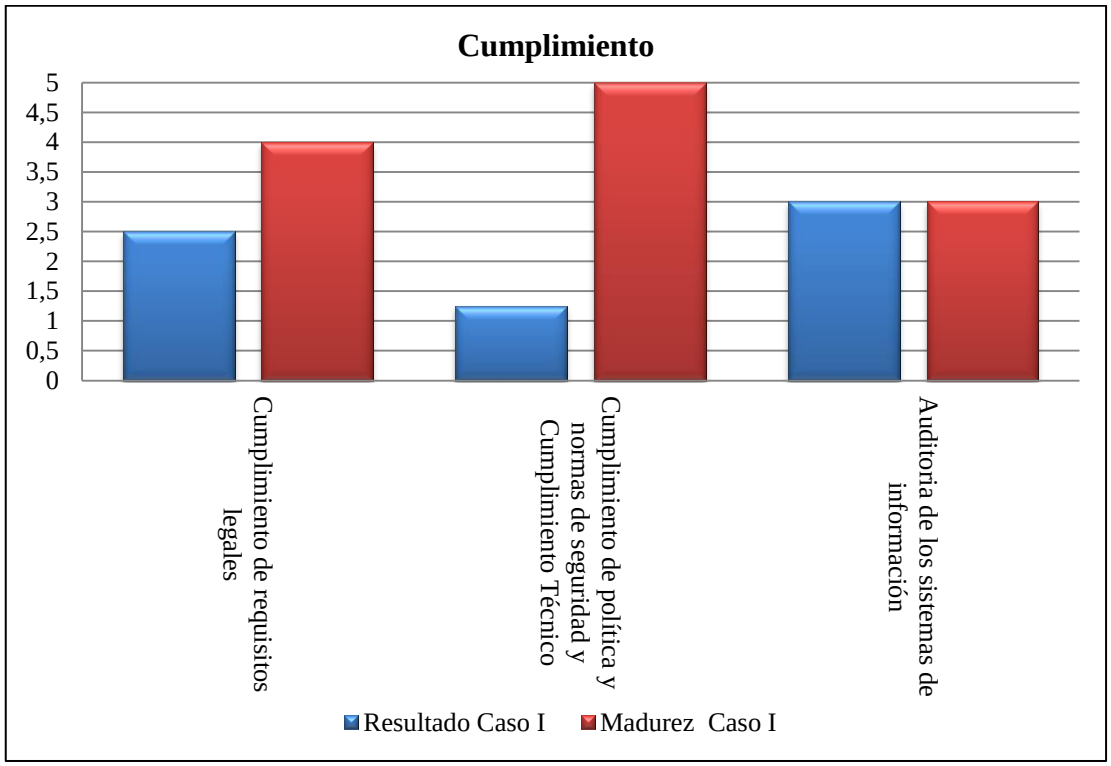

Figura 37: Cumplimiento - Caso 1.

- ✓ **Cumplimiento de requisitos legales (2.5/4):** Con respecto al cumplimiento de requisitos legales se pudo evidenciar que la institución ha identificado los requisitos legales de seguridad aplicables para los sistemas que utilizan, así como los de propiedad intelectual y uso de productos de software (licencias). También se evidencia que la protección de documentos importantes, se rige a los requisitos legales establecidos contractualmente en la legislación vigente y normativa institucional, referentes a la protección de datos y privacidad de la información y que el giro del negocio lo demanda. Sin embargo dicho indicador no alcanza su nivel óptimo de madurez, debido a que no se ha sociabilizado las acciones y/o consecuencias del uso indebido de los recursos de tratamiento de información, así como también el departamento legal desconoce de los procedimientos para validar que la criptografía se encuentra siendo aplicada de la manera correcta.

- ✓ **Cumplimiento de política y normas de seguridad y cumplimiento técnico (1.25/5):** La institución en lo referente al cumplimiento de política, normas de seguridad y cumplimiento técnico al encontrarse en la etapa de implementación, aun no dispone de procedimientos formales para que los directivos exijan o controlen, que se cumplan con los procesos de seguridad que se encuentran implantándose, llevando de esta manera a un nivel bajo al indicador.

- ✓ **Auditoria de los sistemas de información (3/3):** Se aprecia que la auditoria de los sistemas de información está siendo gestionada de un manera correcta, ya que en las mismas disponen de procesos que calendarizan, planifican y protegen la información levantada por las auditorias con el fin de evitar un impacto técnico por su labor, llevando al indicador a un nivel óptimo.

- ✓ **Estado de madurez de la variable cumplimiento:** El estado de madurez obtenida en esta variable es de 3,38 que la sitúa dentro de la escala de madurez nivel tres, lo cual indica que dispone de procesos *Definidos*.

4.2.12 Estado de Madurez de la Institución

Una vez analizada la información y obtenido el nivel de madurez de cada una de las once variables, se utiliza la ponderación de las variables como indica la tabla 13, con el fin de realizar un promedio ponderado de los resultados obtenidos en cada variable, que nos permita obtener el nivel de madurez de la calidad de gestión de la seguridad de la información en base a la norma NTE INEN ISO/IEC 27001:2011.

A continuación se muestra el comportamiento de cada una de las variables y su aporte a la madurez en la calidad de gestión de la seguridad de la información:

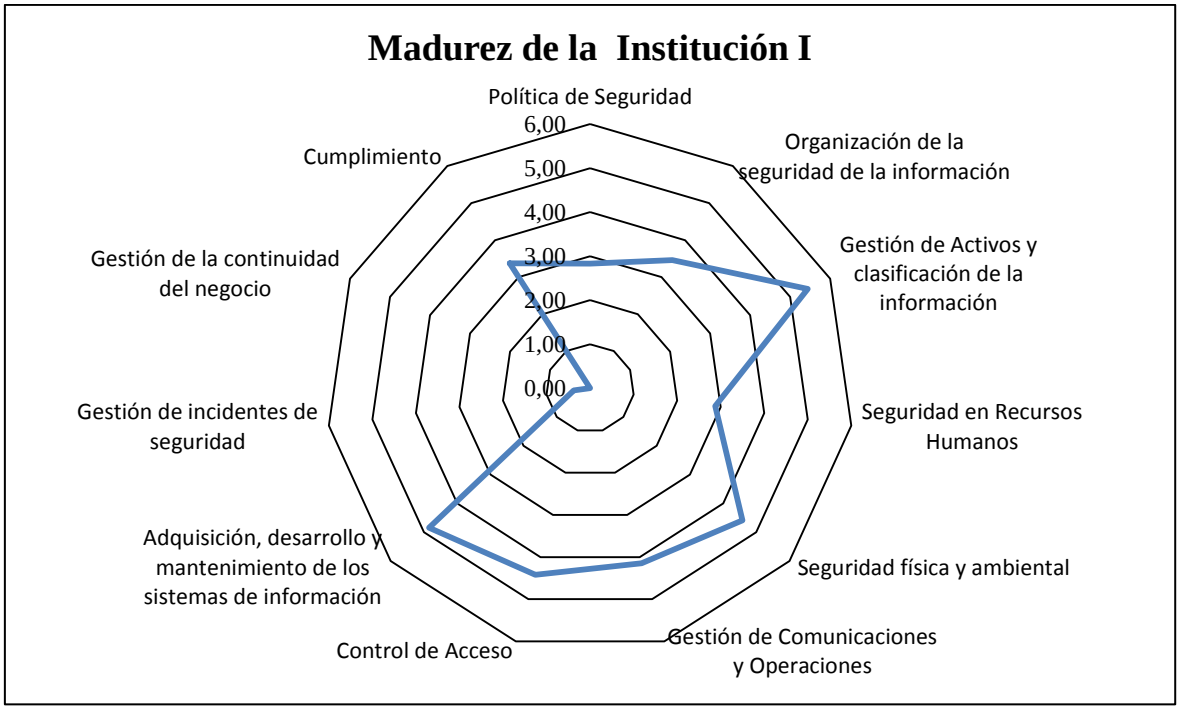

Figura 38: Madurez de la Institución I.

- ✓ **Gestión de la continuidad del negocio (0/5) - gestión de incidentes de seguridad (0/5):** Como se puede observar existen dos variables que se encuentran en un nivel cero de *Inexistencia* siendo los puntos más débiles de la institución.

- ✓ **Política de Seguridad (2/5) – seguridad en recursos humanos (2/5):** También se puede apreciar que dos variables se encuentran en el nivel dos, correspondiente a una madurez *Gestionada*, lo que significa que los procesos se planifican y ejecutan de acuerdo con las políticas.

- ✓ **Cumplimiento (3/5) - organización de la seguridad de la información (3/5):** Se identifican a dos variables en el nivel tres correspondiente a una madurez *Definida*, lo cual nos indica que los procesos están bien caracterizados y comprendidos, y se describen en estándares, procedimientos, herramientas y métodos.

- ✓ **Gestión de comunicaciones y operaciones (4/5) - control de acceso (4/5) – seguridad física y ambiental (4/5) - adquisición, desarrollo y mantenimiento de los sistemas de información (4/5):** El grupo que más variables aglutina (cuatro) se encuentra en el nivel de madurez cuatro, correspondiente a *Gestionada*

Cuantitativamente, es decir se establecen objetivos cuantitativos para medir la calidad y el rendimiento de los procesos, y se los utilizan como criterios de gestión.

- ✓ **Gestión de activos y clasificación de la información (5/5):** Esta variable se encuentra en el nivel cinco, el más alto de la escala de madurez correspondiente a *Optimizada*, donde se mejora continuamente sus procesos basándose en una comprensión cuantitativa de sus objetivos de negocio y necesidades de rendimiento.

- ❖ **Estado Madurez de la Institución Uno.**

A continuación se muestra el resultado de la madurez de cada variable junto a su ponderación:

Tabla 15:

Resultado de variables caso uno

N°	Variables	Madurez Variable	Ponderación Variable
1	Política de Seguridad	2,83	3,60
2	Organización de la seguridad de la información	3,46	3,44
3	Gestión de Activos y clasificación de la información	5,44	4,00
4	Seguridad en Recursos Humanos	2,88	3,43
5	Seguridad física y ambiental	4,58	4,00
6	Gestión de Comunicaciones y Operaciones	4,14	3,93
7	Control de Acceso	4,42	3,85
8	Adquisición, desarrollo y mantenimiento de los sistemas de información	4,85	3,90
9	Gestión de incidentes de seguridad	0,38	4,00
10	Gestión de la continuidad del negocio	0,00	4,50
11	Cumplimiento	3,38	4,00

A continuación se aplica el promedio ponderado de acuerdo a la metodología planteada, obteniendo el nivel de madurez de la institución con respecto a la calidad de gestión de la seguridad de la información.

- Resultado del nivel de madurez del caso uno:
  - 3.27 → **Definido**

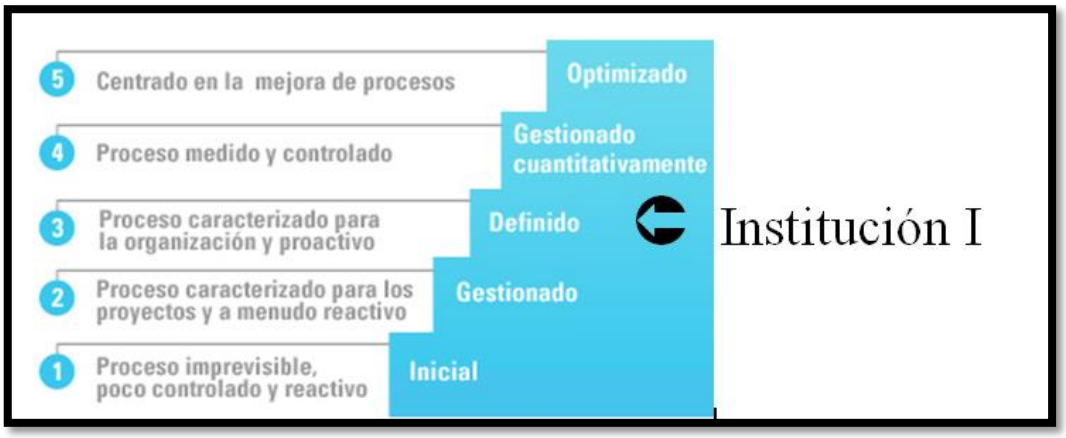

Figura 39: Nivel de madurez caso uno.

La institución analizada en el caso uno, se encuentra en el nivel de madurez tres *Definido,* lo que significa que los procesos que gestionan la seguridad de la información están bien caracterizados y comprendidos, y se describen en estándares, procedimientos, herramientas y métodos de forma proactiva.

4.3 Caso Dos

En el segundo caso se analiza a una institución pública dependiente de la administración central, siendo está uno de los ministerios más importantes en el país, el mismo que es la encargado de proteger los derechos fundamentales de los ciudadanos, y ser el ente rector de la administración del desarrollo institucional y de la gestión del talento humano. Dicha institución está conformada por 1400 funcionarios y su presencia es a nivel nacional, a través de 7 direcciones regionales y delegaciones en todas las provincias del Ecuador y la matriz se encuentra ubicada en Quito.

En septiembre de 2013, la Comisión para la Seguridad y de las Tecnologías de la Información y Comunicación emite el acuerdo interministerial N° 166, para la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), el cual se encuentra basado en la norma técnica ecuatoriana INEN ISO/IEC 27001 para la Gestión de la Seguridad de la Información. El mismo está dirigido para las Instituciones de Administración Pública Central y de implementación obligatoria, este esquema determina un conjunto de directrices prioritarias para la Gestión de la Seguridad de la Información.

En Julio del 2014 la alta dirección de la institución aprueba y publica la política de seguridad de la información acorde a lo solicitado por el esquema Gubernamental de Seguridad de la Información (EGSI), asignando los recursos administrativos y económicos necesarios para la aplicación de la misma. Se planificaron reuniones con las personas encargadas de cada departamento en la oficina matriz ubicada en Quito, para el levantamiento de los datos, de acuerdo a la metodología establecida. Esta investigación se la realizó en 3 días laborables, en periodos de tiempos distintos, ya que dependíamos de la disponibilidad de horarios de los servidores públicos.

A la fecha de inicio de la presente investigación la institución informa que el estado de implementación de controles es del 55% de acuerdo al EGSI, por lo que el objetivo será conocer cuan madura es la organización en relación a la gestión de la seguridad de la información, para lo cual se analiza los resultados de las once variables propuestas por la metodología.

4.3.1 Variable 1: Política de seguridad

Los resultados obtenidos respecto a la política de seguridad se muestran a continuación:

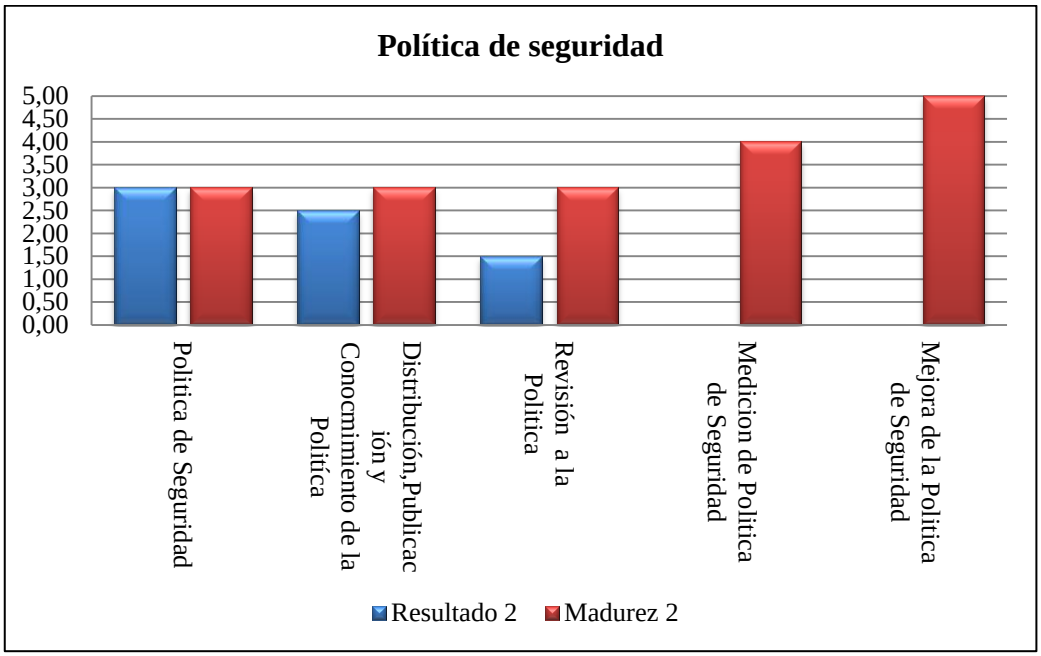

Figura 40: Política de seguridad – Caso 2.

- ✓ **Política de seguridad (3/3):** De acuerdo a la madurez propuesta para el indicador, los resultados obtenidos nos muestran que la institución, dispone de una política de seguridad de la información documentada situándola en el punto óptimo de escala de madurez.

- ✓ **Distribución, publicación y conocimiento de la política (2,5/3):** Se pudo evidenciar que la política de seguridad de la información está siendo distribuida y publicada, sin embargo los funcionarios de la institución no disponen de un conocimiento completo.

- ✓ **Revisión de la política (1,5/3):** La institución ha realizado revisiones de forma reactiva a la política de seguridad de la información, ya que han existido algunos incidentes de seguridad, los cuales requirieron ajustar nuevas normativas que permitan gestionar la seguridad de la información en toda la institución durante el proceso de implementación que se está ejecutando.

- ✓ **Medición de la política (0/4) y mejora de la política de seguridad (0/4):** Durante la investigación de campo funcionarios de la institución supieron indicar que no disponen de indicadores de gestión de la política de seguridad de la información, ni tampoco que existen planes de mejora de la misma, esto se debe a que la implementación de la norma está en marcha.

- ✓ **Estado de madurez de la variable política de seguridad:** El estado de madurez obtenida en esta variable es de 2,33 que la sitúa dentro de la escala de madurez en el nivel dos, lo cual indica que está siendo *Gestionada.*

4.3.2 Variable 2: Organización de la seguridad de la información

Los resultados obtenidos respecto a la organización de la seguridad de la información se muestran a continuación:

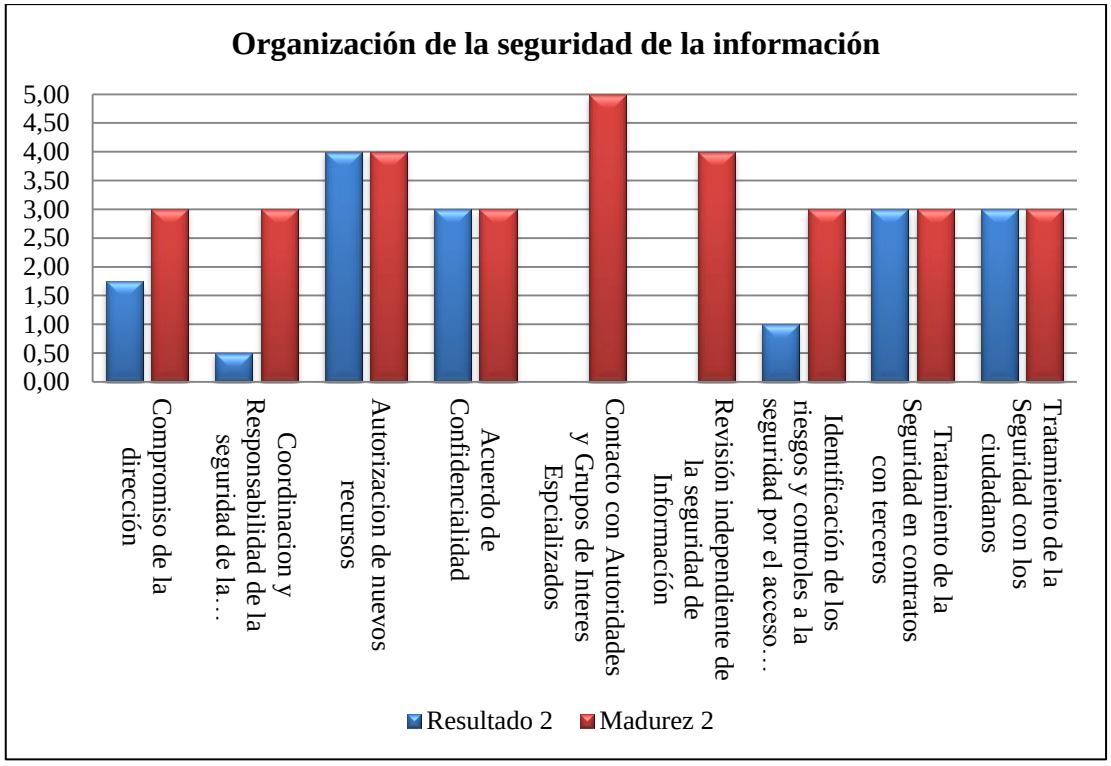

Figura 41: Organización de la seguridad de la información – Caso 2.

- ✓ **Compromiso de la dirección (1,75/3):** De acuerdo a la información obtenida, el compromiso por parte de la dirección es través de acuerdos formales, y el

reconocimiento de las responsabilidades para gestionar la seguridad de la información, sin embargo no llega a su tope óptimo, ya que los recursos económicos y administrativos para la implementación de controles no se encuentran en el presupuesto.

- ✓ **Coordinación y responsabilidad de la seguridad de la información (0,5/3):** La asignación de roles para la gestión de seguridad ha sido identificada para los distintos departamentos de la institución, sin embargo dichos roles solo están documentados, y el proceso de asignación formal está en marcha, lo cual hace que el indicador esté en niveles bajos.

- ✓ **Autorización de nuevos recursos (4/4):** La institución dispone de un procedimiento para autorizar el uso de nuevos recursos o activos para el tratamiento de la información.

- ✓ **Acuerdos de confidencialidad (3/3):** La institución dispone de acuerdos de confidencialidad con todos los actores involucrados, los cuales han sido revisados al menos una vez en el último año, con el objetivo de verificar que se cumpla su propósito.

- ✓ **Contacto con autoridades y grupos de interés especializados (0/4):** La institución no mantiene contacto con profesionales o entidades especializadas en el área de seguridad de la información, lo cual causa que su indicador sea nulo.

- ✓ **Revisión independiente de la seguridad de información (0/4):** La institución no dispone de registros de haber realizado auditorias o de disponer de una planificación para la revisión de la seguridad externa, por lo que su indicador es nulo.

- ✓ **Identificación de los riesgos y controles a la seguridad por el acceso de terceros (1/3):** La institución no ha identificado los riesgos provenientes por el acceso a la información por parte de terceros, sin embargo dispone de una serie de controles para limitar el acceso a la información, haciéndole falta implementar controles de

acceso de los dispositivos que utilizan terceros para acceder a la información, por esta razón el indicador llega a un nivel bajo en su escala.

- ✓ **Tratamiento de la seguridad en contratos con terceros (3/3):** Las cláusulas contractuales de confidencialidad, disponibilidad e integridad de la información se incluyen dentro de los contratos con terceros, dichas clausulas hacen una clara referencia a la política de seguridad de la institución.

- ✓ **Tratamiento de la seguridad con los ciudadanos (3/3):** Se evidencia que la institución identifica a los ciudadanos y define los perfiles de acceso a la información, por lo que logra un nivel óptimo en la aportación a la madurez de la variable.

- ✓ **Estado de madurez de la variable - organización de la seguridad de la información:** El estado de madurez obtenida en esta variable es de 3,14, que la sitúa dentro de la escala de madurez en el nivel tres, lo cual indica que dispone de procesos *Definidos.*

4.3.3 Variable 3: Gestión de activos y clasificación de la información

Los resultados obtenidos respecto a la gestión de los activos y la clasificación de la información se muestran a continuación:

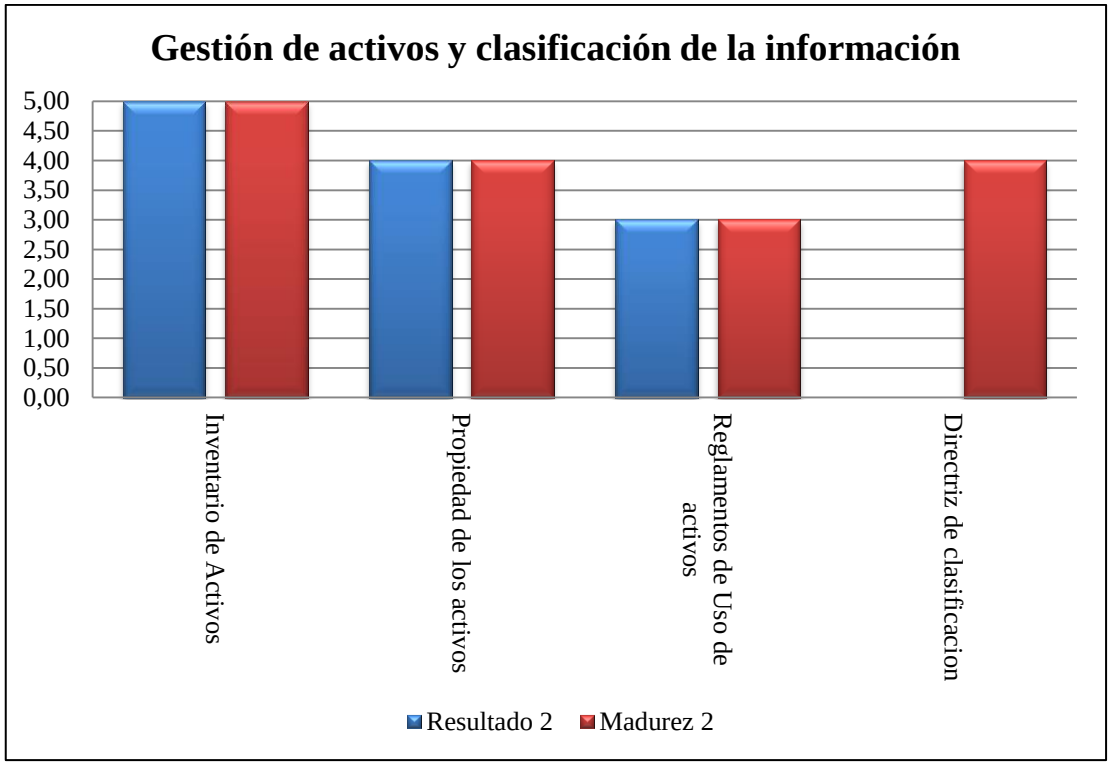

Figura 42: Gestión de activos y clasificación de la información – Caso 2.

- ✓ **Inventario de activos (5/5) - Propiedad de los activos (4/4) - reglamento de uso de activos (3/3):** Como se puede apreciar en la institución se mantiene un control óptimo sobre el inventario de los activos, mediante el uso de software especializado para el manejo de activos. Adicionalmente se evidenció que están claramente definidas las propiedades de cada uno de ellos, y que existe un reglamentos para el uso de dichos activos, estos reglamentos se encuentran documentados y sociabilizados.

- ✓ **Directriz de clasificación (0/4):** Se puedo evidenciar que la institución no dispone de procedimientos o directrices para clasificar la información, esto causa que el indicador sea nulo.

- ✓ **Estado de madurez de la variable gestión de activos y clasificación de la información:** El estado de madurez obtenida en esta variable es de 4,5 que la sitúa dentro de la escala de madurez en el nivel cuatro, lo cual indica que dispone de procesos que están siendo *Gestionados Cuantitativamente.*

4.3.4 Variable 4: Seguridad en recursos humanos

Los resultados obtenidos respecto a la Seguridad en Recursos Humanos se muestran a continuación:

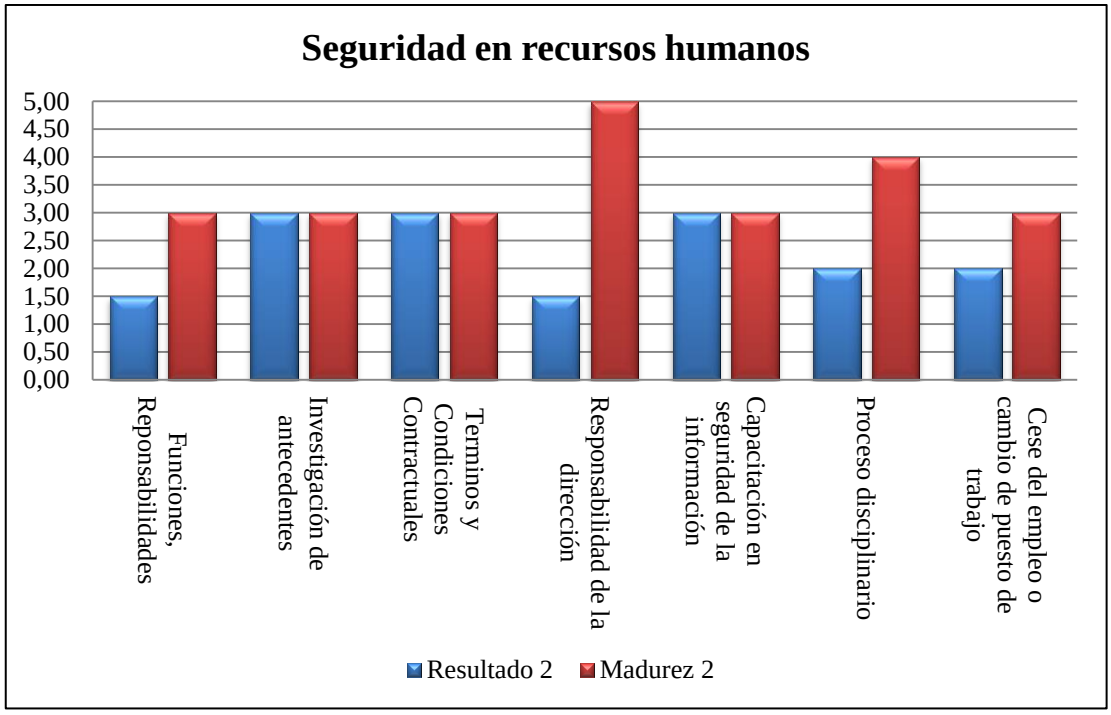

Figura 43: Seguridad en recursos humanos – Caso 2.

- ✓ **Funciones y responsabilidades (1,5/3) – Investigación de antecedentes (1/3):** La institución mantiene definidas las funciones y responsabilidades previas al empleo de un actor, sin embargo no tienen identificados los riesgos referentes a la seguridad de la información que la plaza de trabajo pueda ocasionar. Previa a la contratación se evidenció que el proceso de investigación de los postulantes incluye la verificación de antecedentes penales, antecedentes laborales y conductuales.

- ✓ **Términos y condiciones contractuales (3/3):** Referente a los términos y condiciones contractuales con los actores involucrados, se pudo determinar que la institución está incluyendo cláusulas que precautelan la confidencialidad, integridad y disponibilidad de la información que manejarán los actores, dichas clausulas hacen expresa referencia a la política de seguridad de la información.

- ✓ **Responsabilidad de la dirección (1,50/5):** Al estar la institución en un proceso de implementación de la norma, el sistema de gestión de seguridad no dispone de suficientes indicadores para que la dirección pueda tomar decisiones o acciones de mejora, al momento la dirección solo dispone de informes generales acerca de la implementación de políticas, procedimientos y controles.

- ✓ **Capacitación en seguridad de la información (3/3):** La institución al momento está en el punto más alto referente a la capacitación de los actores involucrados en temas relacionados con la seguridad de la información, siendo esta periódica y constante.

- ✓ **Proceso disciplinario (2/4):** El departamento de talento humano informó que han tomado medidas de tipo económico y legales en contra de funcionarios que han causado incidentes de seguridad, sin embargo no disponen de un proceso documentado, lo cual causa que su indicador no llegue al punto óptimo.

- ✓ **Cese de empleo o cambio de puesto de trabajo (2/4):** El departamento de talento humano informó que dispone de un procedimiento formal para cuando uno de los funcionarios cesan o cambian de puestos de trabajo, dicho procedimiento incluye actividades para la devolución de activos y actividades para retirar los accesos concedidos al funcionario, sin embargo dicho procedimiento carece de responsables para recibir la funciones y responsabilidades de los funcionarios salientes.

- ✓ **Estado de madurez de la variable seguridad en recursos humanos:** El estado de madurez obtenida en esta variable es de 4 que la sitúa dentro de la escala de madurez en el nivel cuatro, lo cual indica que dispone de procesos *Gestionados Cuantitativamente.*

4.3.5 Variable 5: Seguridad física y ambiental

Los resultados obtenidos respecto a la seguridad física y ambiental se muestran a continuación:

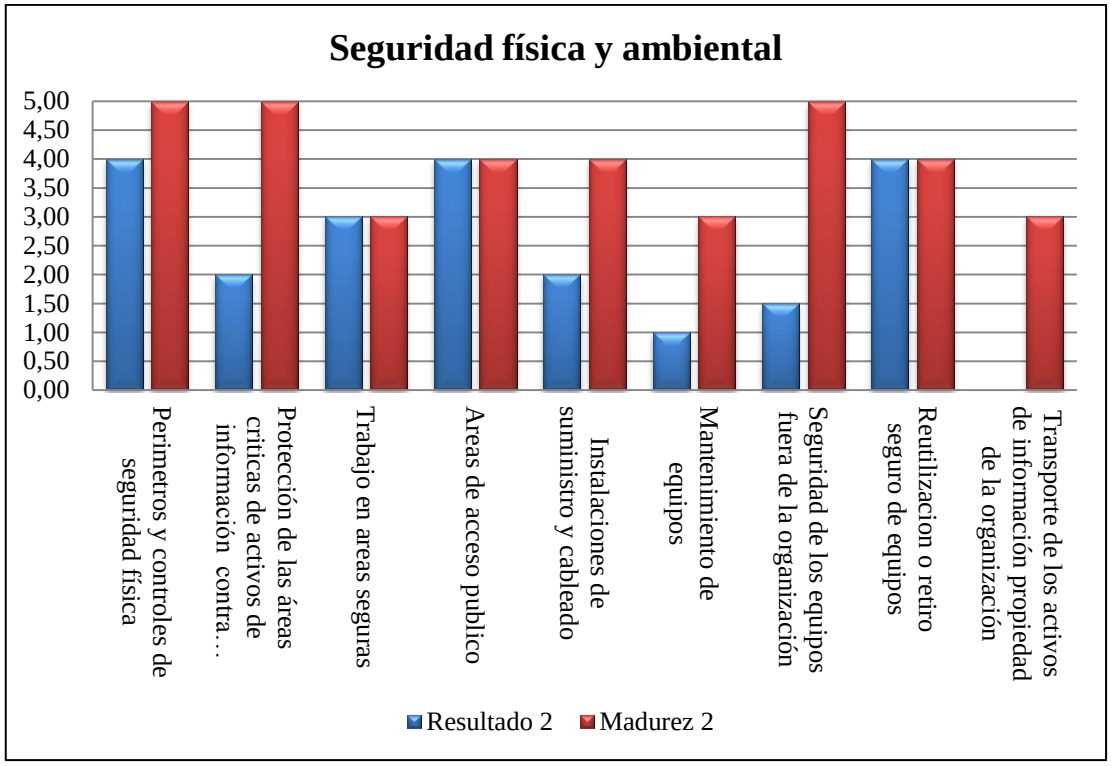

Figura 44: Seguridad física y ambiental – Caso 2.

- ✓ **Perímetros y controles de seguridad física (4/5):** En la institución se mantiene un control óptimo de los perímetros de las instalaciones, sin embargo se pudo observar que los controles de seguridad para el ingreso a las oficinas o despachos estaban desactivados, razón por la cual no llega el indicador a su punto óptimo.

- ✓ **Protección de las áreas críticas de activos de información contra amenazas externas y de origen ambiental (2/5):** Con respecto a la protección de las áreas críticas de tratamiento de la información, estas cuentan con los controles necesarios para asegurar la información, sin embargo se pudo evidenciar que en dichas áreas críticas no disponen de sensores anti-shock para precautelar la integridad de la información en caso de movimientos telúricos y el diseño de las salas no son del tipo bunker.

- ✓ **Trabajo en áreas seguras (3/3):** El trabajo en áreas seguras esta normado por un documento de política de seguridad industrial, el mismo que se encuentra implementado para proteger a las personas y zonas críticas (área de servidores) de posibles incidentes de seguridad.

- ✓ **Áreas de acceso público (4/4):** Se puede evidenciar que desde las áreas de acceso público hacia las privadas de la institución, se encuentran debidamente protegidas por sistemas de seguridad (puestos de vigilancia, controles de accesos físicos y lógicos) implementados para tal efecto.

- ✓ **Instalaciones de suministro y cableado (2/4):** La institución no dispone de una fuente alterna de energía en caso de fallas, lo que provocaría que la disponibilidad de la información sea afectada, sin embargo cuenta con cableado estructurado certificado y ha recibido un mantenimiento adecuado de acuerdo a los cambios físicos realizados en la institución. Por las razones presentadas el indicador no puede llegar a un nivel óptimo.

- ✓ **Mantenimiento de equipos (1/3):** La institución no cuenta con un plan preventivo para los equipos, en el caso de ocurrir un daño en los equipos se aplican medidas correctivas y puntuales. Los funcionarios nos indicaron que en años anteriores si disponían de un plan de mantenimiento preventivo, sin embargo debido a recortes presupuestarios se los eliminaron, razón por la cual el indicador no puede llegar a un nivel óptimo.

- ✓ **Seguridad de los equipos fuera de la organización (1,5/5):** En la seguridad física de los equipos fuera de las áreas seguras de la institución, se evidencia que se los protegen por medio de contraseñas, sin embargo no se utiliza encriptación de datos para proteger la confidencialidad de los mismos y también si los equipos son robados no disponen de un proceso de trazabilidad que permita recuperar o ubicar los equipos.

- ✓ **Reutilización o retiro seguro de equipos (4/4):** Con respecto a la reutilización o retiro seguro de equipos, en este indicador se mide la forma en la que se destruyen los datos de equipos que van a ser reutilizados. Se verificó que la institución realiza este proceso con técnicas de borrado seguras.

- ✓ **Transporte de los activos de información propiedad de la organización (0/3):** La institución no dispone de un proceso para el transporte de los activos de la información, propiedad de institución.

- ✓ **Estado de madurez de la variable seguridad física y ambiental:** El estado de madurez obtenida en esta variable es de 3,58 que la sitúa dentro de la escala de madurez nivel tres, lo cual indica que dispone de procesos *Definidos*.

4.3.6 Variable 6: Gestión de comunicaciones y operaciones

Los resultados obtenidos respecto a la gestión de comunicaciones y operaciones se muestran a continuación:

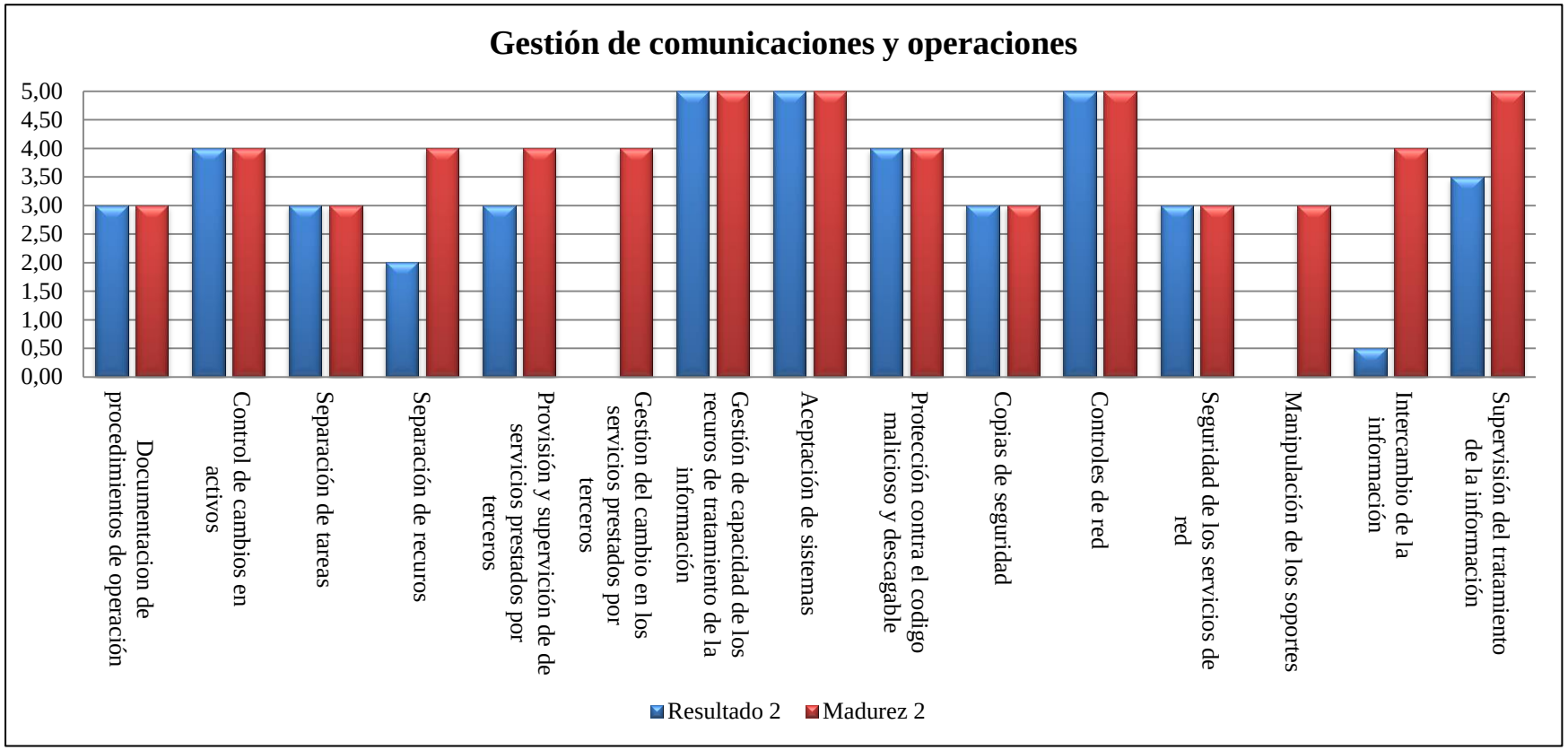

Figura 45: Gestión de comunicaciones y operaciones – Caso 2.

- ✓ **Documentación de procedimientos de operación (3/3):** Como se puede apreciar la institución mantiene de manera documentada los manuales de operación de los distintos sistemas de información, dichos manuales se encuentran a disposición de los usuarios y se los mantienen actualizados.

- ✓ **Control de cambios en activos (4/4):** Cualquier cambio realizado sobre los activos de información, responden a un procedimiento formal en el cual dichos cambios son documentados y se lleva un registro de versionamiento sobre los mismos.

- ✓ **Separación de tareas (3/3):** Dentro de la institución se tienen claramente identificadas las tareas y responsabilidades para el tratamiento de la información, dichas responsabilidades recaen sobre funcionarios como el administrador de base de datos, el administrador de infraestructura, el jefe del área de desarrollo, etc.

- ✓ **Separación de recursos (2/4):** Dentro del departamento que maneja la infraestructura de la institución, se pudo evidenciar que los recursos de tratamiento de la información se encuentran separados en diferentes ambientes, los mismos que son: producción, desarrollo, pruebas y capacitación, sin embargo funcionan dentro de los mismos segmentos de red, lo que causaría que si uno de ellos es comprometido se pueda escalar hacia los otros ambientes.

- ✓ **Provisión y supervisión de servicios prestados por terceros (3/4):** La institución cuando adquiere servicios prestados por terceros, dispone de un procedimiento para validar que dichos servicios cumplan con las expectativas requeridas, en dicho procedimiento se encuentran acuerdos de calidad de servicios, documentación de la implantación del servicio, etc., sin embargo el indicador no llega a su nivel máximo ya que, la institución no dispone de registros de auditoria que validen que el servicio es el esperado.

- ✓ **Gestión del cambio en los servicios prestados por terceros (0/4):** Un punto desfavorable durante la gestión de los servicios prestados por terceros, es que si existe algún cambio en la provisión del servicio y el mismo es aceptado por la institución, no existe ningún procedimiento para verificar si dicho cambio afecta a

la política o controles de seguridad de la información. Debido a la inexistencia de dicha gestión el indicador es nulo.

- ✓ **Gestión de capacidad de los recursos de tratamiento de la información (5/5):** La institución dispone de una planificación anual en donde se proyecta los futuros incrementos de recursos para el tratamiento de la información, permitiendo así garantizar el rendimiento requerido por los sistemas de información.

- ✓ **Aceptación de sistemas (5/5):** El procedimiento de aceptación de nuevos sistemas de información o modificaciones a los existentes realizados por terceros, se los realiza a través de los Términos y Referencias (TDR) del proyecto. Adicionalmente, este procedimiento incluye fases de pruebas durante el desarrollo o modificación de los sistemas, y una fase adicional de pruebas previa a la aceptación de los nuevos sistemas de información. Así también temas relacionados con la actualización o mejoras futuras están siendo contemplados, durante la aceptación de estos sistemas.

- ✓ **Protección contra el código malicioso y descargable (4/4):** La protección para las terminales de los usuarios en la institución está siendo gestionada de manera correcta, ya que disponen de un sistema del tipo EndPoint, que controla todo lo relacionado con virus, malware, y spam. Los usuarios están en constante capacitación para reconocer y evitar riesgos provenientes del internet. Por otro lado, los usuarios de los terminales tienen una estricta restricción que nos les permite instalar o ejecutar software no autorizado.

- ✓ **Copias de seguridad (3/3):** El departamento encargado del área de infraestructura supo indicar que disponen de un procedimiento formal para realizar copias de seguridad de la información, dichas copias de seguridad son sometidas a pruebas periódicas para validar que los datos no se encuentren dañados o corruptos.

- ✓ **Controles de red (5/5):** Las redes de comunicaciones en la institución se encuentran gestionadas por el administrador de red, con la ayuda de hardware especializado para el control y montero de la misma.

- ✓ **Seguridad de los servicios de red (3/3):** Los servicios de red tales como telefonía ip, correo electrónico, sistemas de información, etc., que expone la institución a los actores involucrados, se encuentran identificados y documentados, así como los requisitos relacionados a la seguridad de cada servicio.

- ✓ **Manipulación de los soportes (0/3):** La institución se encuentra desarrollando los mecanismos para gestionar la manipulación de soportes de almacenamiento en todas las terminales de usuario, al momento los usuarios pueden insertar memorias flash, cdrom, etc., sin ninguna restricción, por tanto la evaluación del indicador es nula.

- ✓ **Intercambio de la información (0,5/4):** La institución dispone de procedimientos formales para entregar o intercambiar información, sin embargo dichos procedimientos solo se encuentran documentados y no están socializados en la institución, por esta razón el indicador tiene un nivel bajo.

- ✓ **Supervisión del tratamiento de la información (3,5/5):** La supervisión del tratamiento de la información se encuentra normada por una serie de procedimientos y controles, en donde se registran todas actividades de los sistemas y recursos de tratamiento de la información; sin embargo no disponen de un procedimiento formal para auditar dichos registros generados por los sistemas, estos registros son utilizados de forma reactiva ante algún evento o necesidad, razón por la cual el indicador no llega a su punto óptimo.

- ✓ **Estado de madurez de la variable - gestión de comunicaciones y operaciones:** El estado de madurez obtenida en esta variable es de 3,58 que la sitúa dentro de la escala de madurez en el nivel tres, lo cual indica que dispone de procesos *Definidos.*

4.3.7 Variable 7: Control de accesos

Los resultados obtenidos respecto a los controles de acceso se muestran a continuación:

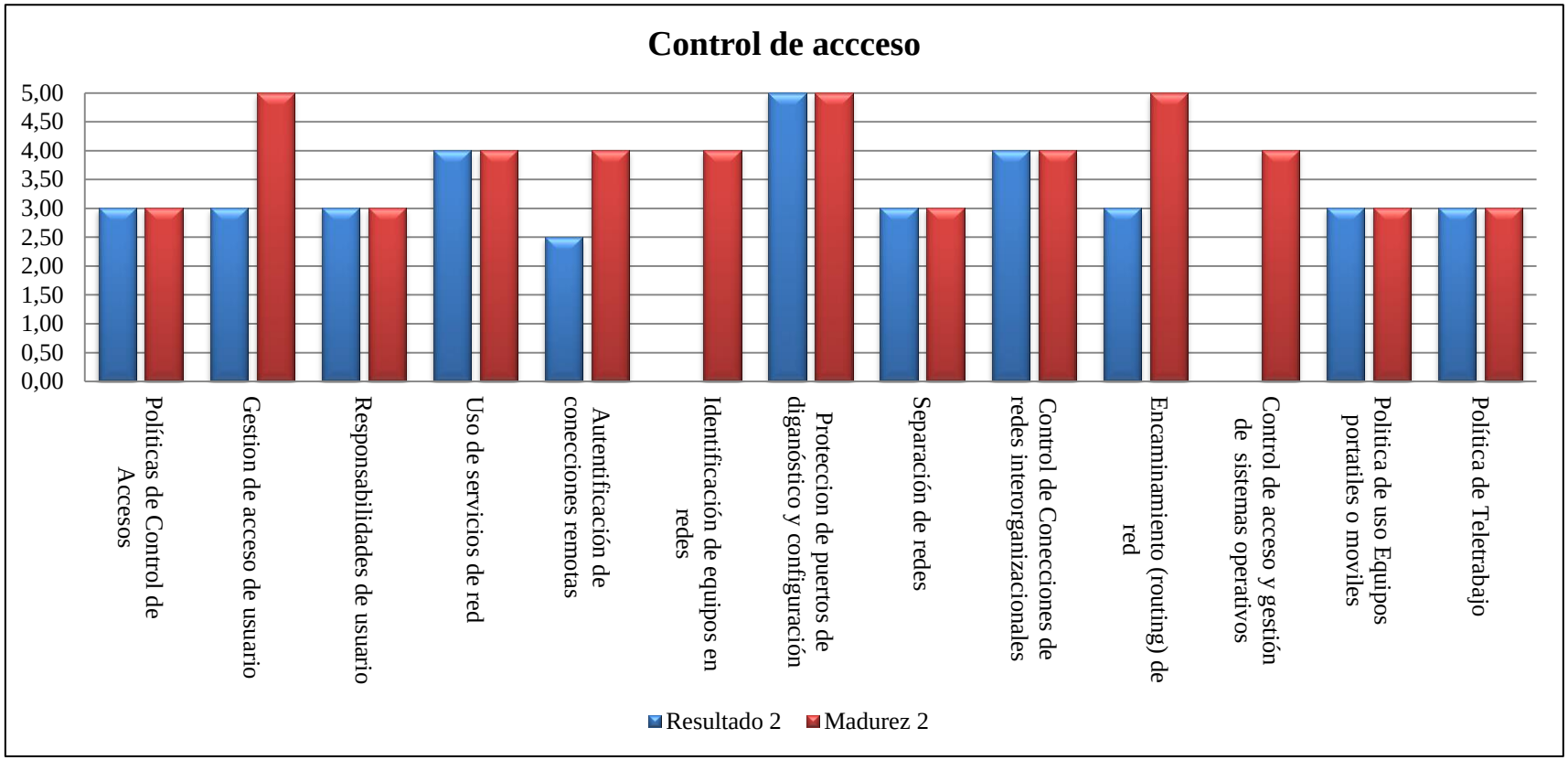

Figura 46: Control de accesos – Caso 2.

- ✓ **Políticas de control de accesos (3/3):** La institución dispone de una política formal de control de accesos, la cual se encuentra publicada e implementada, logrando así un nivel óptimo del indicador.

- ✓ **Gestión de acceso de usuario (3/5):** La institución se encuentra en un proceso de implementación de controles, para prevenir el acceso no autorizado a los sistemas de información, al momento se están definiendo temas para normar la asignación y uso de permisos a los usuarios, así como la revisión periódica de dichos permisos, razón por la cual el indicador no llega a su punto óptimo.

- ✓ **Responsabilidades de usuario (3/3):** Se determina que las responsabilidades de los usuarios con respecto a la seguridad referente al acceso a la información, están siendo cumplidas a cabalidad, las mismas fueron confirmadas con técnicas de observación que permiten situar a este indicador en el nivel óptimo.

- ✓ **Uso de servicios de red (4/4):** Se verifica que en el uso de los servicios de red, la institución dispone de reglas que norman el acceso a los servicios autorizados a los usuarios, con este control y gestión se sitúa el indicador en un nivel óptimo.

- ✓ **Autentificación de conexiones remotas (2,5/4):** Se determinó que la institución cuenta con métodos seguros de autentificación de conexiones remotas (conexiones seguras remotas VPN´s , envío/recepción de correos smtps/pop3s, administración de dispositivos ssh, encriptación wpa2 en conexiones inalámbricas), sin embargo los usuarios no las utilizan de manera adecuada, pudiendo comprometer la confidencialidad, integridad y disponibilidad de la información (uso de HTTPS para aplicativos, uso obligatorio de VPN´s), por esta razón el indicador no llega a un nivel óptimo.

- ✓ **Identificación de equipos en redes (0/4):** La institución no dispone de un proceso para identificar a los equipos en las distintas redes, por lo que cualquier persona puede conectar un equipo no autorizado y ganar acceso a la red.

- ✓ **Protección de puertos de diagnóstico y configuración (5/5):** Se dispone de un inventario y control periódico de los puertos de diagnóstico y configuración en todos los dispositivos concentradores de la red.

- ✓ **Separación de redes (3/3):** La institución dispone de un proceso definido e implementado para la separación de las redes (vlans), siendo esta establecida por grupos de servicios o usuarios.

- ✓ **Control de conexiones de redes inter-organizacionales (4/4):** También disponen de un proceso definido para restringir a los usuarios el acceso a las conexiones a redes entre organizaciones interministeriales, reflejando un control claro en este aspecto.

- ✓ **Encaminamiento (routing) de red (3/5):** Con respecto a las rutas de encaminamiento (tracert o routing) que siguen los flujos de información en la organización, la institución dispone de hardware especializado que gestiona dicho flujo, sin embargo no están definidos los procesos para monitorear o auditar los registros recopilados, por lo cual el indicador no llega al punto óptimo.

- ✓ **Control de acceso y gestión de sistemas operativos (0/4):** Una debilidad muy marcada que tiene la institución, es la no presencia de una solución integral para la administración de los usuarios y sus permisos a nivel del sistema operativo en las terminales, siendo este proceso en la actualidad llevado a cabo de forma manual.

- ✓ **Política de uso equipos portátiles o móviles (3/3):** La institución dispone de una política formal que incluye medidas de seguridad para la utilización de equipos portátiles o móviles, la cual se encuentra publicada y sociabilizada entre los funcionarios.

- ✓ **Política de teletrabajo (3/3):** La institución dispone de una política formal que describe los procedimientos y actividades a controlar con respecto al teletrabajo, esta se encuentra publicada y sociabilizada entre los funcionarios.

- ✓ **Estado de madurez de la variable control de accesos:** El estado de madurez obtenida en esta variable es de 4,47 que la sitúa dentro de la escala de madurez nivel cuatro, lo cual indica que dispone de procesos *Gestionados Cuantitativamente.*

4.3.8 Variable 8: Adquisición, desarrollo y mantenimiento de los sistemas de información

Los resultados obtenidos respecto a la adquisición, desarrollo y mantenimiento de los sistemas de información se muestran a continuación:

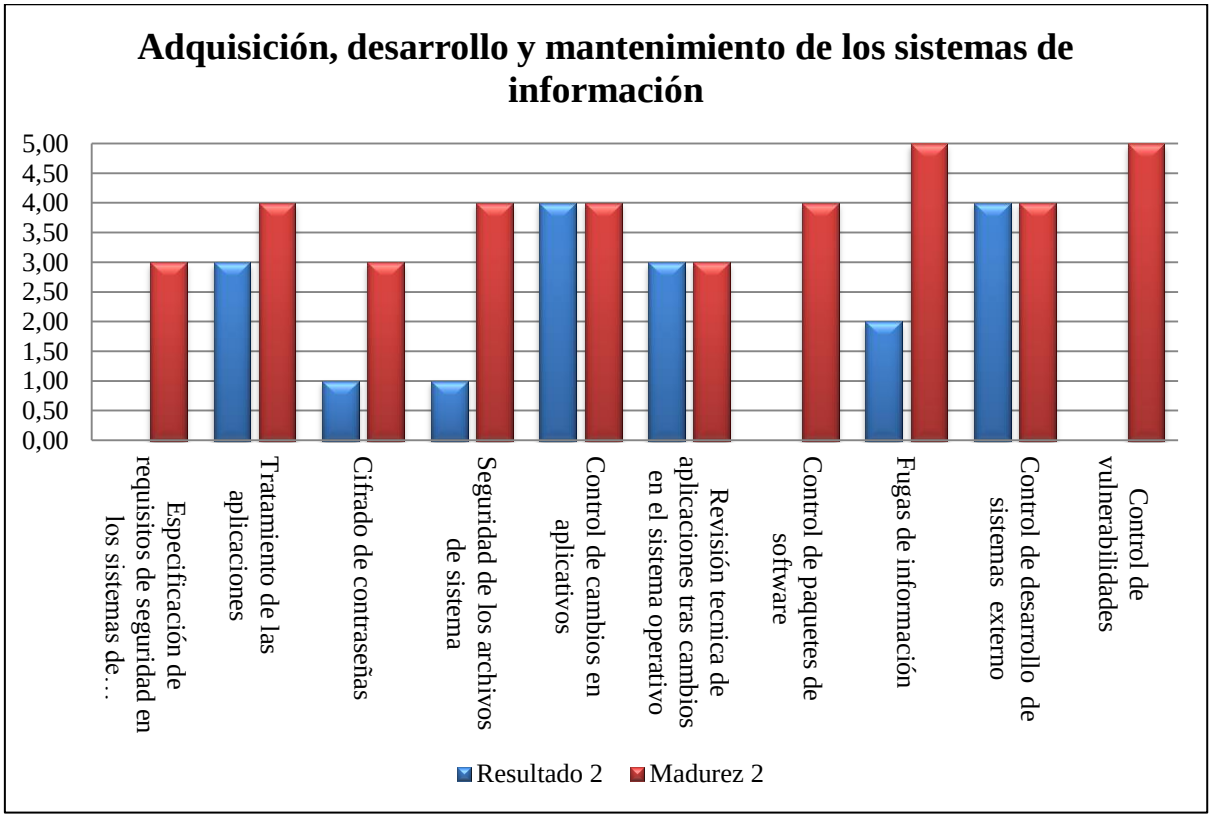

Figura 47: Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información – Caso 2.

- ✓ **Especificación de requisitos de seguridad en los sistemas de información (0/3):** Una importante debilidad se evidencia en el presente indicador, en donde para todo nuevo sistema o modificación de los existentes no se especifican en los términos de referencias los requisitos de controles seguridad, por ello el indicador es nulo.

- ✓ **Tratamiento de las aplicaciones (3/4):** La institución dispone de algunos procedimientos para validar que los datos que procesan los sistemas de información sean los adecuados, sin embargo por temas técnicos, a nivel interno de la institución no se cifran las comunicaciones, lo cual permitiría comprometer la confidencialidad de la información transmitida entre las terminales y los servidores de la organización, por tanto la madurez del indicador no alcanza su nivel óptimo.

- ✓ **Cifrado de contraseñas (1/3):** El departamento de desarrollo de sistemas de la institución supo indicar que utilizan métodos estándar para cifrar las contraseñas de los usuarios, el nivel óptimo de este indicador se alcanza cuando se aplican métodos avanzados de seguridad en la encriptación de contraseñas para precautelar la identidad de los usuarios.

- ✓ **Seguridad de los archivos de sistemas (1/4):** La gestión de seguridad referente a los archivos de los sistemas de información no es llevada a cabo de forma efectiva, ya que no existe un control durante la instalación o modificación de cualquier software que afecte a los mismos, a su vez cuando alguien solicita una copia de estos, no existe un procedimiento para verificar que datos son entregados. Como único control disponen de estrictos procedimientos para acceder al código fuente de los sistemas de información, por estas razones el indicador no llega a su punto óptimo.

- ✓ **Control de cambios en aplicativos (4/4):** Una de las fortalezas que se mencionó anteriormente es que la organización mantiene un control de cambios sobre los activos de información de la institución, siendo los sistemas de información parte de dichos activos, el procedimiento para el control de modificaciones y versionamiento se encuentra implementado.

- ✓ **Revisión técnica de aplicaciones tras cambios en el sistema operativo (3/3):** Es común que los recursos de soporte (servidores o sistemas operativos) para el tratamiento de los sistemas de información, tengan que ser actualizados sea por razones de seguridad o rendimiento, para ello la institución dispone de un

procedimiento formal para validar que tras dicha actualización los sistemas de información funcionen con normalidad.

- ✓ **Control de paquetes de software (0/4):** Al no existir medios y controles tecnológicos para gestionar la instalación y modificación del software en las terminales de toda la institución, está no dispone de una hegemonía en el software que utilizan los distintos usuarios de la organización, teniendo así este indicador como nulo.

- ✓ **Fugas de información (2/4):** La institución ha identificado las potenciales situaciones donde puede ocurrir fugas de información, sin embargo se encuentra en proceso de definición las reglas o procedimientos para prevenirlas, por lo cual el indicador no llega a su nivel óptimo.

- ✓ **Control de desarrollo de sistemas externo (4/4):** Se evidencia que la institución dispone de registros de control y supervisión del software que se desarrolla externamente.

- ✓ **Control de vulnerabilidades (0/5):** La institución no dispone de información acerca de las vulnerabilidades técnicas de sus activos o recursos que tratan la información.

- ✓ **Estado de madurez de la variable adquisición, desarrollo y mantenimiento de los sistemas de información:** El estado de madurez obtenida en esta variable es de 2,46 que la sitúa dentro de la escala de madurez en el nivel dos, lo cual indica que dispone de procesos *Gestionados*.

4.3.9 Variable 9: Gestión de incidentes de seguridad

Los resultados obtenidos respecto a la gestión de incidentes de seguridad se muestran a continuación:

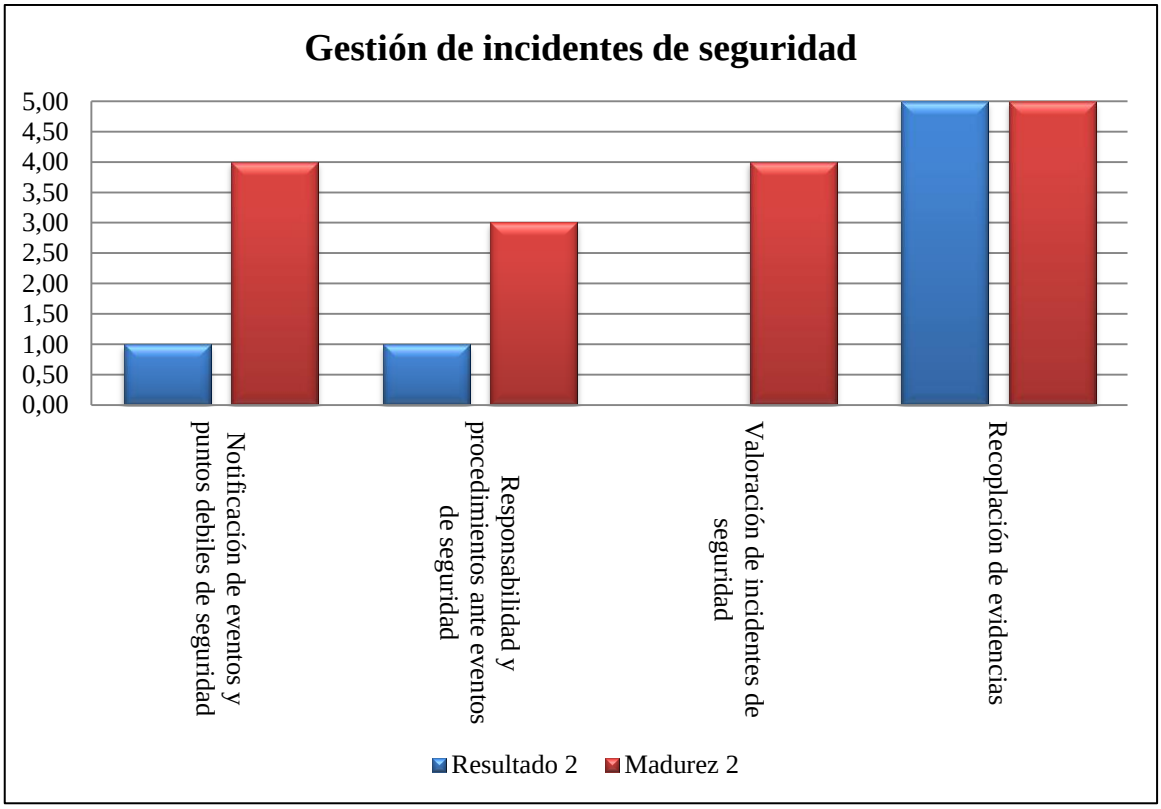

Figura 48: Gestión de incidentes de seguridad – Caso 2.

- ✓ **Notificación de eventos y puntos débiles de seguridad (1/4) - responsabilidad y procedimientos ante eventos de seguridad (1/3) - valoración de incidentes de seguridad (0/4) - recopilación de evidencias (5/5):** Se pudo evidenciar que con respecto a la variable Gestión de incidentes de seguridad, que si bien los usuarios se encuentran alertados y capacitados para que se notifique cualquier anomalía o evento de seguridad, no existe por parte de la organización un procedimiento formal para la notificación de eventos de seguridad, de presentarse algún evento de seguridad no existen responsables y las acciones que se toman son del tipo Ad-hoc, tampoco disponen de un mecanismo para cuantificar un incidente de seguridad, lo que se rescata de esta variable es que la institución durante los últimos meses ha contratado personal capacitado (forense o perito informático), para investigar o

recopilar evidencia que sustenten un evento de seguridad con el objetivo de tomar acciones civiles o penales.

- ✓ **Estado de madurez de la variable gestión de incidentes de seguridad:** El estado de madurez obtenida en esta variable es de 2,63 que la sitúa dentro de la escala de madurez en el nivel dos, lo cual indica que dispone de procesos *Gestionados.*

4.3.10 Variable 10: Gestión de la continuidad del negocio

Los resultados obtenidos respecto a la Gestión de la continuidad del negocio se muestran a continuación:

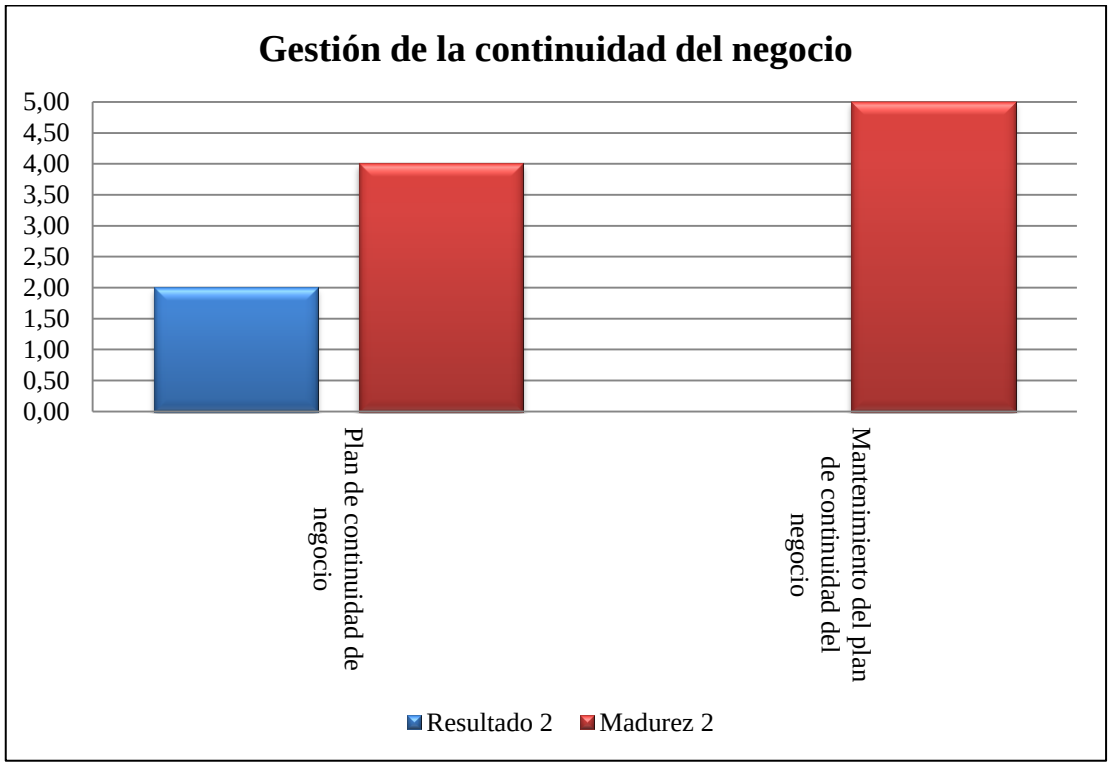

Figura 49: Gestión de la continuidad del negocio – Caso 2.

- ✓ **Plan de continuidad de negocio (2/4) - Mantenimiento del plan de continuidad del negocio (0/5):** La Institución cuenta con un plan de continuidad de negocio, el cual tiene identificado y evaluados los riesgos que pueden causar las interrupciones del servicio, sin embargo dicho plan no se encuentra implementado, por tanto no existe un mantenimiento del plan de continuidad de negocio.

- ✓ **Estado de madurez de la variable gestión de la continuidad del negocio:** El estado de madurez obtenida en esta variable es de 1,33 que la sitúa dentro de la escala de madurez en el nivel uno, lo cual indica que dispone de procesos en la etapa *Inicial.*

4.3.11 Variable 11: Cumplimiento

Los resultados obtenidos respecto al cumplimiento se muestran a continuación:

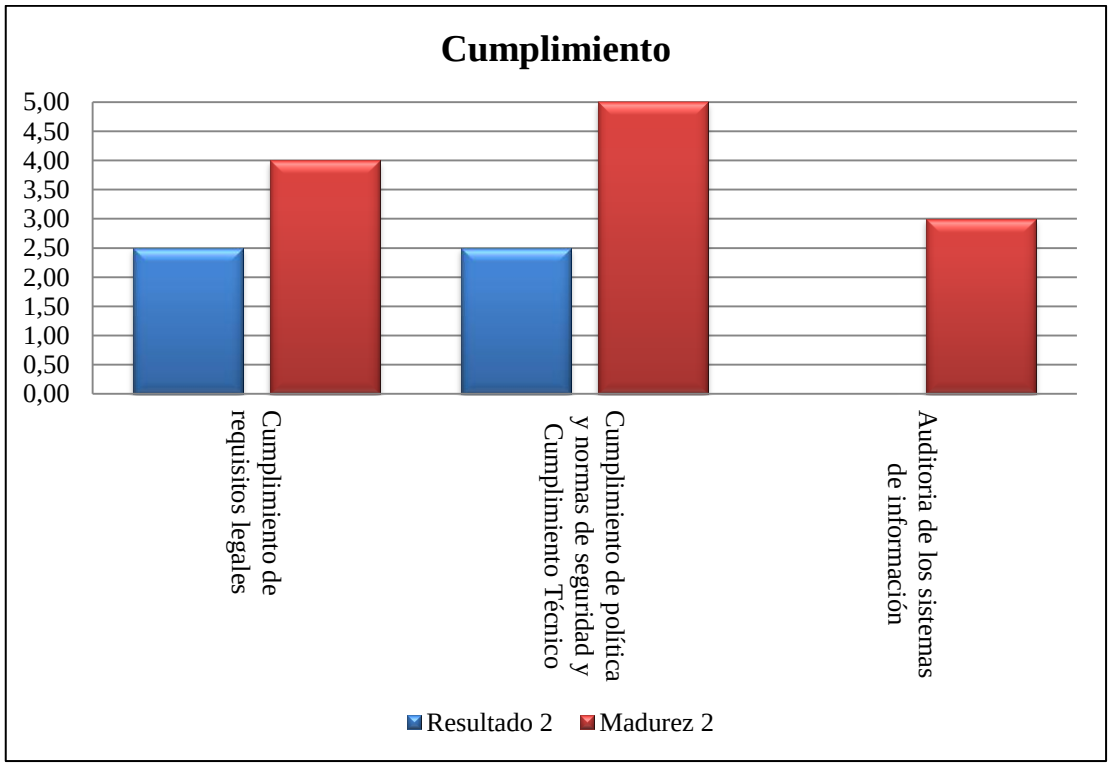

Figura 50: Cumplimiento – Caso 2.

- ✓ **Cumplimiento de requisitos legales (2,5/4):** Con respecto al cumplimiento de requisitos legales se pudo evidenciar que la institución ha identificado los requisitos legales de seguridad aplicables para los sistemas que utilizan, así como los de propiedad intelectual y uso de productos de software (licencias). También se evidencia que no existen las directrices para clasificación y protección de documentos importantes; sin embargo disponen de procedimientos para velar por la privacidad de la información de actores internos y externos. No existe una socialización de las acciones y/o consecuencias del uso indebido de los recursos de

tratamiento de información, así como también el departamento legal desconoce de los procedimientos para validar que la criptografía se encuentra siendo aplicada de la manera correcta.

- ✓ **Cumplimiento de política y normas de seguridad y cumplimiento técnico (2,5/5):** La institución en lo referente al cumplimiento de política, normas de seguridad y cumplimiento técnico al encontrarse en la etapa de implementación, aun no dispone de procedimientos formales para que los directivos exijan o controlen; sin embargo existen reuniones periódicas para evaluar el estado de implementación de controles y procedimientos, por esta razón el indicador no alcanza su nivel óptimo.

- ✓ **Auditoria de los sistemas de información (0/3):** El departamento legal supo indicar que no disponen de registros de auditorías realizadas a los sistemas de información, sin embargo para el presente año ya se encuentran planificas.

- ✓ **Estado de madurez de la variable cumplimiento:** El estado de madurez obtenida en esta variable es de 2,5 que la sitúa dentro de la escala de madurez nivel dos, lo cual indica que dispone de procesos *Gestionados*.

4.3.12 Estado de Madurez de la Institución.

Una vez analizada la información y obtenida el nivel de madurez de cada una de las once variables, se utiliza la ponderación de las variables como indica la tabla 13, con el fin de realizar un promedio ponderado de los resultados obtenidos en cada variable, que nos permita obtener el nivel de madurez de la calidad de gestión de la seguridad de la información en base a la norma NTE INEN ISO/IEC 27001:2011.

A continuación se muestra el comportamiento de cada una de las variables y su aporte a la madurez en la calidad de gestión de la seguridad de la información:

Figura 51: Madurez de la Institución II.

- ✓ **Gestión de la continuidad del negocio (1/5):** Como se puede observar existe una variable que se encuentran en un nivel uno de estado *Inicial*, lo que nos indica que los procesos son generalmente ad hoc y caóticos, siendo el punto más débil de la institución.

- ✓ **Política de Seguridad (2/5) – cumplimiento (2/5) - gestión de incidentes de seguridad (2/5) y adquisición, desarrollo y mantenimiento de los sistemas de información (2/5):** También se puede apreciar que cuatro variables se encuentran en el nivel dos correspondiente a una madurez *Gestionada,* lo que significa que los procesos se planifican y ejecutan de acuerdo con las políticas.

- ✓ **Seguridad física y ambiental (3/5) y organización de la seguridad de la información (3/5):** Se identificaron dos variables en el nivel tres correspondiente a una madurez *Definida,* lo cual nos indica que los procesos están bien caracterizados y comprendidos, y se describen en estándares, procedimientos, herramientas y métodos.

- ✓ **Gestión de comunicaciones y operaciones (4/5) - control de acceso (4/5) – seguridad en recursos humanos (4/5) - gestión de activos y clasificación de la información (4/5):** Se puede apreciar que cuatro variables se encuentra en el nivel de madurez cuatro correspondiente a *Gestionada Cuantitativamente*, es decir se establecen objetivos cuantitativos para medir la calidad y el rendimiento de los procesos, y se los utilizan como criterios de gestión.

❖ **Estado Madurez de la Institución Dos.**

A continuación se muestra el resultado de la madurez de cada variable junto a su ponderación:

Tabla 16:

Resultado de variables

N°	Variables	Madurez Variable	Ponderación Variable
1	Política de Seguridad	2,3	3,60
2	Organización de la seguridad de la información	3,1	3,44
3	Gestión de Activos y clasificación de la información	4,5	4,00
4	Seguridad en Recursos Humanos	4,0	3,43
5	Seguridad física y ambiental	3,6	4,00
6	Gestión de Comunicaciones y Operaciones	4,5	3,93
7	Control de Acceso	4,4	3,85
8	Adquisición, desarrollo y mantenimiento de los sistemas de información	2,8	3,90
9	Gestión de incidentes de seguridad	2,6	4,00
10	Gestión de la continuidad del negocio	1,3	4,50
11	Cumplimiento	2,5	4,00

A continuación se aplica el promedio ponderado de acuerdo a la metodología planteada, obteniendo el nivel de madurez de la institución con respecto a la calidad de gestión de la seguridad de la información.

- Resultado del nivel de madurez del caso uno:
  - 3.21 → **Definido**

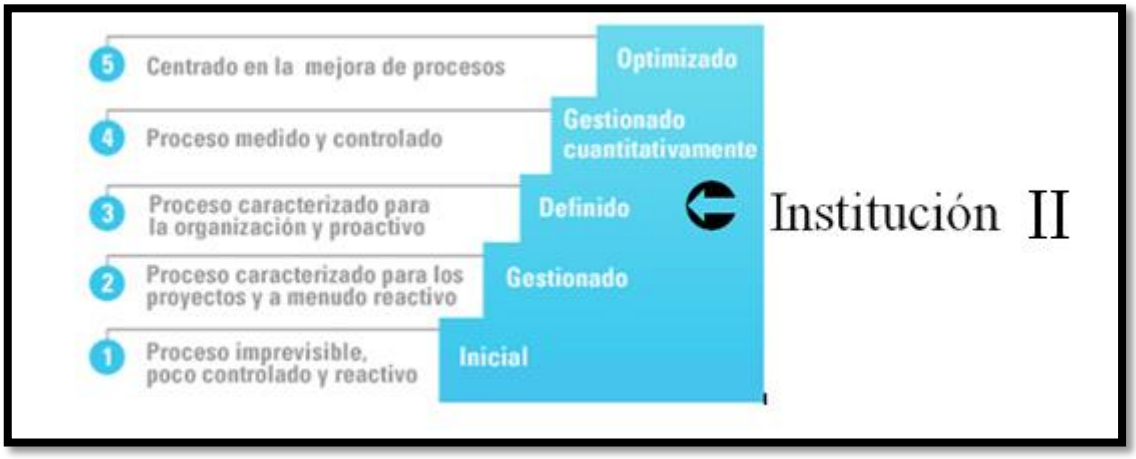

Figura 52: Nivel de madurez caso dos.

La Institución analizada en el caso dos, se encuentra en el nivel de madurez tres *Definido,* lo que significa que los procesos que gestionan la seguridad de la información están bien caracterizados y comprendidos, y se describen en estándares, procedimientos, herramientas y métodos de forma proactiva.

4.4 Caso Tres

En el presente caso se analiza a una institución pública dependiente de la administración central, la misma que ha diseñado, implementado y administra un Sistema Nacional de información pública, sistema que se alimenta por la información de instituciones públicas, información de carácter público de las instituciones privadas, administra el conjunto de normas, políticas, instrumentos, procesos, actividades y recursos que permitan alcanzar el acceso y la transparencia de la información pública acorde a las nuevas tecnologías, garantizando al ciudadano la seguridad jurídica en el marco constitucional y legal vigente.
Esta institución dispone de presencia a nivel nacional cubriendo todo el territorio con 7 regionales y la matriz ubicada en Quito.

En septiembre de 2013, la Comisión para la Seguridad y de las Tecnologías de la Información y Comunicación emite el acuerdo interministerial N° 166, para la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), el cual se encuentra basado en la norma técnica ecuatoriana INEN ISO/IEC 27001 para la Gestión de la Seguridad de la Información. El mismo que está dirigido para las Instituciones de Administración Pública Central y de implementación obligatoria, este esquema determina un conjunto de directrices prioritarias para la Gestión de la Seguridad de la Información.

En el período de Junio-Julio del 2014 la alta dirección de la institución aprueba y publica la política de seguridad de la información acorde a lo solicitado por el esquema Gubernamental de Seguridad de la Información (EGSI), asignando los recursos administrativos y económicos necesarios para la aplicación de la misma.

Se planificaron reuniones con las personas encargadas de cada departamento en la oficina matriz ubicada en Quito, para el levantamiento de los datos, de acuerdo a la metodología establecida, esta investigación se realizó en 3 días laborables, en periodos de tiempos distintos, ya que dependíamos de la disponibilidad de horarios de los servidores públicos.

A la fecha de inicio de la presente investigación la institución informa que el estado de implementación de controles es avanzado de acuerdo al EGSI, por lo que el objetivo será conocer cuan madura es la organización en relación a la gestión de la seguridad de la información, para lo cual se analiza los resultados de las once variables propuestas por la metodología.

4.4.1 Variable 1: Política de seguridad

Los resultados obtenidos respecto a la política de seguridad se muestran a continuación:

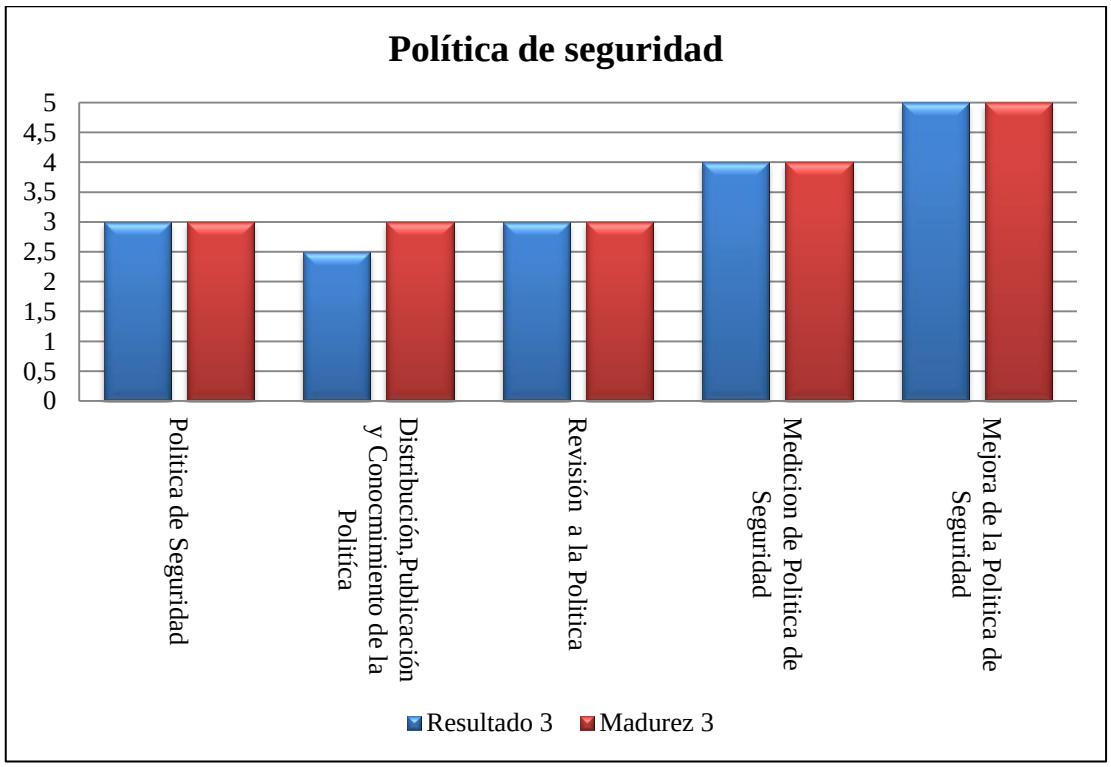

Figura 53: Política de seguridad – Caso 3.

- ✓ **Política de seguridad (3/3):** De acuerdo a la madurez propuesta para cada indicador, los resultados obtenidos nos indican que la institución dispone de una política de seguridad de la información documentada situándola en el punto óptimo de escala de madurez.

- ✓ **Distribución, publicación y conocimiento de la política (2.5/3):** Se pudo evidenciar que la misma está siendo distribuida y publicada sin embargo los funcionarios de la institución no disponen de un conocimiento completo de la misma.

- ✓ **Revisión de la política (3/3):** La institución ha revisado la política de seguridad de la información en base a las necesidades y a las mediciones que realiza de la misma.

- ✓ **Medición de la política (4/4) y mejora de la política de seguridad (4/4):** Durante la investigación de campo se determinó que la institución dispone de indicadores de gestión de la política de seguridad de la información, y existen planes de mejora de la misma.

- ✓ **Estado de madurez de la variable política de seguridad:** El estado de madurez obtenida en esta variable es de 5,83 que la sitúa dentro de la escala de madurez en el nivel cinco, lo cual indica que está siendo *Optimizada*, la gestión de los procesos.

4.4.2 Variable 2: Organización de la seguridad de la información

Los resultados obtenidos respecto a la organización de la seguridad de la información se muestran a continuación:

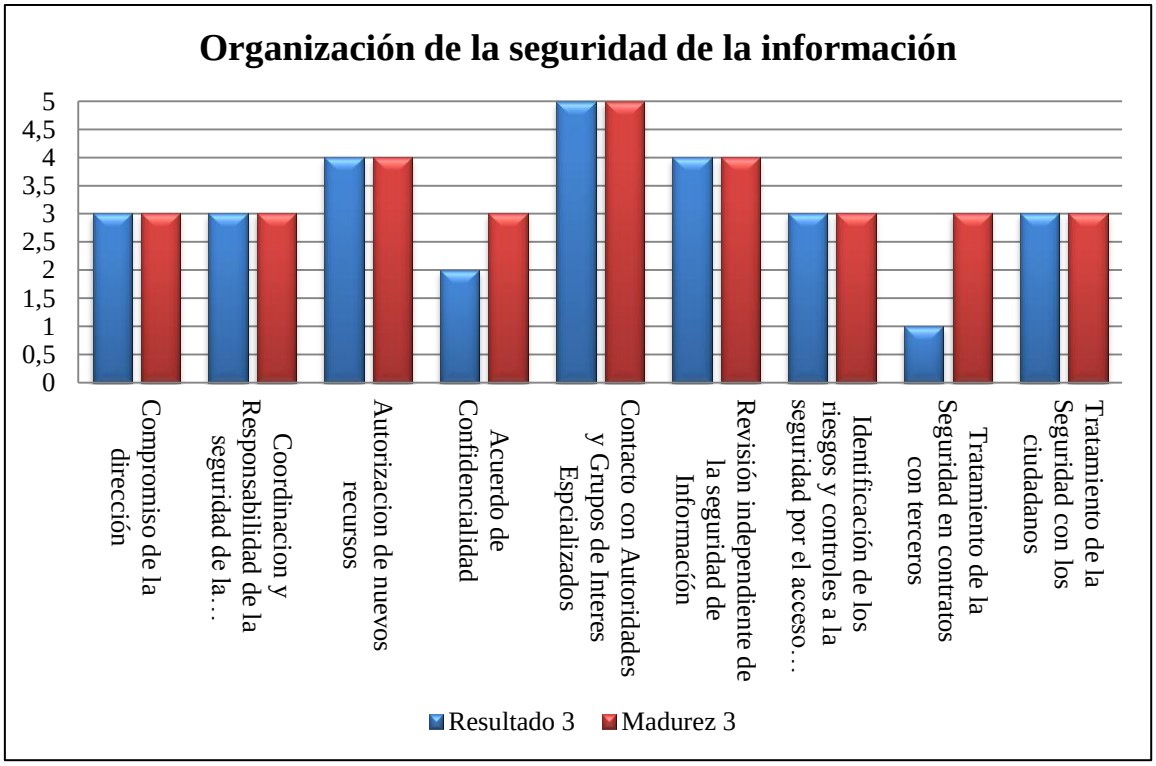

Figura 54: Organización de la seguridad de la información – Caso 3.

- ✓ **Compromiso de la dirección (3/3):** Existe un compromiso por parte de la dirección a través de acuerdos formales y asignación de recursos, llegan a su tope óptimo ya que las responsabilidades referentes a la seguridad de la información se encuentran definidas.

- ✓ **Coordinación y responsabilidad de la seguridad de la información (3/3):** Se pudo evidenciar que la coordinación de las actividades referentes a la seguridad de la información entre los diferentes departamentos, se encuentra plenamente coordinada lo cual le ubica en un nivel de madurez alto.

- ✓ **Autorización de nuevos recursos (4/4):** La institución dispone de un procedimiento formal y definido para autorizar el uso de nuevos recursos de tratamiento de la información, por lo que su nivel de madurez es el óptimo.

- ✓ **Acuerdos de confidencialidad (2/3):** La institución dispone de acuerdos de confidencialidad con todos los actores involucrados, los cuales no han sido revisados desde su firma.

- ✓ **Contacto con autoridades y grupos de interés especializados (4/4):** La institución mantiene contacto con profesionales o entidades especializadas en el área de seguridad de la información, así como con autoridades competentes para tratar temas relacionados con la seguridad de la información, llevando una gestión proactiva con respecto a temas de seguridad de la información.

- ✓ **Revisión independiente de la seguridad de información (4/4):** La institución realiza constantes auditorias y/o análisis de la seguridad de la información por parte de terceras personas o empresas, para asegurar una opinión imparcial con respecto a la seguridad de la información.

- ✓ **Identificación de los riesgos y controles a la seguridad por el acceso de terceros (3/3):** La institución ha identificado los riesgos provenientes por el acceso a la información por parte de terceros, para lo cual ha implementado controles de acceso lógico a la información, incluyendo controles de acceso a los dispositivos que utilizan terceros para acceder a la información.

- ✓ **Tratamiento de la seguridad en contratos con terceros (1/3):** Las cláusulas contractuales de confidencialidad se incluyen dentro de los contratos con terceros, sin embargo no se toma en cuenta cláusulas sobre la disponibilidad e integridad de la información que pueda ser afectada.

- ✓ **Tratamiento de la seguridad con los ciudadanos (3/3):** Se evidencia que la institución identifica a los ciudadanos y define los perfiles de acceso a la

información, por lo que logra un nivel óptimo en la aportación a la madurez de la variable.

- ✓ **Estado de madurez de la variable organización de la seguridad de la información:** El estado de madurez obtenida en esta variable es de 5,42 que la sitúa dentro de la escala de madurez en el nivel cinco, lo cual indica que dispone de procesos *Optimizados*, centrados en la mejora de los procesos.

4.4.3 Variable 3: Gestión de activos y clasificación de la información.

Los resultados obtenidos respecto a la gestión de los activos y la clasificación de la información se muestran a continuación:

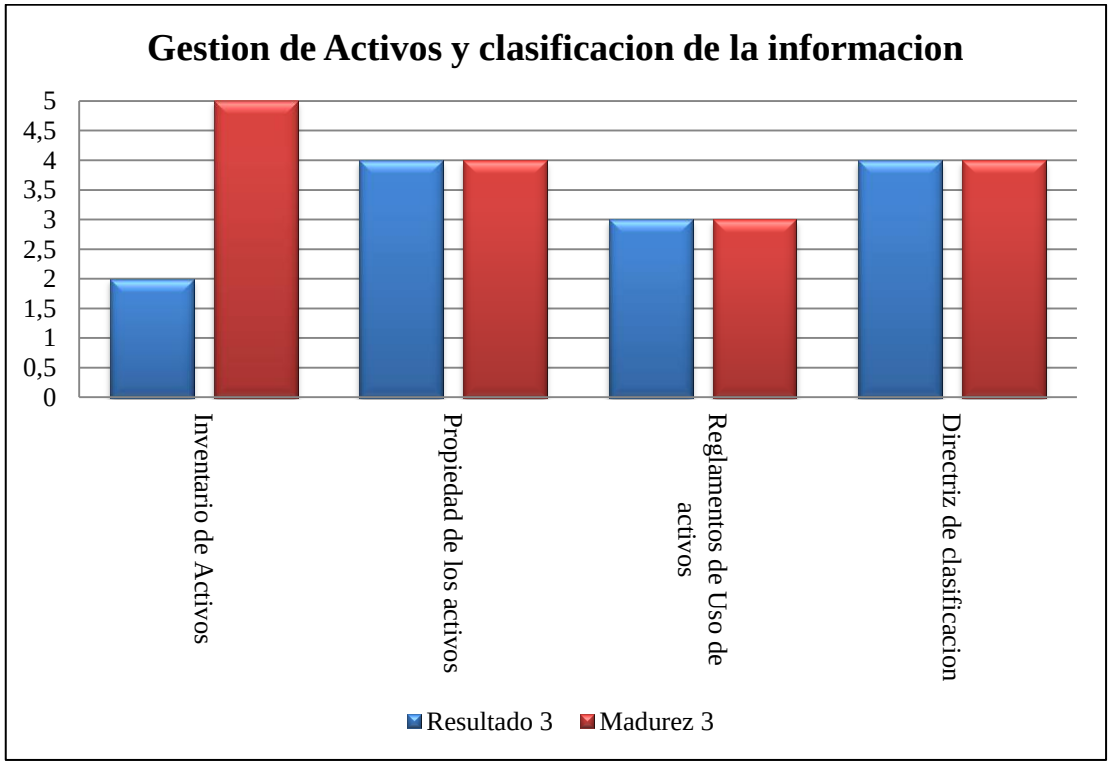

Figura 55: Gestión de activos y clasificación de la información – Caso 3.

- ✓ **Inventario de Activos (2/5) - Propiedad de los activos (4/4) - reglamento de uso de activos (3/3):** Se determina que la institución mantiene un control sobre el inventario de los activos, sin embargo se lleva manualmente el proceso y no disponen de una herramienta especializada para control del mismo, está claramente

definida las propiedad de cada uno de los activos y disponen de reglamento para el uso de los mismos, documentado e implementado el proceso dentro de la institución. También mantienen un proceso de sociabilización constante del mismo.

- ✓ **Directriz de clasificación (4/4):** Se puede evidenciar que la institución dispone de directrices de clasificación de la información definidas e implementadas

- ✓ **Estado de madurez de la variable gestión de activos y clasificación de la información:** El estado de madurez obtenida en esta variable es de 4,88 que la sitúa dentro de la escala de madurez en el nivel cuatro, lo cual indica que dispone de procesos *Gestionados Cuantitativamente.*

4.4.4 Variable 4: Seguridad en recursos humanos

Los resultados obtenidos respecto a la seguridad en recursos humanos se muestran a continuación:

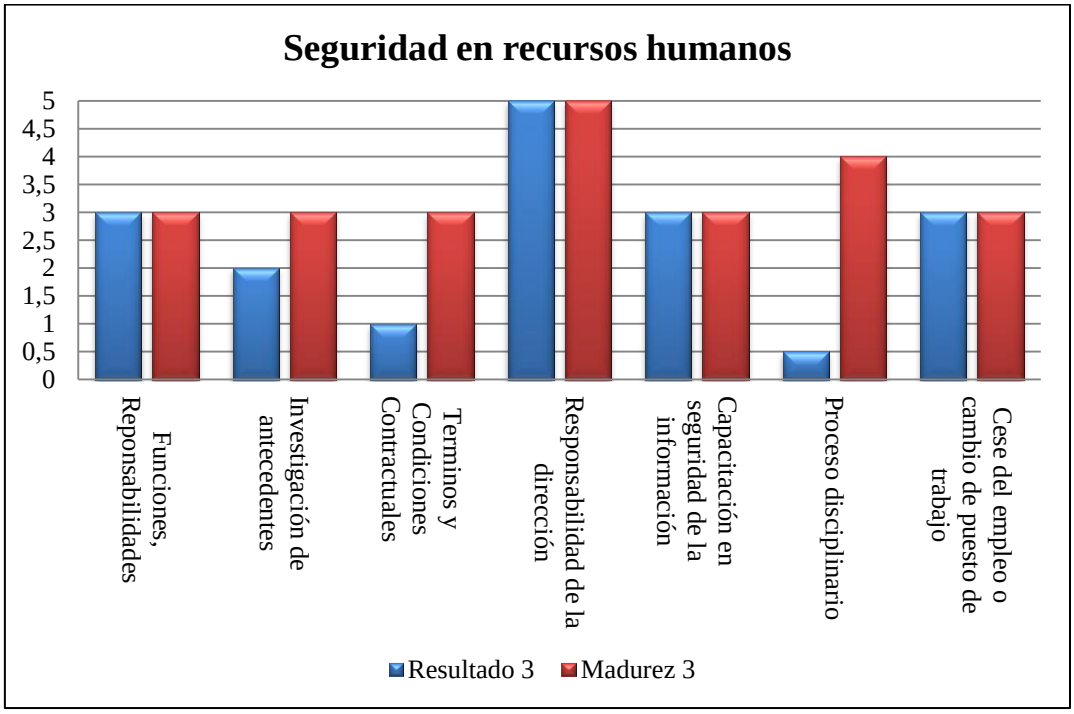

Figura 56: Seguridad en recursos humanos – Caso 3.

- ✓ **Funciones y responsabilidades (3/3) – Investigación de antecedentes (2/3):** La institución mantiene definidas las funciones y responsabilidades previas al empleo de un actor, sin embargo se denota una falta de investigación de los antecedentes previo al empleo, la institución verifica los antecedentes laborales y antecedentes penales, sin embargo no se realizan pruebas conductuales.

- ✓ **Términos y condiciones contractuales (1/3):** Referente a los términos y condiciones contractuales con los actores involucrados, se puede determinar que la institución no está incluyendo cláusulas en los contratos que precautelan la confidencialidad, integridad y disponibilidad de la información que manejarán los actores, se basa solo en acuerdos de confidencialidad firmados.

- ✓ **Responsabilidad de la dirección (5/5):** La dirección al estar comprometida con la implantación del EGSI, solicita mediciones regulares de la aplicación de la política y procedimientos, solicita informes de cumplimiento de políticas y procedimientos y toma decisiones en base a los indicadores disponibles.

- ✓ **Capacitación en seguridad de la información (3/3):** La institución al momento está en el punto más alto referente a la capacitación de los actores involucrados, en temas relacionados con la seguridad de la información, siendo esta periódica y constante.

- ✓ **Proceso disciplinario (0,5/4):** El departamento de recursos humanos informó que no tiene definido un proceso disciplinario, en el caso de que uno de sus actores provoque un evento de seguridad, solo existen amonestaciones verbales.

- ✓ **Cese de empleo o cambio de puesto de trabajo (0/4):** El departamento de recursos humanos también informó que dispone de un procedimiento formal e implementado para cuando uno de los funcionarios cese o cambien de puestos de trabajo, es decir dicho procedimiento mantiene responsables para recibir las funciones de los funcionarios salientes.

- ✓ **Estado de madurez de la variable seguridad en recursos humanos:** El estado de madurez obtenida en esta variable es de 4,88 que la sitúa dentro de la escala de madurez en el nivel cuatro, lo cual indica que dispone de procesos *Gestionados Cuantitativamente.*

4.4.5 Variable 5: Seguridad física y ambiental

Los resultados obtenidos respecto a la seguridad física y ambiental se muestran a continuación:

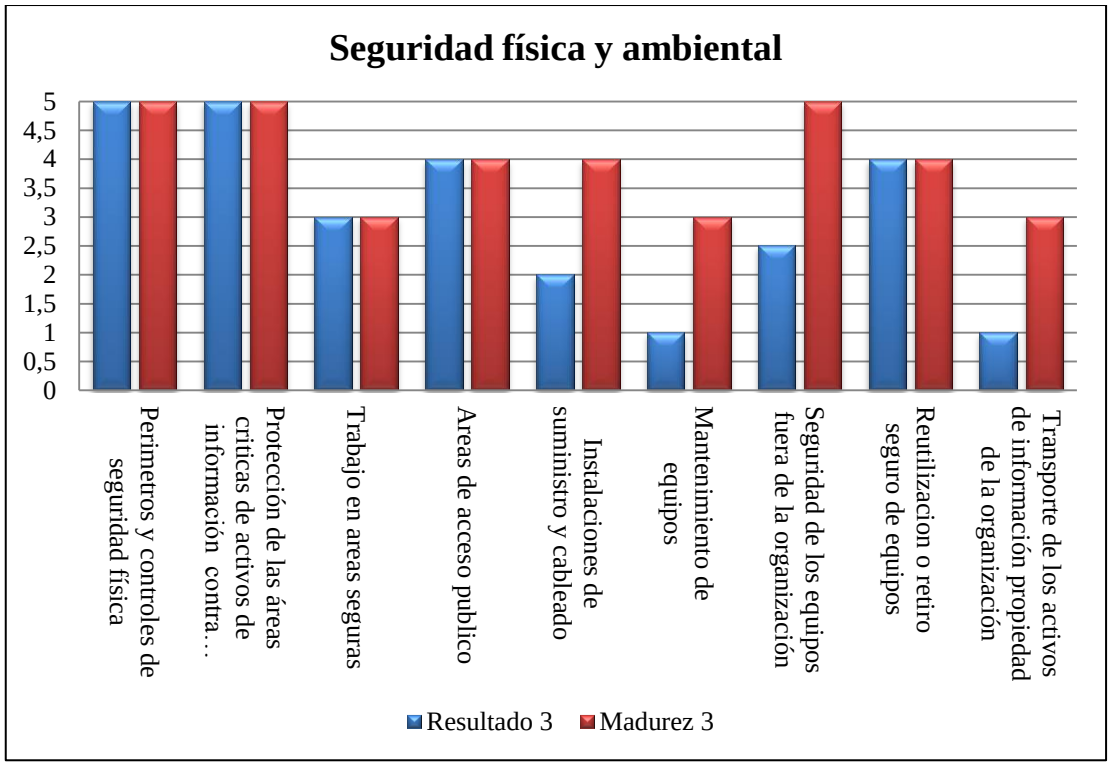

Figura 57: Seguridad física y ambiental – Caso 3.

- ✓ **Perímetros y controles de seguridad física (5/5):** En la institución se mantiene un control óptimo de los perímetros de las instalaciones así como de los controles de seguridad física de las instalaciones.

- ✓ **Protección de las áreas críticas de activos de información contra amenazas externas y de origen ambiental (5/5):** Con respecto a la protección de las áreas críticas de tratamiento de la información, estas cuentan con los controles

necesarios para asegurar la información en caso de desastres naturales o provocados por el hombre.

- ✓ **Trabajo en áreas seguras (3/3):** El trabajo en áreas seguras esta normado por un documento de política de seguridad industrial, el mismo que se encuentra implementado para proteger a las personas y zonas críticas (área de servidores) de posibles incidentes de seguridad

- ✓ **Áreas de acceso público (4/4):** Se puede evidenciar que desde las áreas de acceso público hacia las privadas de la institución, se encuentran debidamente protegidas por sistemas de seguridad (puestos de vigilancia controles de acceso físicos y lógicos) implementados par el efecto.

- ✓ **Instalaciones de suministro y cableado (2/4):** La institución dispone de una fuente alterna de energía en caso de fallas de la misma que asegura la disponibilidad de la información, sin embargo no cuenta con bancos de energía que den soporte hasta la puesta en marcha de la fuente alterna, se evidencia que disponen de cableado estructurado el mismo que recibe el mantenimiento debido de acuerdo a los cambios físicos realizados en la institución.

- ✓ **Mantenimiento de equipos (1/3):** Como se aprecia en el gráfico la institución cuenta solo con un plan correctivo para los equipos, al no disponer de un plan preventivo se solucionan los problemas sobre la marcha, lo cual lleva a un nivel de madurez bajo a este indicador.

- ✓ **Seguridad de los equipos fuera de la organización (2,5/5):** En la seguridad física de los equipos fuera de las áreas seguras de la institución, se evidencia que se los protegen por medio de contraseñas y encriptación de datos para proteger la confidencialidad de los mismos, sin embargo si los equipos son robados no disponen de un proceso de trazabilidad que permita recuperar o ubicar los equipos.

- ✓ **Reutilización o retiro seguro de equipos (4/4):** Con respecto a la reutilización o retiro seguro de equipos, en este indicador se mide la forma en la que se destruye

los datos de equipos que van a ser reutilizados, se verificó que la institución realiza este proceso con técnicas de sobre-escritura, seguras para no permitir la recuperación indeseada de datos afectando la confidencialidad de los mismos, por lo cual se obtiene un nivel de madurez alto.

- ✓ **Transporte de los activos de información propiedad de la organización (1/3):** La institución dispone de un proceso verbal para el transporte de los activos de la información propiedad de institución, por lo que se sitúa este indicador en un nivel bajo.

- ✓ **Estado de madurez de la variable seguridad física y ambiental:** El estado de madurez obtenida en esta variable es de 4,58 que la sitúa dentro de la escala de madurez nivel cuatro, lo cual indica que dispone de procesos *Gestionados Cuantitativamente.*

4.4.6 Variable 6: Gestión de comunicaciones y operaciones

Los resultados obtenidos respecto a la Gestión de Comunicaciones y Operaciones se muestran a continuación:

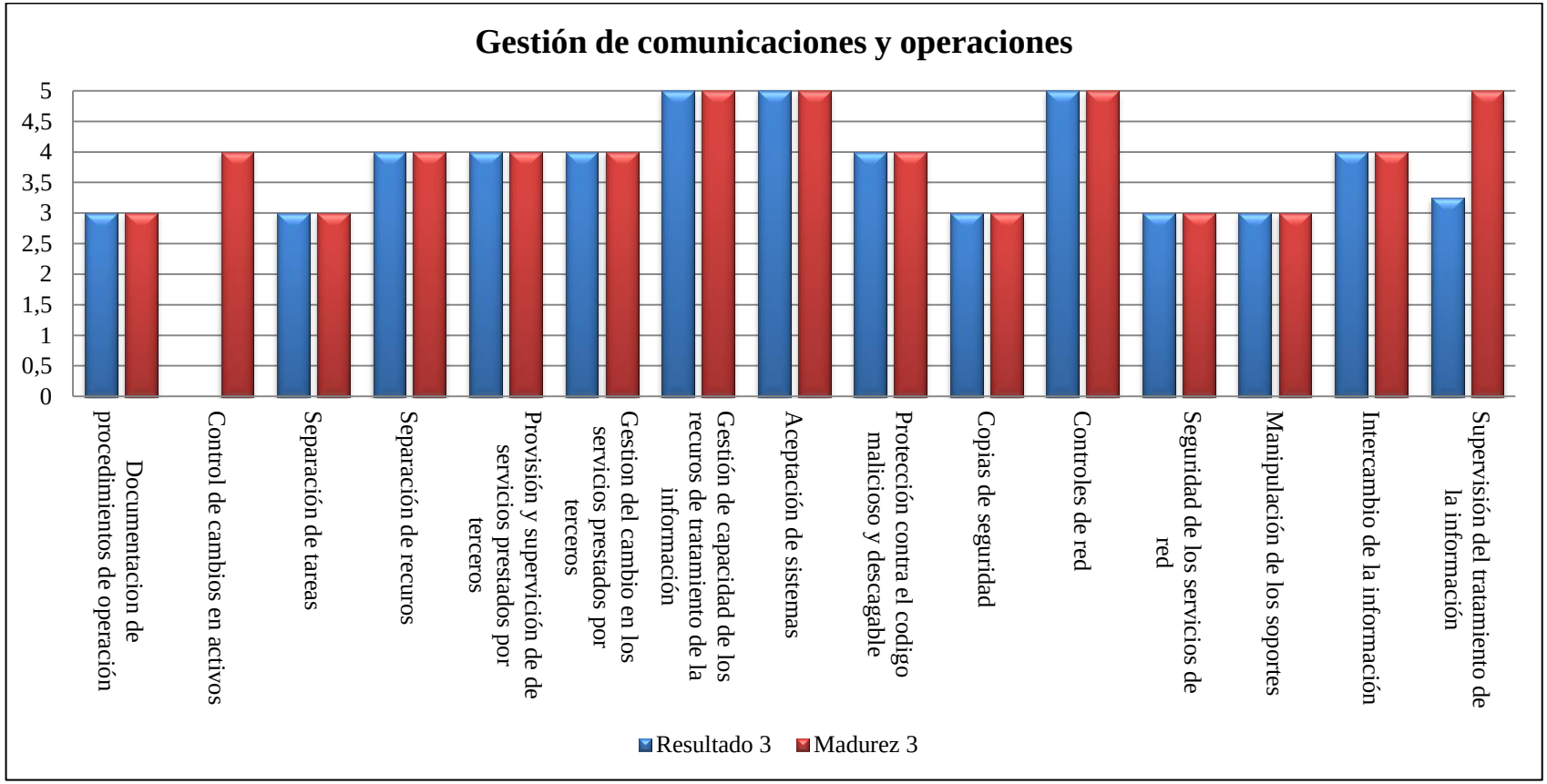

Figura 58: Gestión de comunicaciones y operaciones – Caso 3.

- ✓ **Documentación de procedimientos de operación (3/3):** La institución mantiene de manera documentada los manuales de operación de los distintos sistemas de información, dichos manuales se encuentran a disposición de los usuarios y se los mantienen actualizados.

- ✓ **Control de cambios en activos (4/4):** Se evidencia que para los cambios realizados sobre los activos de información no disponen de un procedimiento formal, en el cual dichos cambios no son documentados ni se lleva un registro de versionamiento sobre los mismos, llevando este indicador a un nivel nulo de gestión.

- ✓ **Separación de tareas (3/3):** Dentro de la institución se tienen claramente identificadas las tareas y responsabilidades para el tratamiento de la información, dichas responsabilidades recaen sobre funcionarios como el administrador de base de datos, el administrador de infraestructura, el jefe del área de desarrollo, etc.

- ✓ **Separación de recursos (4/4):** Dentro del departamento que maneja la infraestructura de la institución, se pudo evidenciar que los recursos de tratamiento de la información se encuentran separados en diferentes ambientes, los mismos que son: producción, desarrollo, pruebas y capacitación.

- ✓ **Provisión y supervisión de servicios prestados por terceros (4/4):** La institución cuando adquiere servicios prestados por terceros, dispone de un procedimiento para validar periódicamente que estos servicios cumplan con las expectativas requeridas, en dicho procedimiento se encuentran acuerdos de calidad de servicios, auditoras planificadas, etc.

- ✓ **Gestión del cambio en los servicios prestados por terceros (4/4):** La institución dispone de uno o más de estos procedimiento para gestionar los cambios en los servicios prestados por terceros, cuando estos se realizan se llevan a cabo controles como revisión a la política de seguridad, revisión a los procedimientos de seguridad, revisión de controles de seguridad, reevaluación de los riegos, llevando a esta variable a un nivel de madurez óptimo.

- ✓ **Gestión de capacidad de los recursos de tratamiento de la información (5/5):** La institución dispone de una planificación anual en donde se proyecta los futuros incrementos de recursos para el tratamiento de la información, permitiendo así garantizar el rendimiento requerido por los sistemas de información.

- ✓ **Aceptación de sistemas (5/5):** El procedimiento de aceptación de nuevos sistemas de información o modificaciones a los existentes realizadas por terceros, se los realiza a través de los Términos y Referencias (TDR) del proyecto, adicionalmente este procedimiento incluye fases de pruebas durante el desarrollo o modificación de los sistemas y una fase adicional de pruebas previa a la aceptación de los nuevos sistemas de información, así como la actualización o mejoras futuras de dichos sistemas están siendo contemplados, razón por la cual el indicador llega a su punto óptimo.

- ✓ **Protección contra el código malicioso y descargable (4/4):** La protección para las terminales de los usuarios en la institución está siendo gestionada de manera correcta, ya que disponen de sistemas de seguridad que controlan todo lo relacionado con virus, malware, y spam. Los usuarios están en constante capacitación para reconocer y evitar riesgos provenientes del internet. Por otro lado, los usuarios de los terminales tienen una estricta restricción que nos les permite instalar o ejecutar software no autorizado.

- ✓ **Copias de seguridad (3/3):** El departamento encargado del área de infraestructura supo indicar que disponen de un procedimiento formal para realizar copias de seguridad de la información, también disponen de un procedimiento para probar si dichas copias de seguridad son cien por ciento funcionales, por lo que el indicador llega a su punto óptimo.

- ✓ **Controles de red (5/5):** Las redes de comunicaciones en la institución se encuentran gestionadas por el administrador de red, con la ayuda de hardware especializado para el control de la misma, una tarea importante como el monitoreo del tráfico de la red está siendo implementado dentro de la gestión, por tanto el indicador llega a su punto óptimo.

- ✓ **Seguridad de los servicios de red (3/3):** Los servicios de red tales como telefonía ip, correo electrónico, sistemas de información, etc., que expone la institución a los actores involucrados, se encuentran identificados y documentados, los requisitos relacionados a la seguridad de cada servicio se encuentran siendo identificados y documentados, razón por la cual el indicador llega su punto óptimo.

- ✓ **Manipulación de los soportes (3/3):** La institución se encuentra gestionando la manipulación de soportes de almacenamiento en todas las terminales de usuario, al momento los usuarios tienen estrictos controles para insertar memorias flash, CD-ROM, etc., existen procedimientos formales para retirar un medio de soporte y existe un responsable de la manipulación, custodia y almacenamiento de los soportes.

- ✓ **Intercambio de la información (4/4):** La institución dispone de procedimientos formales para entregar o intercambiar información con los actores involucrados, dicho procedimiento incluye formularios de solicitud de información y uso de protocolos seguros para el intercambio electrónico (mail) de la información, se utilizan medidas de encriptación para protegerla, llevando este indicador al punto óptimo de la escala de madurez.

- ✓ **Supervisión del tratamiento de la información (3,25/5):** La institución realiza auditorías a las actividades de tratamiento de información de los actores involucrados, también realizan revisiones de los registros de auditoria de los sistemas, se registran las actividades realizadas en los sistemas, se registran excepciones generadas por el usuario, se registran eventos de seguridad, se mantienen los registros históricos y se registran las actividades de los administradores de sistemas. Sin embargo no disponen de medidas de seguridad y procesos para evitar la manipulación de registros, no analizan los resultados de las actividades de los sistemas y por ende no se sugieren cambios basados en los resultados de los mismos.

- ✓ **Estado de madurez de la variable gestión de comunicaciones y operaciones:** El estado de madurez obtenida en esta variable es de 5,36 que la sitúa dentro de la escala de madurez en el nivel cinco, lo cual indica que dispone de procesos *Optimizados,* y se encuentran centrados en la mejora de los procesos.

4.4.7 Variable 7: Control de accesos

Los resultados obtenidos respecto a los controles de acceso se muestran a continuación:

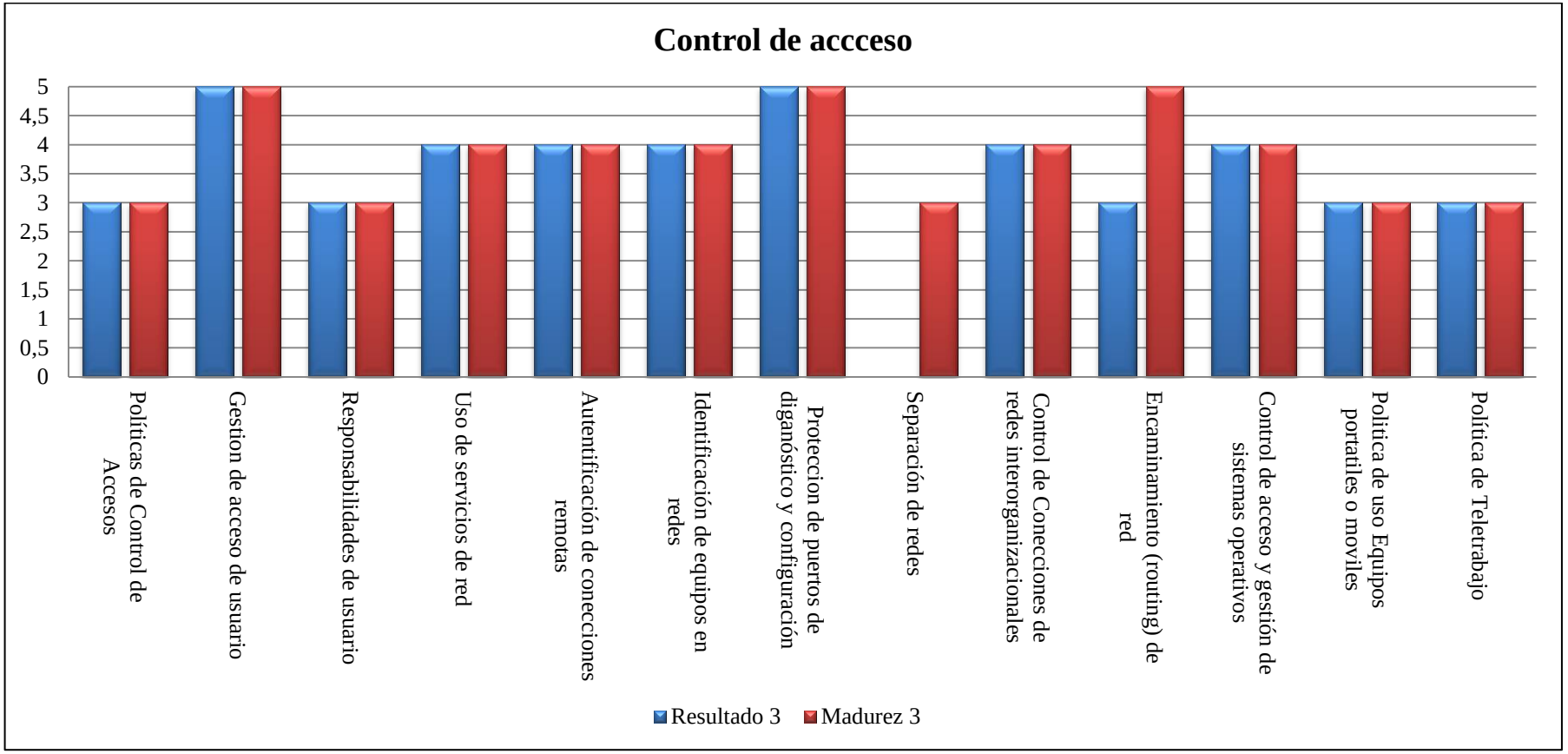

Figura 59: Control de accesos – Caso 3.

- ✓ **Políticas de control de accesos (3/3):** La institución dispone de una política formal de control de accesos para normar los mismos, disponen de un documento formal de política, esto le permite llegar a un nivel óptimo al indicador.

- ✓ **Gestión de acceso de usuario (5/5):** Como se aprecia en el gráfico la institución mantiene gestionado e implementado todos los objetivos de control solicitados por la norma NTE/ISO-27001:2011, para prevenir el acceso no autorizado a los sistemas de información.

- ✓ **Responsabilidades de usuario (3/3):** Se determina que las responsabilidades de los usuarios con respecto a la seguridad referente al acceso a la información, están siendo cumplidas a cabalidad, las mismas fueron corroboradas con técnicas de observación que permiten situar a este indicador en el nivel óptimo.

- ✓ **Uso de servicios de red (4/4):** Se verifica que en el uso de los servicios de red, la institución dispone de reglas que norman el acceso a los servicios autorizados a los usuarios, con este control y gestión se sitúa el indicador en un nivel óptimo.

- ✓ **Autentificación de conexiones remotas (4/4):** Se determinó que la institución cuenta con métodos seguros de autentificación de conexiones remotas (conexiones seguras remotas VPN, envío/recepción de correos smtps/pop3s, administración de dispositivos ssh, encriptación wpa2 en conexiones inalámbricas, uso de HTTPS para aplicativos, transferencia de archivos por FTPS).

- ✓ **Identificación de equipos en redes (4/4):** La institución tiene claramente definido el proceso de autentificación de los equipos en las distintas redes a las que los usuarios tienen acceso, así como su segmentación de acuerdo a la criticidad o a la actividad realizada.

- ✓ **Protección de puertos de diagnóstico y configuración (5/5):** Se dispone de un inventario de puertos de diagnóstico y configuración y existen los controles necesarios para dar un seguimiento a los mismos.

- ✓ **Separación de redes (3/3):** La institución no dispone redes separadas (vlans) por grupos de servicios o usuarios. Esto lleva a este indicador a un nivel de gestión nulo.

- ✓ **Control de conexiones de redes inter-organizacionales (4/4):** Disponen de un proceso definido para restringir a los usuarios el acceso a las conexiones a redes entre organizaciones interministeriales, reflejando un control claro en este aspecto.

- ✓ **Encaminamiento (routing) de red (3/5):** La institución dispone de procesos definidos para la revisión y control de rutas de encaminamiento (tracert o routing) que siguen los flujos de información en la organización, sin embargo no valida periódicamente esos datos.

- ✓ **Control de acceso y gestión de sistemas operativos (4/4):** La institución cuenta con una solución integral (tipo Active Directory o LDAP) que abarca la administración de los usuarios, permisos de sistema operativos y límites de sesión, indicando un claro control de acceso y gestión de los sistemas operativos.

- ✓ **Política de uso equipos portátiles o móviles (3/3):** La institución dispone de una política formal que incluyen las medidas de seguridad para la utilización de equipos portátiles o móviles dentro de la institución, la misma se encuentra implementada ubicando este indicador en un nivel de madurez óptimo.

- ✓ **Política de teletrabajo (1/3):** Existe una política formal que describe los procedimientos y actividades a controlar con respecto al teletrabajo, disponen de un documento para solicitar la autorización y acceso a redes privadas virtuales seguras, también se lleva un control de las actividades realizadas dentro de la misma.

- ✓ **Estado de madurez de la variable control de accesos:** El estado de madurez obtenida en esta variable es de 5,40 que la sitúa dentro de la escala de madurez nivel cuatro, lo cual indica que dispone de procesos *Optimizados,* y se encuentran centrados en la mejora de los procesos.

4.4.8 Variable 8: Adquisición, desarrollo y mantenimiento de los sistemas de información

Los resultados obtenidos respecto a la adquisición, desarrollo y mantenimiento de los sistemas de información se muestran a continuación:

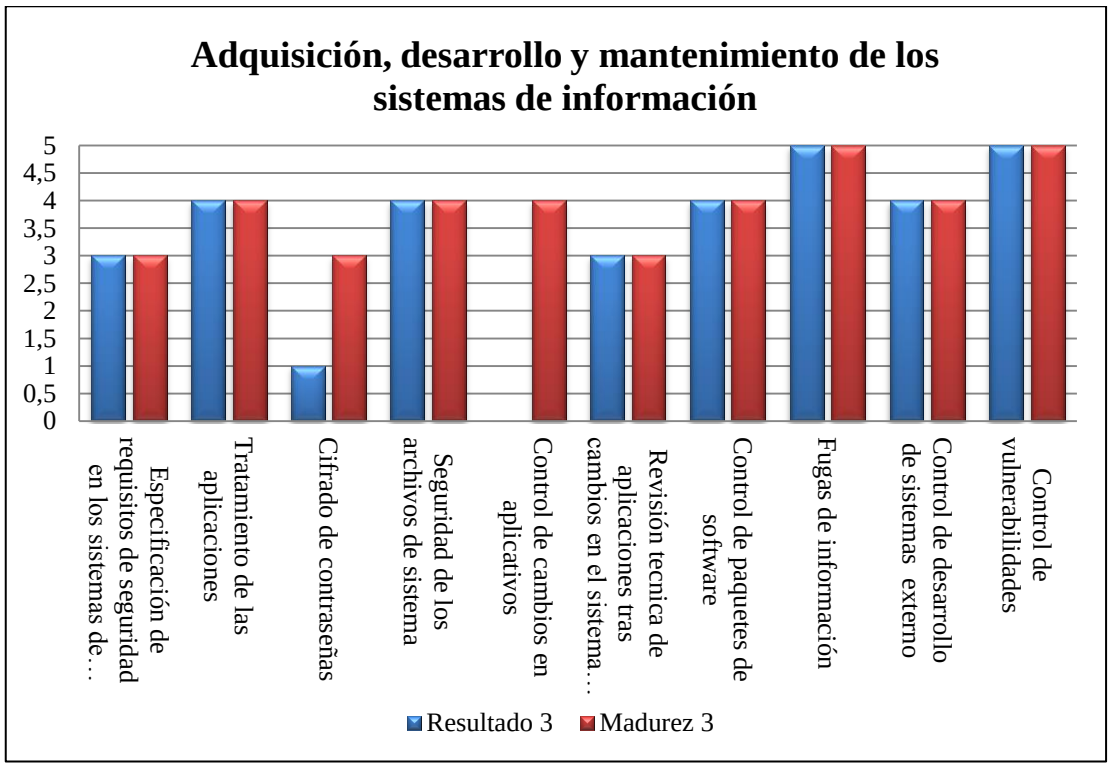

Figura 60: Adquisición, desarrollo y mantenimiento de los sistemas de información – Caso 3.

- ✓ **Especificación de requisitos de seguridad en los sistemas de información (3/3):** Todo nuevo sistema de información o modificación a los existentes, disponen de requisitos de controles de seguridad que se especifican en los términos de referencia (TDR) desarrollados para cada proyecto.

- ✓ **Tratamiento de las aplicaciones (4/4):** La institución dispone de procedimientos para validar que los datos que procesan los sistemas de información sean los adecuados, se cifran las comunicaciones para no comprometer la confidencialidad de la información transmitida entre las terminales y los servidores de la organización, por tanto la madurez del indicador alcanza su nivel óptimo.

- ✓ **Cifrado de contraseñas (1/3):** La institución utiliza métodos estándar para cifrar las contraseñas de los usuarios, el nivel óptimo de este indicador se alcanza cuando se aplican métodos avanzados de seguridad en la encriptación de contraseñas para precautelar la identidad de los usuarios.

- ✓ **Seguridad de los archivos de sistemas (4/4):** La gestión de seguridad referente a los archivos de los sistemas de información es llevada a cabo mediante procedimientos de control durante la instalación o modificación de cualquier software que afecte al mismo, a su vez el acceso al código fuente de dichos sistemas de información es protegido celosamente, la gestión de estos archivos de información cuando alguien solicita una copia es controlada por un procedimiento para verificar qué datos son entregados, por esta razón el indicador llega a su nivel de madurez óptimo.

- ✓ **Control de cambios en aplicativos (0/4):** Una de las debilidades que se mencionó anteriormente es que la institución no mantiene un control de cambios sobre los activos de información, siendo los sistemas de información parte de dichos activos, no existen procedimientos para el control de modificaciones y versionamiento de los mismos.

- ✓ **Revisión técnica de aplicaciones tras cambios en el sistema operativo (3/3):** Es común que los recursos de soporte (servidores o sistemas operativos) para el tratamiento de los sistemas de información tengan que ser actualizados sea por razones de seguridad o rendimiento, para ello la institución dispone de un procedimiento formal para validar que tras dicha actualización los sistemas de información funcionen con normalidad.

- ✓ **Control de paquetes de software (4/4):** Al existir medios y controles tecnológicos para gestionar la instalación y modificación del software en las terminales de toda la institución, está dispone de una hegemonía en el software que utilizan los distintos usuarios de la organización.

- ✓ **Fugas de información (4/4):** La institución ha identificado las potenciales situaciones donde puede ocurrir fugas de información, para ello ha implementado reglas y procedimientos formales para el tratamiento de la información.

- ✓ **Control de desarrollo de sistema externo (4/4):** Se evidencia que la institución dispone registros de control y supervisión del software que se desarrolla externamente.

- ✓ **Control de vulnerabilidades (5/5):** Un punto importante dentro la gestión de la seguridad en los sistemas de información, es conocer las vulnerabilidades asociadas a cada uno de ellos. La institución para identificar las vulnerabilidades asociadas a sus sistemas de información ha contratado los servicios de consultoría para el análisis de vulnerabilidades, a nivel interno se verifica que existe un procedimiento para detectar vulnerabilidades en su sistema de información.

- ✓ **Estado de Madurez de la variable adquisición, desarrollo y mantenimiento de los sistemas de información:** El estado de madurez obtenida en esta variable es de 5,80 que la sitúa dentro de la escala de madurez en el nivel cinco, lo cual indica que dispone de procesos *Optimizados*, y se encuentran centrados en la mejora de los procesos.

4.4.9 Variable 9: Gestión de incidentes de seguridad

Los resultados obtenidos respecto a la gestión de incidentes de seguridad se muestran a continuación:

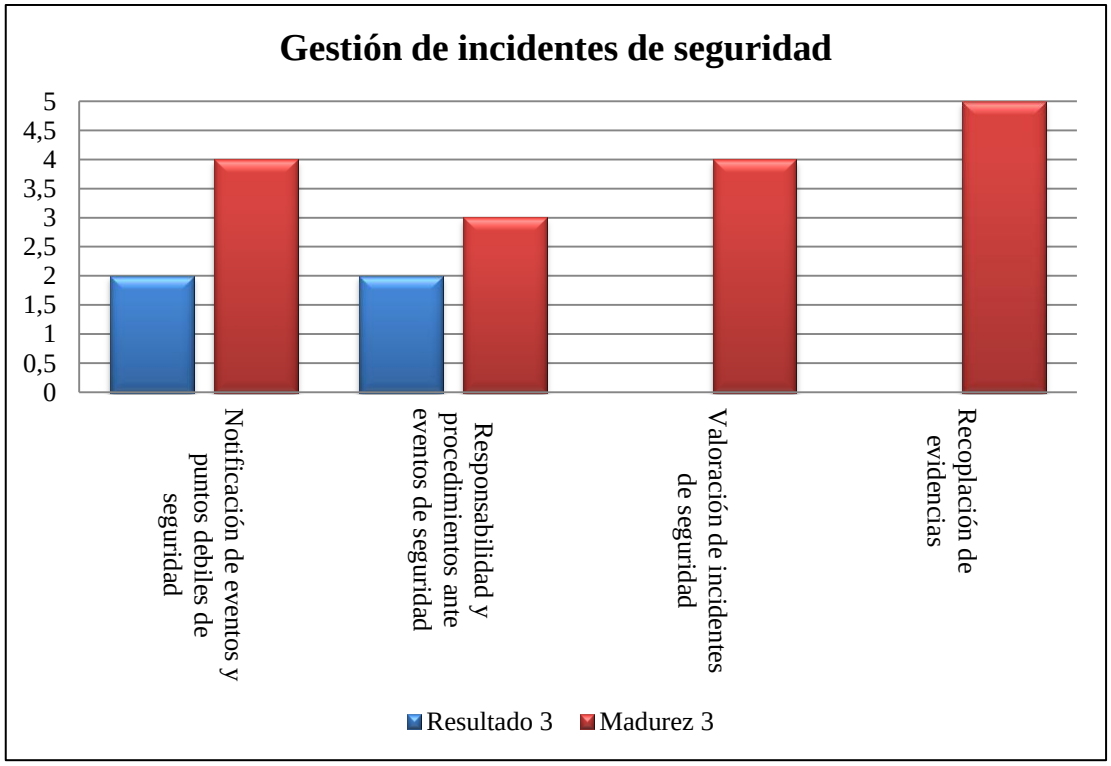

Figura 61: Gestión de incidentes de seguridad – Caso 3.

- ✓ **Notificación de eventos y puntos débiles de seguridad (2/4) - responsabilidad y procedimientos ante eventos de seguridad 2/3) - valoración de incidentes de seguridad (0/4) - recopilación de evidencias (0/5):** Se pudo evidenciar que con respecto a la variable gestión de incidentes de seguridad, los usuarios se encuentran alertados y capacitados para que se notifique cualquier anomalía o evento de seguridad que consideren su ocurrencia, además disponen por parte de la institución un procedimiento formal para la notificación de eventos de seguridad, sin embargo no disponen de un mecanismo para cuantificar un incidente de seguridad, ni tampoco se recopila evidencia, por personal capacitado o personal externo (forense o perito informático), que sustenten un evento de seguridad con el objetivo de tomar acciones civiles o penales.

- ✓ **Estado de madurez de la variable gestión de incidentes de seguridad:** Esto sitúa a los indicadores en un nivel bajo o nulo y por ende a la variable en un estado de madurez de 1,5 que la sitúa dentro de la escala de madurez nivel uno, lo cual indica que el estado de implementación del mismo está en etapa *Inicial*, donde los procesos son pocos controlados y por lo general reactivos.

4.4.10 Variable 10: Gestión de la continuidad del negocio

Los resultados obtenidos respecto a la gestión de la continuidad del negocio se muestran a continuación:

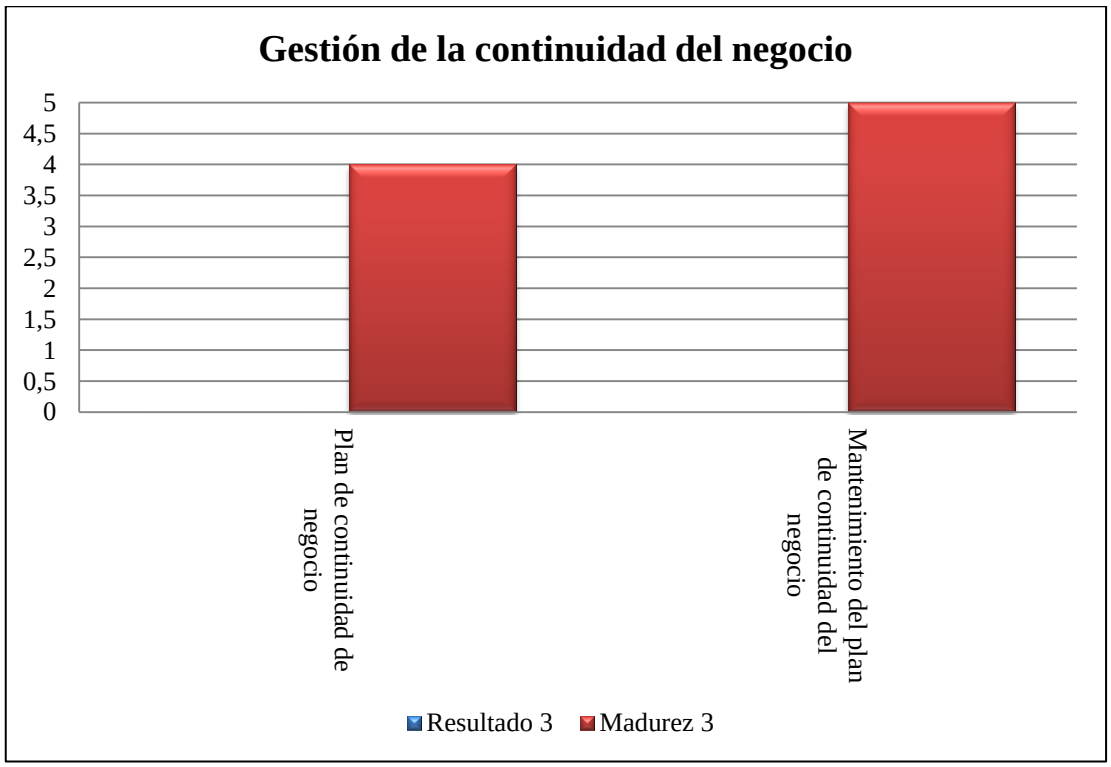

Figura 62: Gestión de la continuidad del negocio – Caso 3.

- ✓ **Plan de continuidad de negocio (0/4) - mantenimiento del plan de continuidad del negocio (0/5):** La institución no cuenta con un plan de continuidad de negocio así como no tiene identificado y evaluados los riesgos que pueden causar las interrupciones del servicio, esta variable desatendida podría ocasionar que se afecte la disponibilidad de la información a todos los actores involucrados con la institución.

- ✓ **Estado de madurez de la variable gestión de la continuidad del negocio:** El estado de madurez obtenida en esta variable es de 0,00 que la sitúa dentro de la escala de madurez nivel cero, lo cual indica que *No dispone de procesos o controles*.

4.4.11 Variable 11: Cumplimiento

Los resultados obtenidos respecto al cumplimiento se muestran a continuación:

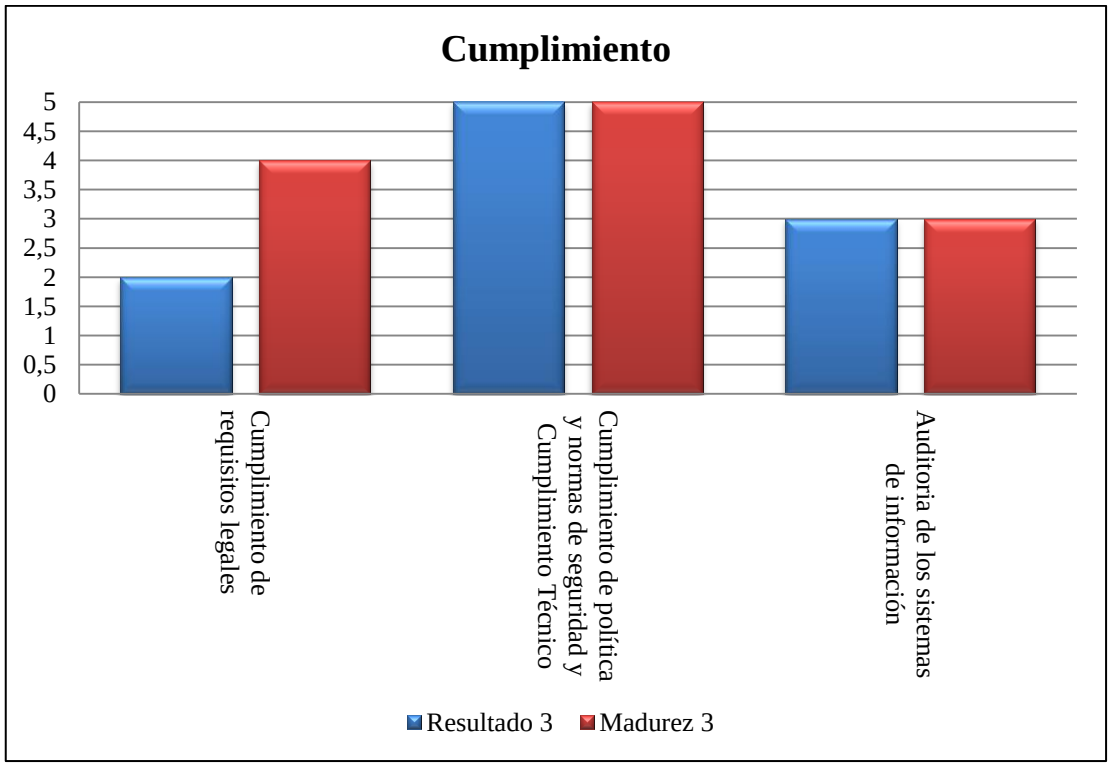

Figura 63: Cumplimiento – Caso 3.

- ✓ **Cumplimiento de requisitos legales (2/4):** Con respecto al cumplimiento de requisitos legales se pudo evidenciar que la institución ha identificado los requisitos legales de seguridad aplicables para los sistemas que utilizan, así como los de propiedad intelectual y uso de productos de software (licencias). También se evidencia que la protección de documentos importantes, se rige a los requisitos legales establecidos contractualmente en la legislación vigente y normativa institucional, referentes a la protección de datos y privacidad de la información y que el giro del negocio lo demanda. Sin embargo, dicho indicador no alcanza su

nivel óptimo de madurez debido a que no se ha sociabilizado las acciones y/o consecuencias del uso indebido de los recursos de tratamiento de información.

- ✓ **Cumplimiento de política y normas de seguridad y cumplimiento técnico (5/5):** La institución en lo referente al cumplimiento de política, normas de seguridad y cumplimiento técnico dispone de procedimientos formales para que los directivos exijan o controlen, que se cumplan con los procesos de seguridad que se encuentran implantándose llevando de esta manera a un nivel bajo al indicador.

- ✓ **Auditoria de los sistemas de información (3/3):** Se aprecia que la auditoria de los sistemas de información se encuentra siendo gestionada de un manera correcta, ya que en las mismas disponen de procesos que calendarizan, planifican y protegen la información levantadas por las auditorias con el fin de evitar impacto técnico por su labor, llevando al indicador a un nivel óptimo.

- ✓ **Estado de madurez de la variable cumplimiento:** El estado de madurez obtenida en esta variable es de 5,00 que la sitúa dentro de la escala de madurez nivel cinco, lo cual indica que dispone de procesos *Optimizados,* y se encuentran centrados en la mejora de los procesos.

4.4.12 Estado de Madurez de la Institución

Una vez analizada la información y obtenida el nivel de madurez de cada una de las once variables, se utiliza la ponderación de las variables como indica la tabla 13, con el fin de realizar un promedio ponderado de los resultados obtenidos en cada variable, que nos permita obtener el nivel de madurez de la calidad de gestión de la seguridad de la información en base a la norma NTE INEN ISO/IEC 27001:2011.

A continuación se muestra el comportamiento de cada una de las variables y su aporte a la madurez en la calidad de gestión de la seguridad de la información:

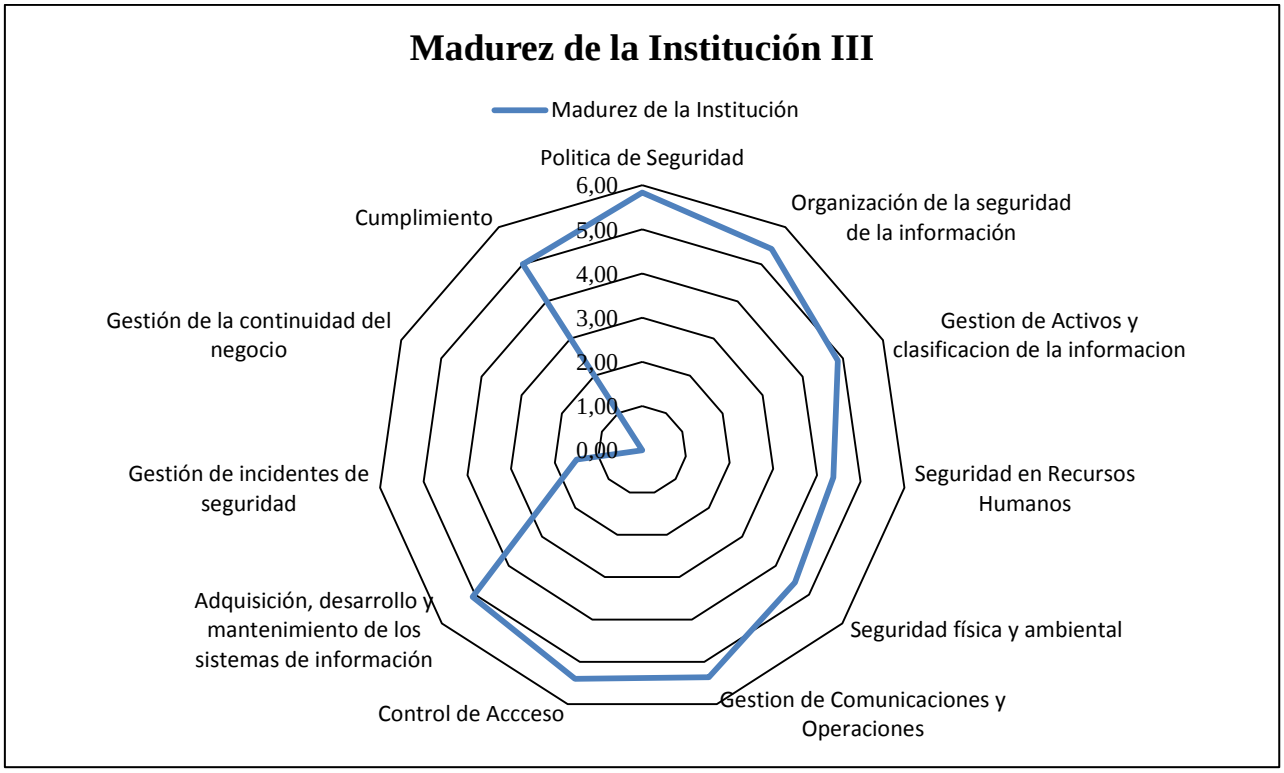

Figura 64: Madurez de la Institución III.

- ✓ **Gestión de la continuidad del negocio (0/5,00) - gestión de incidentes de seguridad (1,00/5,00):** Se observa que existen dos variables que se encuentran en un nivel cero y nivel uno indicando en el primer caso *inexistencia* de gestión y en el segundo caso una gestión *Inicial*, siendo los dos puntos más débiles de la institución.

- ✓ **Seguridad en recursos humanos (4,00/5), seguridad física y ambiental (4,00/5), gestión de activos y clasificación de la información (4,00/5):** Existen tres variables que se encuentra en el nivel de madurez cuatro correspondiente a *Gestionada Cuantitativamente*, es decir se establecen objetivos cuantitativos para medir la calidad y el rendimiento de los procesos, y se los utilizan como criterios de gestión.

- ✓ **Cumplimiento (5,00/5), adquisición, desarrollo y mantenimiento de los sistemas de información (5,00/5), gestión de comunicaciones y operaciones (5,00/5,00), control de acceso (5,00/5,00), organización de la seguridad de la información (5,00/5), política de seguridad (5,00/5):** Este grupo son las que mayor cantidad de variables reúnen, las mismas se encuentran en el nivel cinco, el más alto de la escala de madurez correspondiente a *Optimizada*, donde se mejora continuamente sus procesos basándose en una comprensión cuantitativa de sus objetivos de negocio y necesidades de rendimiento.

- ❖ **Estado Madurez de la Institución Tres.**

A continuación se muestra el resultado de la madurez de cada variable junto a su ponderación:

Tabla 17:

Resultado de variables

N°	Variable	Madurez Variable	Ponderación Variable
1	Política de Seguridad	5,83	4,50
2	Organización de la seguridad de la información	5,42	4,00
3	Gestión de Activos y clasificación de la información	4,88	3,43
4	Seguridad en Recursos Humanos	4,38	4,00
5	Seguridad física y ambiental	4,58	4,00
6	Gestión de Comunicaciones y Operaciones	5,36	4,00
7	Control de Acceso	5,40	3,90
8	Adquisición, desarrollo y mantenimiento de los sistemas de información	5,08	3,93
9	Gestión de incidentes de seguridad	1,50	3,85
10	Gestión de la continuidad del negocio	0,00	3,44
11	Cumplimiento	5,00	3,60

A continuación se aplica el promedio ponderado de acuerdo a la metodología planteada, obteniendo el nivel de madurez de la institución con respecto a la calidad de gestión de la seguridad de la información.

- Resultado del nivel de madurez del caso uno:
  - 4.22 → **Gestionado cuantitativamente**

Figura 65: Nivel de madurez.

La Institución analizada en el caso tres, se encuentra en el nivel de madurez cuatro *Gestionado Cuantitativamente,* lo que significa que los procesos que gestionan la seguridad de la información se manejan con procesos medidos y controlados.

4.5 Análisis comparativo

Una vez obtenidos los resultados de los tres casos evaluados, se procede a comparar de forma cualitativa el resultado de las variables obtenidas para cada caso, con el objetivo de analizar dichos resultados y establecer fortalezas y debilidades en relación a cada variable de los 3 casos de estudio.

Posteriormente se realiza un análisis comparativo de la madurez obtenida en las instituciones objeto de la presente investigación, con el objetivo de determinar el mejor grado de gestión, respecto a la seguridad de la información basada en la norma NTE INEN ISO/IEC 27001:2011.

4.5.1 Comparación de variables

A continuación se muestra un cuadro comparativo de las once variables resultantes de los tres casos estudiados:

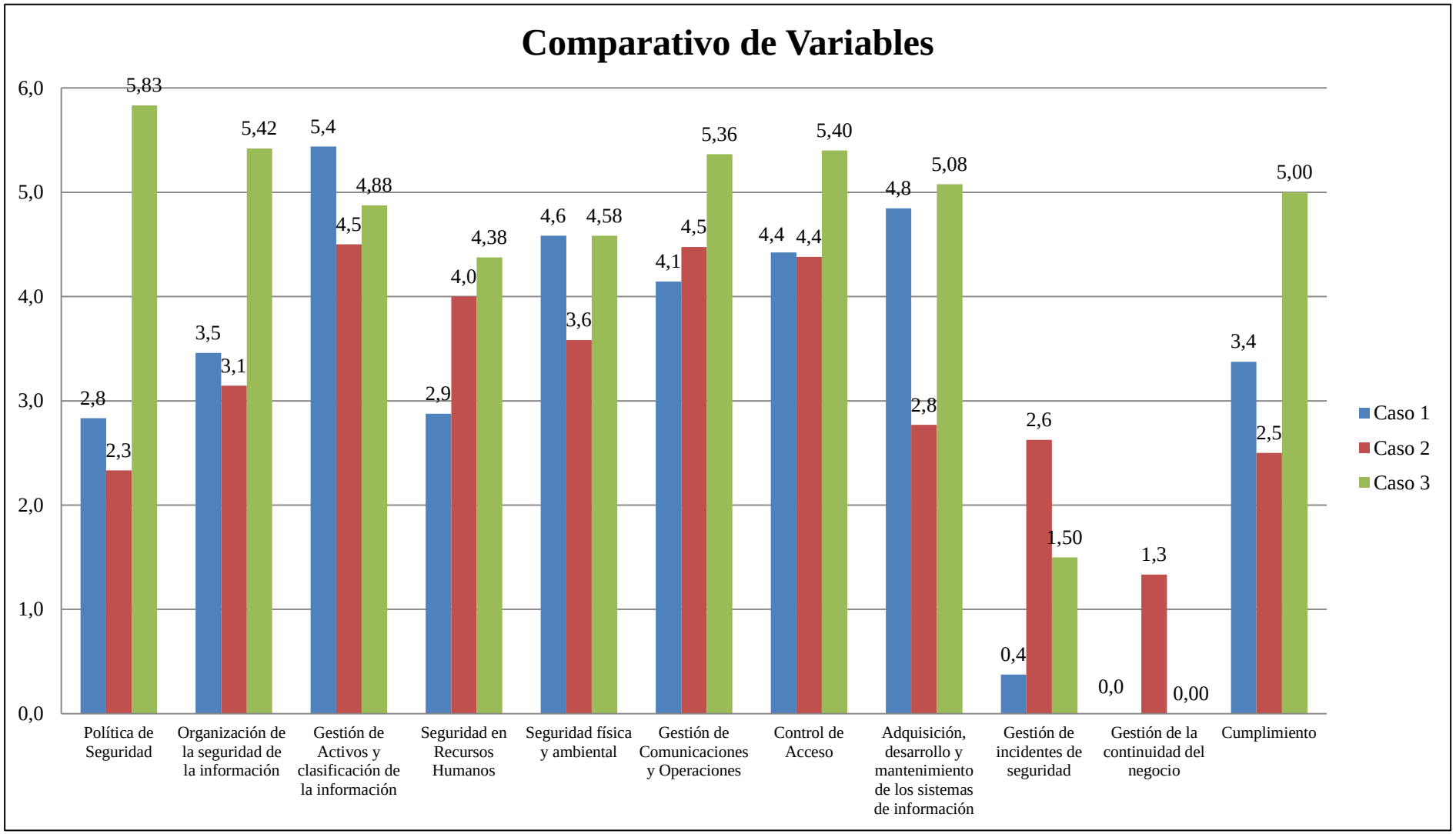

Figura 66: Comparativo de Variables.

- ✓ **Política de seguridad:** Se determina que en esta variable dos instituciones se encuentran en un nivel de madurez dos *(Gestionada),* lo que nos indica que la política de seguridad está siendo gestionada y en base a esta se plantean directrices en el proceso de implementación que sufren dichas instituciones. La tercera institución denota un nivel de madurez cinco *(Optimizada),* que indica que la gestión referente a la política de seguridad se encuentra siendo medida y en base a resultados obtenidos se han implementado acciones de mejora.

- ✓ **Organización de la seguridad de la información:** Se determina que en esta variable dos instituciones se encuentran en un nivel de madurez tres *(Definida),* lo que significa que los procesos para la organización de la seguridad de la información se encuentran estandarizados, permitiendo de esta manera mantener un alineamiento integro de la organización con respecto a la seguridad de la información. La tercera institución denota un nivel de madurez cinco *(Optimizada),* que nos indica que además de mantener estándares para la organización de la seguridad de la información, los mide, analiza sus resultados y de ser el caso toma acciones de mejora

- ✓ **Gestión de activos y clasificación de la información:** De acuerdo a los resultados obtenidos para esta variable, se denota que las instituciones han establecido objetivos cuantitativos para la calidad y el rendimiento de los procesos relacionados con la gestión de los activos y la clasificación de la información, ubicando en el nivel de madurez cuatro *(Gestionado cuantitativamente)* a dos instituciones, adicionalmente la tercera institución se ubica en un nivel de madurez cinco *(Optimizada),* ya que demuestra que toma acciones de mejora, basada en una compresión cuantitativa sobre la gestión realizada.

- ✓ **Seguridad en recursos humanos:** Se pudo observar que en una de las instituciones, la variable en análisis se encuentra siendo *Gestionada* (nivel 2), ya que los procesos se están planificando y ejecutando de acuerdo a la política de seguridad de la información ya establecida. Las otras dos instituciones mantienen un nivel de madurez cuatro *(Gestionado cuantitativamente),* ya que han establecido objetivos cuantitativos y sus decisiones son basadas en los resultados obtenidos.

- ✓ **Seguridad física y ambiental:** Como se puede observar en el gráfico una institución se encuentra en el nivel de madurez tres *(Definida),* lo que significa que los procesos para gestionar la seguridad física y ambiental se encuentran estandarizados, permitiendo de esta manera mantener un alineamiento integro de la institución y siendo su objetivo precautelar la seguridad de la información. Las otras dos instituciones mantienen un nivel de madurez cuatro *(Gestionado cuantitativamente),* ya que disponen de objetivos cuantitativos y sus decisiones de gestión se basan en los resultados obtenidos.

- ✓ **Gestión de comunicaciones y operaciones y controles de accesos:** En los resultados de estas dos variables se aprecia que las instituciones analizadas mantienen un nivel de madurez alto relacionado con la gestión de las comunicaciones y operaciones y controles de accesos, siendo estas áreas consideradas críticas al momento de gestionar la seguridad de la información. Como se puede observar dos instituciones mantienen un nivel de madurez cuatro *(Gestionado cuantitativamente),* ya que disponen de objetivos cuantitativos y sus decisiones de gestión se basan en los resultados obtenidos y la tercera institución se ubica en un nivel de madurez cinco *(Optimizada),* ya que demuestra que toma acciones de mejora.

- ✓ **Adquisición, desarrollo y mantenimiento de los sistemas de información:** Como se puede observar las tres instituciones se encuentran en niveles de madurez distintos, ubicándolas en los niveles de madurez dos, cuatro y cinco *(Gestionada, Gestionada Cuantitativamente y Optimizada).* Teniendo así a una institución que se encuentran planificando y ejecutando sus procesos en base a la política de seguridad de la información, a otra de ellas ya dispone de objetivos cuantitativos y sus decisiones de gestión se basa en los resultados obtenidos y la tercera institución ya se encuentra en un proceso de optimización.

- ✓ **Gestión de incidentes de seguridad:** El resultado obtenido en esta variable por las instituciones denota que existe una falencia en los procesos o en la falta de implementación de controles, ya que en el mejor de los casos una de las instituciones alcanza un nivel de madurez dos (*Gestionada),* en donde sus procesos

y controles están en una etapa de desarrollo y planificación alineadas con la política de seguridad de la información.

- ✓ **Gestión de la continuidad del negocio:** Al igual que la anterior variable, el resultado obtenido por las instituciones denota que es un aspecto desatendido, en el cual no se dispone de una definición formal de procesos y controles con el objetivo de que la información mantenga la continuidad necesaria para el funcionamiento de las instituciones, teniendo así a una de ellas en el nivel de madurez uno *(Inicial),* dependiendo de la heroicidad del personal de la organización, y no del uso de procesos probados.

- ✓ **Cumplimiento:** Para está variable las tres instituciones se ubican en niveles de madurez distintos, ubicando a una de ellas en el nivel de madurez dos *(Gestionada),* otra institución en el nivel de madurez tres *(Definida)* y la tercera institución en un nivel de madurez cinco (*Optimización),* lo que demuestra que el cumplimento relacionado con los aspectos legales, administrativos y técnicos objetos de medición se encuentran en desarrollo, implementación, medición y mejora, acorde a la realidades y necesidades de cada institución.

4.5.2 Comparación de niveles de madurez

A continuación se muestra un cuadro comparativo con el nivel de madurez obtenido, correspondiente a la gestión de la seguridad de la información de los 3 casos estudiados:

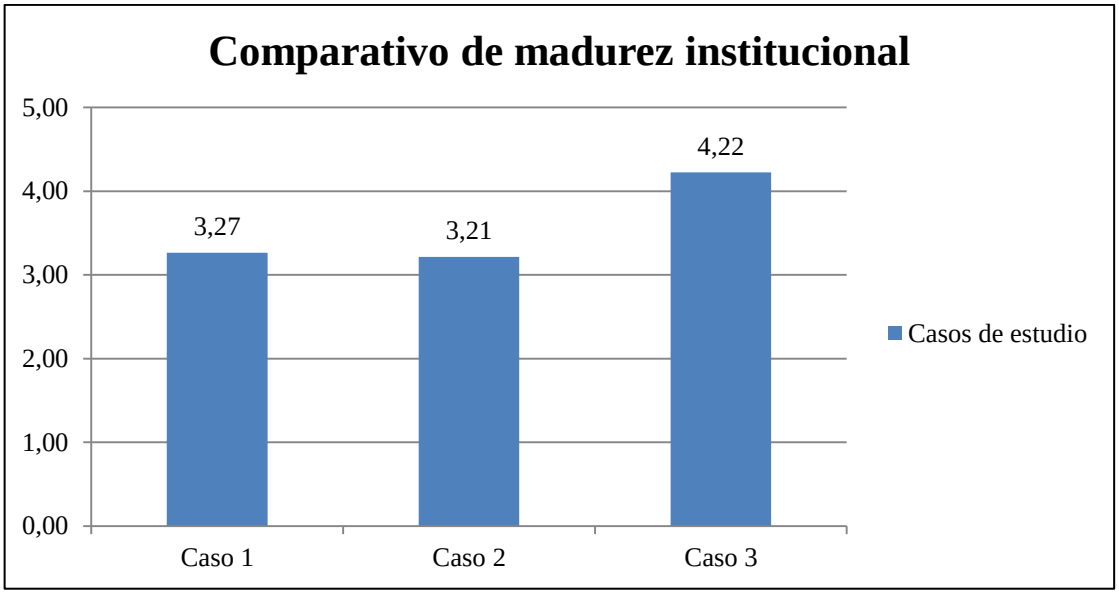

Figura 67: Comparativo de madurez institucional.

Como se puede observar existen dos instituciones que se encuentran en el nivel de madurez tres *(Definida),* lo que significa que los procesos para gestionar la seguridad de la información se encuentran claramente caracterizados y comprendidos, estos procesos son parte de un estándar, donde se mantiene la integridad de la gestión de la seguridad de la información en toda la institución. La tercera institución se ubica en un nivel de madurez cuatro *(Gestionada cuantitativamente),* lo que indica que tiene definidos objetivos cuantitativos para la calidad y el rendimiento de los procesos durante la gestión de la seguridad de la información, la información obtenida de estos objetivos es utilizada como criterios para la toma de decisiones.

Las motivaciones para la implementación de un sistema de gestión de la seguridad de la información en las tres instituciones son distintas, debido a que cada una tiene un objetivo del negocio diferente. Siendo así en el caso uno, la institución de dependencia municipal, actúa de una manera proactiva ya que su objetivo al momento de gestionar la seguridad es establecer una cultura institucional con respecto a la seguridad de la información. En el caso dos, la institución al ser dependiente de la administración pública central, tiene por obligación la implementación del Esquema Gubernamental de Seguridad para la información (EGSI). Finalmente en el caso tres, la institución es también dependiente de la

administración pública central, por tanto su obligación es implementar el EGSI, sin embargo por la criticidad de la información que aglutina, es parte fundamental de su giro del negocio el mantener la gestión de la seguridad de la información en los niveles más altos.

4.6 Validación de la metodología.

La validación de la presente metodología se la realizó junto a los tres Oficiales de Seguridad de la Información de las instituciones analizadas, y por medio de la investigación de campo se pudo concluir que los resultados obtenidos comparados con las mediciones realizadas internamente en cada institución, son muy cercanos a la realidad de cada una de ellas.

Posterior a la ejecución de la investigación de campo existieron reuniones con los tres Oficiales de Seguridad de la Información en cada una de las instituciones, con el fin de presentar los resultados y realizar la validación del instrumento metodológico desarrollado.

El proceso de validación del instrumento desarrollado se basa en una serie de preguntas realizadas a los tres Oficiales de Seguridad de la Información, siendo las siguientes:

1. ¿Informa la finalidad de la investigación?
2. ¿Se asegura la confidencialidad de la información entregada?
3. ¿El número de interrogantes planteadas son las adecuadas?
4. ¿Las respuestas de cada interrogante son apropiadas?
5. ¿Respecto a la codificación de las variables e indicadores están de acuerdo?
6. Recomendaciones generales para el instrumento metodológico.

Posteriormente se analizó los resultados cada una de estas preguntas.

Respecto a la finalidad de la investigación todos los Oficiales de Seguridad coincidieron que mediante la aplicación del presente instrumento, es posible medir el nivel de calidad de gestión en la seguridad de la información en instituciones públicas, el mismo que al estar

basado en la norma NTE INEN –ISO/IEC 27001:2011, permite que los resultados se encuentren alineados a los estándares de gestión internacionales para la seguridad de la información.

Es importante destacar que se mantuvo una estricta confidencialidad con la información entregada por parte de las instituciones, en donde los Oficiales de Seguridad de la Información tuvieron la confianza de entregar la información requerida previa a la autorización de las autoridades y la firma de acuerdos de confidencialidad por parte del investigador. Los oficiales indicaron que firmar acuerdos de confidencialidad se debe extender a todo ambito en las instituciones, cuando se entrega información a terceros.

Con respecto al instrumento aplicado en las instituciones, los Oficiales de Seguridad de la Información indicaron que la entrevista aplicada era extensa, sin embargo al estar basado en un conjunto de objetivos de control y controles de la norma NTE INEN –ISO/IEC 27001:2011, estaba justificado el número de interrogantes planteadas, siendo las mismas necesarias para conocer si la gestión de la seguridad de la información era la adecuada en las instituciones.

La metodología propuesta permite medir la gestión de la seguridad de la información a través de la respuesta de un grupo de interrogantes, los oficiales de seguridad de la información y las personas entrevistadas estuvieron de acuerdo con las opciones de respuestas presentadas, sin embargo cada institución dispone de métodos y procedimientos de gestión para aplicar los controles a la información, siendo estos válidos y no contemplados en el instrumento desarrollado, por lo se agregaron estos métodos de gestión y se ajustaron a la realidad.

Como parte esencial de la metodología desarrollada se encuentran la valoración de las variables e indicadores ya que a través de estos se puede determinar el nivel de madurez de la organización que mantiene con respecto a la gestión de la seguridad de la información. A continuación se muestra la tabla con las ponderaciones de las once variables que fueron analizadas y modificas por criterio de los oficiales de seguridad de la información:

Tabla 18:

Ponderaciones Ajustadas

	Variable	Ponderación modificada Variable
1	Política de seguridad	3.00
2	Organización de la seguridad de la información	3,00
3	Gestión de activos y clasificación de la información	4,00
4	Seguridad en recursos humanos	3,00
5	Seguridad física y ambiental	4,00
6	Gestión de comunicaciones y operaciones	4,00
7	Control de acceso	4,00
8	Adquisición, desarrollo y mantenimiento de los sistemas de información	4,00
9	Gestión de incidentes de seguridad	5,00
10	Gestión de la continuidad del negocio	5,00
11	Cumplimiento normativo	4,00

Como se puede apreciar en la tabla existen tres grupos de ponderaciones, las de nivel 5 que llevan a un estado de madurez de optimización, las de nivel 4 que permiten gestionar a la organización basado en resultados cuantitativos en pro de la mejora y los de nivel 3 que son requeridos para iniciar un proceso de gestión de la seguridad de la información.

Se recomienda que para aplicaciones futuras del presente instrumento metodológico se aplique las ponderaciones validadas a las variables y se ajusten de igual manera las ponderaciones para cada uno de los indicadores.

Por otro lado, al haber aplicado la presente herramienta metodológica en tres instituciones públicas de impacto nacional, se puede recomendar la aplicación a nivel nacional de dicho instrumento con el objetivo de determinar la madurez de las organizaciones a nivel nacional con respecto a la gestión de la seguridad de la información.

Una de las recomendaciones de los oficiales de seguridad de la información fue que el instrumento desarrollado debe ser actualizado hacia la nueva versión de la ISO/IEC 27001:2013, ya que este actualmente es de la versión 2005, por lo que para futuras aplicaciones se debe actualizar las variables e indicadores de acuerdo a la nueva versión de la norma.

5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

La investigación realizada permitió cumplir con los objetivos propuestos y establecer las siguientes conclusiones:

- El Gobierno ecuatoriano implementa el Plan Nacional para el Buen Vivir para el manejo de la administración pública, teniendo por objetivo articular políticas de inversión y gestión pública, siendo una de las metas el cambio de la matriz productiva, para lo cual implementa el Plan Nacional de Gobierno Electrónico. Por lo que se concluye que la visión del actual gobierno es mejorar cualitativamente los servicios de información que se ofrecen a las ciudadanas y ciudadanos, aumentando la eficiencia y eficacia de la gestión pública, mediante el uso de las Tecnologías de la Información y Comunicaciones (TIC) por parte de las instituciones públicas.

- El Plan Nacional de Gobierno Electrónico ha venido siendo implementado desde su creación y en la actualidad el Gobierno ecuatoriano, ha medido su estado de desarrollo a través de múltiples estudios que han determinado la penetración de las TIC en las instituciones públicas y localiza a las mismas en un estado Transaccional, por tanto pudiendo concluir que los portales gubernamentales incluyen servicios transaccionales con una comunicación bidireccional entre el ciudadano y el gobierno.

- Para controlar la creciente implementación de las TIC, se han creado herramientas legales para normar el uso, ente ellas la Código Orgánica Integral Penal, la cual incluye una sección completa para tratar los delitos referentes a la seguridad de la información. Adicionalmente la Secretaria Nacional de Administración Pública ordena la implementación obligatoria del Esquema Gubernamental de Seguridad de la Información (EGSI) basado en la norma NTE INEN ISO/IEC 27001:2011, a través del acuerdo interministerial N° 166 en las instituciones públicas dependientes de la administración central. Concluyendo que mediante la aplicación y ejecución de estas políticas públicas se busca minimizar la creciente ocurrencia de eventos de seguridad

sucedidos en el país y asegurar la integridad, confidencialidad y disponibilidad de la información administrada y procesada por el sector público.

- En las instituciones públicas del Ecuador se han registrado una serie de incidentes de seguridad en los sistemas de información, causando graves perjuicios económicos y generando desconfianza en la población. Se concluye que las principales causas se deben a la ausencia o incumplimiento de controles, normas o políticas para proteger la información.

- En el año 2011 el Instituto Ecuatoriano de Normalización, realiza una traducción idéntica de la Norma Internacional ISO/IEC 27001:2005, la cual se adopta para el Ecuador como NTE INEN –ISO/IEC 27001:2011, dicha norma proporciona un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información, concluyendo que dicha norma permite garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por parte de la institución de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

- Se desarrolla una metodología de evaluación, con el fin de determinar el grado de calidad con el cual es gestionado la seguridad de la información en instituciones públicas, llegando a la conclusión que es posible cuantificar el estado de madurez en las instituciones públicas respecto a procesos de las TIC, permitiendo a su vez conocer el grado con el cual se gestiona la calidad de la seguridad de la información.

- Para ejecutar la metodología planteada se desarrolló un modelo de entrevista y observación, el cual permite levantar la información necesaria de una forma ágil y eficiente, para ello se identificaron las unidades organizacionales responsables de los procesos para gestionar la seguridad de la información en las instituciones. Esta metodología fue ejecutada en tres instituciones públicas, en donde se obtuvieron datos que permitieron ajustar el modelo y validar la aplicación del mismo. Port tanto se concluye que esta metodología puede ser ejecutada en cualquier institución pública del

país que tengan diferentes giros de negocios y motivaciones para gestionar la seguridad de la información.

- Analizando los resultados obtenidos en las tres instituciones, se llegó a conocer el grado o nivel de madurez con respecto a la calidad de gestión de la seguridad de la información basado en la norma NTE INEN ISO/IEC 27001:2011, determinando que las instituciones se encuentran en el nivel de madurez tres (Definida) y con tendencia de mejora , lo que permite concluir que los procesos para gestionar la seguridad de la información se encuentran claramente caracterizados y comprendidos, estos procesos son parte de un estándar, donde se mantiene la integridad de la gestión de la seguridad de la información en toda las instituciones.

- Se denota una particularidad en los tres casos analizados, las variables sobre el manejo de incidentes de seguridad y los planes de continuidad de negocio, no evidencian una gestión planificada de acuerdo a la política de seguridad de cada institución. Para el resto de variables estudiadas se evidencia que las instituciones las están gestionando acorde a la política de seguridad.

5.2 Recomendaciones

Para finalizar esta investigación, a continuación se presentan algunas recomendaciones:

- Es evidente que el Gobierno ecuatoriano se encuentra actuando proactivamente con el objetivo de precautelar la seguridad de la información, para ello ha desarrollado el Esquema Gubernamental para la Gestión de la Seguridad de la Información (EGSI.), este esquema debe implementarse en todas las instituciones dependientes de la administración central, el mismo que denota una visión de obligatoriedad, por lo que se recomienda enfocar la visión de la implementación del EGSI como una cultura organizacional, en donde todos los actores involucrados participen proactivamente para lograr un nivel óptimo de calidad en la gestión de la seguridad de la información.

- Con respecto al Esquema Gubernamental para la Gestión de la Seguridad de la Información se recomienda que el mismo sea implementado inicialmente solo en los procesos críticos de las instituciones para posteriormente causar un efecto cascada hacia el resto de procesos. Por otro lado se recomienda revaluar los tiempos concebidos (18 meses) para la implementación del EGSI, así como sus presupuestos, ya que se determinó durante la investigación realizada que las instituciones no han completado la implementación durante el tiempo establecido y adicionalmente los presupuestos fueron insuficientes.

- El Instituto Ecuatoriano de Normalización en el año 2011, realizó una traducción idéntica de la Norma Internacional ISO/IEC 27001 Versión: 2005, la cual se adoptó en el Ecuador como NTE INEN –ISO/IEC 2700: 2011, sin embargo dicha versión base tiene ya 10 años de publicación, existiendo a la fecha una actualización realizada en el año 2013, en donde se incluyen nuevas clausulas y objetivos de control. Por lo que se recomienda al Instituto Ecuatoriano de Normalización, adoptar la última versión, que incluyen modificaciones acordes a las nuevas tendencias para el uso de las TIC y la gestión de la seguridad de la información.

- Al haber validado la eficiencia y eficacia de la metodología desarrollada en la presente investigación, es posible conocer el nivel de calidad en la gestión de seguridad de la información en cualquier organización pública del país, por lo que se recomienda realizar un posterior estudio estadístico para conocer el nivel de madurez con el cual está siendo gestionado el EGSI en el Ecuador, y de esta manera disponer de información para ajustar los planes de implementación a nivel general y en las instituciones públicas.

- Luego de haber analizado los resultados obtenidos de los tres casos estudiados, se recomienda trabajar en prioridad alta sobre las variables:

    a. Gestión de los Incidentes de la Seguridad.
    b. Gestión de la Continuidad del Negocio.

  Las mismas que muestran resultados deficientes con respecto a su gestión, estas variables críticas garantizan que en el caso de ocurrir un incidente de seguridad, este sea tratado de la forma adecuada y que los sistemas de información dispongan de un plan de continuidad que permita mantener la disponibilidad, integridad y confidencialidad de los mismos.

- Las recomendaciones generales para el caso uno están basadas en las siguientes variables:

    a. Política de Seguridad de la Información.
    b. Seguridad en recursos humanos.

  Dichas variables demuestran un nivel de gestión bajo, en el caso de la política de seguridad de la información, esta no se encuentra siendo medida ni mejorada debido a que su implementación es reciente, por lo que se recomienda que su gestión sea basada en indicadores que permitan tomar decisiones y acciones de mejora. La seguridad en recursos humanos denota falencias en los procesos que gestionan la misma, por lo que se recomienda realizar una revisión integral de todos los controles plateados por la norma para garantizar la seguridad de la información

con respecto a los recursos humanos. Por último se recomienda a la institución continuar con el proceso de implementación de los controles de la norma hacia los procesos restantes.

- Las recomendaciones generales para el caso dos están basadas en las siguientes variables:

    a. Política de Seguridad de la Información.
    b. Adquisición, desarrollo y mantenimiento de los sistemas de información.
    c. Cumplimiento normativo

    Dichas variables demuestran un nivel de gestión bajo, en el caso de la política de seguridad de la información, esta no se encuentra siendo revisada, medida ni mejorada debido a que la implantación de la norma en todos los procesos de la organización demanda tiempo y recursos, por lo que se recomienda que su gestión sea basada en indicadores que permitan tomar decisiones y acciones de mejora. Con respecto a la adquisición, desarrollo y mantenimiento de los sistemas de información, se demuestra que existen falencias en el control de vulnerabilidades, lo cual puede permitir fugas de información afectando la seguridad de la misma, por lo que se recomienda tomar acciones inmediatas para definir y especificar los requisitos de seguridad que deben disponer los sistemas de información. Por último el cumplimiento normativo también demuestra debilidades en su gestión, específicamente en el tema de auditorías de los sistemas de información, recomendado que se enfaticen los controles que gestionan las auditorias de los sistemas de información.

- En el caso tres se presentan una situación atípica debido a la criticidad de la información y al giro del negocio que esta institución dispone, en donde se puede evidenciar que el nivel de calidad de gestión de la seguridad de la información se encuentra en un nivel de madurez cuatro (Gestionando Cuantitativamente), con la proyección del alcanzar el nivel máximo cinco (Optimización), por el avanzado estado de implementación de la norma. Sin embargo como se mencionó anteriormente existen dos variables que requieren especial atención, la gestión de

los incidentes de la seguridad y la gestión de la continuidad del negocio que son factores fundamentales para gestionar incidentes de seguridad y garantizar la disponibilidad de la información, por lo que se recomienda implementar los controles y procedimientos necesarios para gestionar adecuadamente estas variables y poder llegar a un estado de madurez óptimo.

.

BIBLIOGRAFÍA

CONGRESO DE ECUADOR. (2002). *LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS.* Quito.

Activate Ecuador. (2014). *Activate Ecuador*. Obtenido de Activate Ecuador: http://www.activate.ec/content/presidencia

Asamblea Constituyente. (2007). *Constitución de la Republica.* Manabí.

Asamblea Nacional. (2009). *Ley Orgánica de la Función Legislativa.* Quito.

Asamblea Nacional. (28 de 02 de 2012). *Sistema de curul electrónica entró en funcionamiento y se hizo efectivo el plan cero papeles.* Obtenido de Asamblea Nacional: http://www.asambleanacional.gob.ec/kichwa/noticia/sistema_de_curul_electronica_entro_en_funcionamiento_y_se_hizo_efectivo_el_plan_cero_papeles

Asamblea Nacional. (25 de 06 de 2013). *Ley Orgánica de Comunicación.* Obtenido de Asamblea Nacional: http://www.asambleanacional.gob.ec/system/files/ley_organica_comunicacion.pdf

CASTILLO PEÑAHERREA, C. (2013). *Acuerdo No 166.* Quito.

CONGRESO DE COLOMBIA. (1999). *LEY 527.* Obtenido de Ministerio de Tecnologías de la Información y las Comunicaciones: http://www.mintic.gov.co/portal/604/articles-3679_documento.pdf

Consejo de la Judicatura. (2012). *JUSTICIA 2.0.* Obtenido de Consejo de la Judicatura: http://www.funcionjudicial.gob.ec/index.php/es/component/content/article/25-consejo-judicatura/235-justicia-20

Contraloria General del Estado. (2013). *Rendición de Cuentas 2013.* Obtenido de Contraloria General del Estado: http://www.contraloria.gob.ec/documentos/informes/RendicionCuentas2013/index.html

Corletti Estrada, A. (2006). *ISO-27001: Los Controles.* Obtenido de El portal de ISO 27001 en Español: http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_I.pdf

Corporación EKOS. (2013). *Gestión Publica Mejores Prácticas.* Quito: Ekos.

Corte Constitucional del Ecuador. (2013). *Informe de Rendición de Cuentas 2013.* Obtenido de Corte Constitucional del Ecuador: https://www.corteconstitucional.gob.ec/images/stories/pdfs/informe_2013.pdf

Ecuamex. (202). *Escándalo de falsas afiliaciones a partidos políticos*. Obtenido de EcuadorInmediato: http://www.ecuadorinmediato.com/index.php?module=Noticias&func=news_user_view&id=178354

El Telégrafo. (2012). *Siete años de cárcel por robar al Estado*. Obtenido de El Telégrafo: http://www.telegrafo.com.ec/justicia/item/siete-anos-de-carcel-por-robar-al-estado.html

El Telégrafo. (2013). *Juan Salazar fue declarado culpable en Riobamba*. Obtenido de El Telégrafo: http://www.telegrafo.com.ec/regionales/regional-centro/item/juan-salazar-fue-declarado-culpable-en-riobamba.html

Falconí, F. (2013). Plan Nacional del Buen Vivir.

Instituto Colombiano de Normas Técnicas. (2009). *NORMA TÉCNICA NTC-ISO/IEC 27005.* Bogota: Icontec.

Instituto Colombiano de Normas Técnicas y Certificación. (2007). *Código de Practica para la Gestión de la Seguridad de la Información ISO27002.* Bogota: ICONTEC.

Instituto Ecuatoriano de Normalización. (2011). *Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27001:2011*. Quito.

Instituto Ecuatoriano de Normalización. (2012). *Gestión del Riesgo en la Seguridad de la Información.* Quito: INEN.

Iso27000.es. (2014). *Sistema de Gestión de Seguridad de la Información*. Obtenido de El portal de ISO 27001 en Español: http://www.iso27000.es/sgsi.html

ISOTools (Dirección). (2013). *Webinar. Diagnóstico de la Seguridad de la Información para el Sector Público.* [Película].

IT360.es. (2014). *Seguridad de la Información*. Obtenido de IT Audit & Innovation: http://www.it360.es/iso27001.php

Jurado Vargas, R. (Abril de 2005). *Diagnóstico de las Políticas de TIC en el Ecuador.* Obtenido de Facultad Latinoamericana de Ciencias Sociales Sede Ecuador: https://www.flacso.org.ec/docs/diagnostico_tic.pdf

Ministerio de Finanzas. (2014). *Ministerio de Finanzas*. Obtenido de Sector Público: http://www.finanzas.gob.ec/que-es-el-sector-publico-2/

Ministerio de Justicia del Ecuador. (2014). *Código Orgánico Integral Penal.* Quito.

Ministerio De Telecomunicaciones, y. d. (Enero de 2014). *Tecnologías de la Información y Comunicaciones para el Desarrollo.* Obtenido de Subsecretaría de Fomento de la Sociedad de la Información y Gobierno en Línea: http://www.industrias.ec/archivos/CIG/file/CARTELERA/MINTEL-TIC%20para%20el%20Desarrollo.pdf

Naciones Unidas. (2012). *Estudio de las Naciones Unidas sobre el Gobierno Electrónico.* Obtenido de Naciones Unidas: http://workspace.unpan.org/sites/Internet/Documents/EGovSurvey2012_Spanish.pdf

Patiño Cruz, C. A. (26 de Agosto de 2013). *Niveles de madurez de CMMI* . Obtenido de Estándares de calidad de Software: http://estandarcalidadcarlosp.blogspot.com/2013/08/niveles-de-madurez-de-cmmi.html

Pazmiño, L. M. (05 de 06 de 2014). *CALIDAD DE LA GESTIÓN EN LA SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO/IEC 27001, EN INSTITUCIONES PÚBLICAS, EN LA CIUDAD DE QUITO D.M.* Quito.

Procuradoria General del Estado. (2013). *Informe de Gestión 2013.* Obtenido de Procuradoria General del Estado: http://www.pge.gob.ec/index.php/documents/transparencia/747-informe-de-gestion-2013-final/file

Ramírez Castro, A., & Ortiz Bayona, Z. (Agosto de 2011). *Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios.* Obtenido de Revisión Técnico Mecánica Colombia: http://rtm.colserauto.com/rtm/Portals/1/3833-16128-1-PB.pdf

Secretaría Nacional de la Administracion Pública . (2013). *Esquema Gubernamental de Seguridad de la Información.* Quito.

Secretaria Nacional de la Administración Pública. (2014). *Plan Nacional de Gobierno Electrónico.* Obtenido de Plan Nacional de Gobierno Electrónico: http://www.gobiernoelectronico.gob.ec/PlanGobiernoElectronicoV1.pdf

Secretaria Nacional de Planificación y Desarrollo, Senplades. (17 de 09 de 2014). *Estadísticas Plan Nacional del Buen Vivir 2013-2017*. Obtenido de Sistema Nacional de Información:

http://indestadistica.sni.gob.ec/QvAJAXZfc/opendoc.htm?document=SNI.qvw&host=QVS@kukuri&anonymous=truehttp://indestadistica.sni.gob.ec/QvAJAXZfc/opendoc.htm?document=SNI.qvw&host=QVS@kukuri&anonymous=true&bookmark=Document/BM71

Senplades. (2012). *Transformación de la Matriz Productiva.* Obtenido de Secretaria Nacional de Planificación y Desarrollo: http://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/01/matriz_productiva_WEBtodo.pdf

Senplades. (2013). *Plan Nacional del Buen Vivir.* Quito.

Software Engineering Institute. (2010). *Mejora de los procesos para el desarrollo de mejores productos y.* España: CMMI.

Tribunal Contencioso Electoral del Ecuador. (06 de 2013). *Jueces Electorales asisten a presentación de tecnología del voto electrónico.* Obtenido de Tribunal Contencioso Electoral del Ecuador: http://www.tce.gob.ec/jml/index.php/1241-jueces-electorales-asisten-a-presentacion-de-tecnologia-del-voto-electronico

UNESCO, & MCCTH. (2013). Comparativo de gasto en I+D+ i .

URUEÑA LEÓN, E. E. (2008). *SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN - SGSI.* Obtenido de REDES, COMPUTACIÓN Y MANTENIMIENTO: edselenrique.wikispaces.com/file/view/SGSI.pdf

Villacrés, S. (2014). *Función ejecutiva en el Ecuador.* Obtenido de derechosageo: http://derechosageo.blogspot.com/2012/11/funcion-ejecutiva-en-el-ecuador.html

ANEXOS

ANEXO 1

MODELO DE LA METODOLOGÍA

GUÍA DE ENTREVISTA

Guia de Entrevista								
Variable	Madurez Indicador	Inidcadores	Preguntas		Respuestas			Peso
Politica de Seguridad	3	Politica de Seguridad	1	¿Dispone de una politica de seguridad de la información?	NO			-
					Si	Verbal/AdHOC	◯ Botón de	1.00
						Desarrollo de Politica Formal	◯ Botón de	2.00
						Documento de Politica	◯ Botón de	3.00
	3	Distribución,Publicación y Conocmimiento de la Politíca	2	¿Usted recibio la Politica de seguridad de la información de la organzacion?	NO			-
					Si	A traves de inducción	☐ Casilla de	0.50
						Fisicamente /digitalmente	☐ Casilla de	0.50
				¿Conoce usted la Politica de Seguridad?	NO			
			3		SI	Poco	◯ Botón de	0.50
						Completa	◯ Botón de	1.00
	3	Revisión a la Politica	4	¿Se han realizado revisiones o cambios a la politica de seguridad?	NO			
					SI	Revision Reactiva	◯ Botón de	1.50
						Revision Proactiva	◯ Botón de	3.00
	4	Medicion de Politica de Seguridad	5	¿Dispone de indicadores de gestión de la politica?	NO			
					SI		☐ Casilla de	4
	5	Mejora de la Politica de Seguridad	6	¿Ha realizado mejoras en base a los indicares de gestión?	NO			
					SI		☐ Casilla de	5

Anexo 1: (Continuación)

Organización de la seguridad de la información	3	Compromiso de la dirección	7	¿Existe apoyo activo por parte de la dirección?	NO			
					SI	Compromiso formales	☐ Casilla de	0.5
						Asignación de recuros	☐ Casilla de	1.25
						Reconocimiento de responsabilidades	☐ Casilla de	1.25
	3	Coordinacion y Responsabilidad de la seguridad de la información	8	¿Se coordinan entre los departamentos temas de seguridad de la información?	NO			
					SI	Existen Roles definidos por departamento	☐ Casilla de	0.5
						Existe asignación formal de funciones de trabajo	☐ Casilla de	1
						Existen responsabilidades definidas	☐ Casilla de	1.5
	4	Autorizacion de nuevos recursos para el tratamiento de la información	9	¿Dispone de un proceso por parte de la dirección para la autorización de nuevos recursos o activos de información?	NO			
					SI	Definido	◯ Botón de	2
						Implantado	◯ Botón de	4
	3	Acuerdo de Confidencialidad	10	¿Dispone de acuerdos de confidencialidad firmados con sus coloboradores	NO			
					Si		☐ Casilla de	2
					Se ha revisado periodicamente, en el ultimo año		☐ Casilla de	1
	5	Contacto con Autoridades y Grupos de Interes Espcializados	11	¿Mantiene la organizaocion contacto con personas/entidad enternas para tratar temas relacionados con la seguridad de la información?/¿Si es positivo es forma reactiva o proactiva?	NO			
					SI	Autoridades competentes (deparmaneto de crimines informaticos de la policia)	☐ Casilla de	2
						Profesionales o foros especializados en seguridad (Asesoria especialzada)	☐ Casilla de	3
	4	Revisión independiente de la seguridad de Informacíón	12	¿Se ha realizado una Revisión Externa a la gestion de seguridad?	NO			
					SI	Se ha revisado Politicas	☐ Casilla de	0.5
						Se ha revisado Objetivos	☑ Casilla de	0.5
						Se ha revisado Controles	☐ Casilla de	1
						Se ha revisado procesos	☐ Casilla de	2
	3	Identificación de los riesgos y controles a la seguridad por el acceso de terceros	13	¿ Se han Identificado los riesgos a la seguridad por el acceso de	NO			
					SI		☐ Casilla de	1
			14	¿ha implementado controles de acceso de terceros?	NO			
					Si	Ha implantado Controles para elacceso a la informacion	☐ Casilla de	1
						Ha implantado Controles de acceso a los dispositivos	☐ Casilla de verificación 4	1
	3	Tratamiento de la Seguridad en contratos con terceros	15	¿Disponen los contratos de clausulas referentes a la seguridad con terceros?	NO			
					SI	Clausulas de Confidencialidad	☐ Casilla de	1
						Clausulas con respecto a la integridad de la información	☐ Casilla de	1
						Clausulas que aseguren la disponibilidad de la informacion	☐ Casilla de	1
	3	Tratamiento de la Seguridad con los ciudadanos	16	¿Controla el acceso a la infromacion por parte de los ciudadados ?	NO			
					SI	Se indetifica al ciudadano	☐ Casilla de	1.5
						Se otorgan perfiles	☐ Casilla de	1.5

Anexo 1: (Continuación)

Gestion de Activos y clasificacion de la informacion	5	Inventario de Activos	17	Dispone de un inventario de Activos?	NO			
					SI	Lo lleva manualmente	◯ Botón de	0.5
						Dispone de un aplicativo o sistema para llevarlo	◯ Botón de	1
				¿Mantiene actualizado el inventario de activos?	NO			
					SI	Periodicamente	☐ Casilla de	1
						Cuanto haya movimientos en los activos o los usuarios	☐ Casilla de	1
	4	Propiedad de los activos	18	Tiene designado usuarios responsables para cada activo asociado con el tratamiento de la informacion?	NO			
					SI		☐ Casilla de	2
	3	Reglamentos de Uso de activos	19	Dispone de Reglas de uso de activos de infromación	NO			
					Si	Identificadas las reglas	☐ Casilla de	0.5
						Documentadas las reglas	☐ Casilla de	1
						Implementadas las reglas	☐ Casilla de	1.5
	4	Directriz de clasificacion	20	Dispone de directrices de clasificacion de la informacion	NO			
					SI	la clasifica por su valor	☐ Casilla de	1
						la clasifica por criticidad	☐ Casilla de	1
Seguridad en Recursos Humanos	3	Funciones, Reponsabilidades	21	¿Se encuentran definidas y docuementas los requisitos de seguridad previo al empleo de un actor?	NO			
					SI	Están definidas las funciones	☐ Casilla de	0.75
						Estaán definidas las responsabilidades	☐ Casilla de	0.75
						Están idenficiados los riesgos	☐ Casilla de	1.5
	3	Investigación de antecedentes	22	¿se realiza una investigación de antecedentes , previo al empleo de los actores invlocrados con la organización?	NO			
					SI	Certificado de Antecedentes Penales MDI	☐ Casilla de	1
						Antecedentes laborables	☐ Casilla de	1
						Antecedentes conductuales	☐ Casilla de	1
	3	Terminos y Condiciones Contractuales	23	¿Incluye el contrato con los actores invlocurados de terminos y condiciones relativos a la seguridad de la información?	NO			
					SI	Clausulas de Confidencialidad	☐ Casilla de	1
						Clausulas con respecto a la integridad de la información	☐ Casilla de	1
						Clausulas que aseguren la disponibilidad de la informacion	☐ Casilla de	1
	5	Responsabilidad de la dirección	24	¿Exige la dirección a la organización la aplicación de la politica y procedemientos de segurdad de la información?	NO			
					SI	Dispone de mediciones regulares de la aplicación de la plitica y procedemintos	☐ Casilla de	1.5
						Dispone o solicita de informes de cumplimiento de politcas y procedimientos	☐ Casilla de	1.5
						Se han tomado acciones para la mejora	☐ Casilla de	2
	3	Capacitación en seguridad de la información	25	¿Reciben los actores involucrados capacitaciones sobre la seguridad de la información	NO			
					SI	Tras un incidente de seguridad	◯ Botón de	1
						Es periodico y constante	◯ Botón de	3
	4	Proceso disciplinario	26	Dispone de proceso disciplinario formal para los actores involucrados, cuando hayan provocado un incidente de seguridad?	NO			
					Si	Verbal/AdHOC	☐ Casilla de	0.5
						Memo	☐ Casilla de	1.5
						Acciones Económicas y/o legales	☐ Casilla de	2
	3	Cese del empleo o cambio de puesto de trabajo	27	¿Dispone de proceso definido para cuando los actores involucrados cesen o cambien de su puesto de trabajo?	NO			
					SI	Dispone de un responsable para la recepcion de funciones y responsabilidades del actor	☐ Casilla de	1
						Dispone de un procedimiento para la devolución de activos	☐ Casilla de	1
						Dispone de un procedimiento para retirar los accesos concedidos a los actores salientes	☐ Casilla de	1

Anexo 1: (Continuación)

3.583333333	Seguridad física y ambiental	5	Perimetros y controles de seguridad física						
		5	Protección de las áreas criticas de activos de información contra amenazas externar y de origen ambiental	28	¿Dispone de protección física para las áreas críticas de los activos de informacion (Areas servidores) contra desastres naturalez o provocados por el hombre	NO			
						SI	Sensores de contra incendios	☐ Casilla de	1
							Sensores de temperatura y humedad	☐ Casilla de	1
							Sensores de Anti-Shock	☐ Casilla de	1
							Diseños tipo bunkers para las áreas mas críticas	☐ Casilla de	2
		3	Trabajo en areas seguras	29	¿Dispone de politicas de seguridad industrial para el trabajo en las zonas seguras (Areas de servidores)?	NO			
						SI	Verbal/AdHOC	◯ Botón de	1
							Desarrollo de Politica de seguridad industrial	◯ Botón de	2
							Documento de Politica	◯ Botón de	3
		4	Areas de acceso publico						
		4	Instalaciones de suministro y cableado	30	¿Dispone de una fuente alterna de alimentación contra fallas de energia	NO			
						SI	☐ Casilla de	2	
				31	¿Dispone de redes de cableado estrucurado (electrico y telecominucaciones) basado en los estandares de la industria?	NO			
						SI	☐ Casilla de	2	
		3	Mantenimiento de equipos	32	¿Dispone de un plan de mantenimiento de equipos?	NO			
						SI	Correctivo	◯ Botón de	1
							Preventivo	◯ Botón de	3
		5	Seguridad de los equipos fuera de la organización	33	¿Dispone de procedimientos para asegurar los equipos que se encuentran fuera del área fisica de la organización?	NO			
						SI	Mecanismos de encriptación de datos	☐ Casilla de	1
							Mecanismos de autentificacion (uso de passwords) para el acceso a los equipos	☐ Casilla de	1.5
							Mecanismos de trazabilidad de los equipos	☐ Casilla de	2.5
		4	Reutilizacion o retiro seguro de equipos	34	¿Dispone de procedimientos de destrucción segura de datos?	NO			
						SI	Tecnicas de borrado standares	◯ Botón de	2
							Tecnicas de sobreescritura seguras	◯ Botón de	4
		3	Transporte de los activos de información propiedad de la organización	35	¿Dispone de procedimientos para autorizar la movilización de los activos de información?	NO			
						Si	Verbales	◯ **Botón de**	1
							Por escrito	◯ **Botón de**	3

Anexo 1: (Continuación)

Gestion de Comunicaciones y Operaciones	3	Documentacion de procedimientos de operación	36	¿Dispone de manuales de operación documentados?	NO			
					SI		☐ Casilla de	1
						Los usuarios tienen accesos a los mismo	☐ Casilla de	1
						Se realizan acutalizaciones periodicas	☐ Casilla de	1
	4	Control de cambios en activos	37	¿Controla los cambios realizados sobre los activos de información la organizacón?	NO			
					SI	Documenta los cambios	☐ Casilla de	2
						Registro de versionamiento	☐ Casilla de	2
	3	Separación de tareas	38	¿Se encuentran separadas las tareas y responsabilidades para el tratamientos de la infromación(dba, admin red, jefe	NO			
					SI		☐ Casilla de	3
	4	Separación de recuros	39	¿Se encuentran separados los recusrsos de tratamiendo de información en los diferentes ambientes de desarrollo, pruebas y produccion?	NO			
						Separacion Física o Logica	☐ Casilla de	2
					SI	Separación en redes distintas	☐ Casilla de	2
	4	Provisión y supervición de de servicios prestados por terceros	40	¿Comprueba que los servicios ofrecidos por terceros(hardware, software, internet, telefonia) cumplan con las expectativas requeridas por la organización?	NO			
					SI	Firma un acuerdo de calidad de servicio con el tercero (SLA o Contrato)	☐ Casilla de	1
						Dispone de registros de implantación y cumplimiento del acuerdo de calidad (Acta de Entrega)	☐ Casilla de	1
						Recibe usted peridicamente por parte de terceros documentos o registros acerca de la calidad de servicio	☐ Casilla de	1
						Realiza auditorias periódicas del mismo	☐ Casilla de	1
	4	Gestion del cambio en los servicios prestados por terceros	41	¿Dispone de uno o mas de estos procedimiento para gestionar los cambios en los e servicios prestados por terceros?	NO			
					SI	Revisión a la politica de seguridad	☐ Casilla de	1
						Revision a los procedimientos de seguridad	☐ Casilla de	1
						Revision de controles de seguridad	☐ Casilla de	1
						Reevaluación de los riegos	☐ Casilla de	1
	5	Gestión de capacidad de los recuros de tratamiento de la información	42	¿Gestiona usted los requerimientos de recursos necesarios para garantizar el rendimiento requerido por los sistemas de la organización?	NO			
					SI	ADHOC - Cuando se hace evidente la necesidad de aumento de recursos	◯ Botón de	1
						Estan definidos los recursos de acuerdo a las especificaciones y conocen los limites	◯ Botón de	3
						Monitoriza los recursos utlizados para, de ser el caso tomar las acciones necesarias	◯ Botón de	4
						Proyecta futuros incrementos de recursos para garantizar el redimiento de los sistemas	◯ Botón de	5
	5	Aceptación de sistemas	43	¿Cuáles son sus procedimientos de aceptación de nuevos sistemas de información?	Ninguno			
					Dispone de criterios para la aceptacion TDR		☐ Casilla de	1
					Dipone de criterios para actualizacion o nuevas versiones		☐ Casilla de	1
					Lleva a cabo pruebas durante el desarrollo		☐ Casilla de	1.5
					Lleva a cabo pruebas previo a la aceptacion		☐ Casilla de	1.5
	4	Protección contra el codigo malicioso y descagable	44	¿Dispone de controles contra codigo malicioso o descargable?	NO			
					SI	Sofware Base Antivirus	◯ Botón de	1
						Soluciones EndPoint	◯ Botón de	2
						Concientizacion a los usuarios	☐ Casilla de	1
						Controla la instalación y ejecución de nuevo software	☐ Casilla de	1

Anexo 1: (Continuación)

Gestion de Comunicaciones y Operaciones	4	Protección contra el codigo malicioso y descagable	44	¿Dispone de controles contra codigo malicioso o descargable?	SI	Soluciones EndPoint	◯ Botón de	2
						Concientizacion a los usuarios	☐ Casilla de	1
						Controla la instalación y ejecución de nuevo software	☐ Casilla de	1
	3	Copias de seguridad	45	¿Realiza copias de seguridad periodicamente de los sistemas de información?	NO			
					SI		☐ Casilla de	1.5
					Las prueba periodicamente		☐ Casilla de	1.5
	5	Controles de red	46	¿Las redes de su organización están gestionadoas y controladas?	NO			
					SI	Dispone de administrador de red	☐ Casilla de	1.5
						Dispone de infraestrucura de control de red(checkpoint , cisco)	☐ Casilla de	1.5
						Análiza la información en transito dentro de su red	☐ Casilla de	2
	3	Seguridad de los servicios de red	47	¿Tiene identificados y dcoumentados los servicios de red expuestos en su organizción?	NO			
					SI		☐ Casilla de	1
					Tiene identificado los requisistos de seguridad de cada servicio		☐ Casilla de	2
	3	Manipulación de los soportes	48	¿Dispone de procedimientos para la gestion, manipulación y seguridad de soportes?	NO			
					SI	Los soportes extraibles son gestionados	☐ Casilla de	1
						Hay procedimientos formales para retirar un medio de soporte	☐ Casilla de	1
						Existe un responsable de la manipulación, custodia y alamacenamiento de los soportes	☐ Casilla de	1
	4	Intercambio de la información	49	¿Existen procedimientos para el intercambio de información con actores internos y externos?	NO			
					SI	Dispone de acuerdos formales	☐ Casilla de	0.5
						Protegue los soportes de accesos no autorizados, en el caso de transporte fuera de las instalaciones	☐ Casilla de	1
						Utiliza protcolos seguros para la mensajeria electrónica	☐ Casilla de	1.25
						Utliza protocolos seguros para la interconección de sistemas entre organizaciones	☐ Casilla de	1.25
	5	Supervisión del tratamiento de la información	50	¿Realiza auditorias a las actividades de tratamiento de información de los actores involucrados	NO			
					SI	Registro de actividades realizadas en los sistemas	☐ Casilla de	0.5
						Registra exepciones generadas por el usuario	☐ Casilla de	0.25
						Registra eventos de seguridad	☐ Casilla de	0.5
						Mantiene los registros históricos	☐ Casilla de	0.25
						Registra las actividades de los administradores de sistemas	☐ Casilla de	0.5
			51	¿Dispone de procedimietos de supervisión de las activiades de tratamiento de información?	NO			
					SI	Revisa los registros de auiditoria de los sistemas	☐ Casilla de	0.75
						Dispone de medidas de seguridad para evitar la manipulacion de registros	☐ Casilla de	0.5
						Analiza los resultados de las actividades de los sistemas	☐ Casilla de	0.75
						Sugiere cambios basado en los resultados	☐ Casilla de	0.5
			52	¿Dispone de un mecanismo de sincronización de tiempo único para sus servidores?	NO			
					SI		☐ Casilla de	0.5

Anexo 1: (Continuación)

Control de Accceso	3	Políticas de Control de Accesos	53	¿Dispone de una política de control de acceso a la información?	NO			
					SI	Verbal/AdHOC	◯ Botón de	1.00
						Desarrollo de Politica Formal	◯ Botón de	2.00
						Documento de Politica	◯ Botón de	3.00
	5	Gestion de acceso de usuario	54	¿Utilza alguno de los siguientes procedimientos para prevenir el acceso no autorizado a los sistemas de información?	NO			
					SI	Dispone de un procedimiento de creación de usuario	☐ Casilla de	0.50
						Dispone de un procedimiento para la anulación de un usuario	☐ Casilla de	0.50
						Dispone de un procedimiento para asignar persmisos a los usuarios	☐ Casilla de	1.00
						Dispone de un procedimiento para controlar la asignación y uso de permisos	☐ Casilla de	1.00
						Dispone de un procedimiento para la entrega formal de contraseñas	☐ Casilla de	1.00
						La dirección revisa periodicamente los derechos de accesos, con procedimientos formales	☐ Casilla de	1.00
	3	Responsabilidades de usuario	55	¿Utliza usted alguna regla para la seleccioón y uso de contraseñas?	NO			
					SI		☐ Casilla de	1.00
	4	Uso de servicios de red	56	¿En el firewall interno dispone de reglas que permitan controlar el acceso a los servicios autorizados a los usuarios?	NO			
					SI		☐ Casilla de	4
	4	Autentificación de conecciones remotas		¿Utliza alguno de los siguientes métodos seguraros para autentificar a usuarios remotos?	NO			
					SI			
					☑ Casilla de	Uso de connecciones seguras remotas: VPN	☐ Casilla de	0.5
					☑ Casilla de	Uso de HTTPS para los aplicativps	☐ Casilla de	0.5
					☑ Casilla de	Envia correo electronico SMTPS	☐ Casilla de	0.5
					☑ Casilla de	Recibe correos electronico POP3S	☐ Casilla de	0.5
					☑ Casilla de	Recibe correo con IMAP Secure	☐ Casilla de	0.5

Anexo 1: (Continuación)

Control de Accceso	4	Autentificación de conecciones remotas	57	seguraros para autentificar a usuarios remotos?	☑ Casilla de	Recibe correos electronico POP3S	☐ Casilla de	0.5
					☑ Casilla de	Recibe correo con IMAP Secure	☐ Casilla de	0.5
					☑ Casilla de	Transfiere archivos por FTPS	☐ Casilla de	0.5
					☑ Casilla de	Administra sus dispositos SSH	☐ Casilla de	0.5
					☑ Casilla de	Las redes inalbricas son WPA2	☐ Casilla de	0.5
	4	Identificación de equipos en redes	58	¿Dispone de procedimiento para identificar automaticamente los equipos conectados a la red? (considerar que alguien ocupe una dirección fija)	NO			
					SI		☐ Casilla de	4
	5	Proteccion de puertos de diganóstico y configuración	59	¿Dispone de un inventario y controles de acceso a los pueros de diagnóstico y configuración?	NO			
					SI	Imventario	☐ Casilla de	2
						Control	☐ Casilla de	3
	3	Separación de redes	60	¿Se encuentran separadas las redes (vlans) por grupos de servicios o usuarios?	NO			
					SI		☐ Casilla de	3
	4	Control de Conecciones de redes interorganizacionales	61	¿Restringe a los usuarios las conecciones a redes interorganizacionales?(interministerial)	NO			
					SI		☐ Casilla de	4
	5	Encaminamiento (routing) de red	62	¿Conoce usted las rutas de encaminamientos(tracert o routing) que siguen los flujos de información en su organuizacion?	NO			
					SI		☐ Casilla de	3
					Se realizan validaciones peridicicas del flujo		☐ Casilla de	2
	4	Control de acceso y gestión de sistemas operativos	63	¿Disponde de una solución integral (tipo Active Directory o LDAP) que abarque la administración de los usuarios, permisos de sistema operativos y limites de sesion?	NO			
					SI		☐ Casilla de	4
	3	Politica de uso Equipos portatiles o moviles	64	Dispone de una politica que incluya medidas de seguridad para la utlizacion de equipos portatiles o moviles?	NO			
					SI	Verbal/AdHOC	◯ Botón de	1.00
						Desarrollo de Politica Formal	◯ Botón de	2.00
						Documento de Politica	◯ Botón de	3.00
	3	Política de Teletrabajo	65	¿Dispone de una politica de actividades y procedimientos para el teletrabajo?	NO			
					SI	Verbal/AdHOC	◯ Botón de	1.00
						Desarrollo de Politica Formal	◯ Botón de	2.00
						Documento de Politica	◯ Botón de	3.00

Anexo 1: (Continuación)

Adquisición, desarrollo y mantenimiento de los sistemas de información	3	Especificación de requisitos de seguridad en los sistemas de información	66	¿Especifica en los TDR para nuevos sistemas o mejoras a los existentes requisitos de controles de seguridad?	NO			
					SI		☐ Casilla de	3
	4	Tratamiento de las aplicaciones	67	¿Dispone de metodos que validen alguno de los siguientes controles?	NO			
					Se validan los datos de entrada		☐ Casilla de	1
					Vigila como las aplicación procesa los datos		☐ Casilla de	1
					Crifa la comunicación de las aplicaciones		☐ Casilla de	0.5
					Cifra los mensajes que su aplicación transnmite		☐ Casilla de	0.5
					Se validad los datos de salida		☐ Casilla de	1
	3	Cifrado de contraseñas	68	¿Dispone de un método de gestión y cifrado de contraseñas?	NO			
					SI		☐ Casilla de	1
					Se utliza un salt para almacenarlas		☐ Casilla de	2
	4	Seguridad de los archivos de sistema	69	¿Dispone de alguno de los siguientes procedimientos para garantizar la seguridad de los archivos de los sistemas?	NO			
					SI	Contola la instalación del software en sus diferentes ambientes	☐ Casilla de	1
						Selecciona, controla y protegue cuidadosamente los datos de prueba	☐ Casilla de	2
						Se encuentran restringuido el acceso al codigo fuente de los sistemas	☐ Casilla de	1
	4	Control de cambios en aplicativos	70	¿Dispone de procedimientos formales de control de cambios realizados en los aplicativos?	NO			
					SI	Se encuentran documentados	☐ Casilla de	2
						Registro de versionamiento	☐ Casilla de	2
	3	Revisión tecnica de aplicaciones tras cambios en el sistema operativo	71	¿Cuándo se realizan modificaciones en el sistema operativo verifca el correcto funcionamiento de las aplicaciones críticas?	NO			
					SI		☐ Casilla de	1.5
					Dispone de un procedimiento formal de pruebas		☐ Casilla de	1.5
	4	Control de paquetes de software	72	¿Dispone de hegemonia en los paquetes de software en los usuarios?	NO			
					SI		☐ Casilla de	2
					Controla y limita sus cambios		☐ Casilla de	2
	5	Fugas de información	73	¿Ha identificado las potenciales situaciones que puedan permitir fugas de información?	NO			
					SI		☐ Casilla de	2
					Existen reglas o procedimientos formales para prevenirlas		☐ Casilla de	3
	4	Control de desarrollo de sistemas externo	74	¿Dispone registros de control y supervisión del software que se desarrolla externamente?	NO			
					SI		☐ Casilla de	4
	5	Control de vulnerabilidades	75	¿Dispone de información acerca de las vulnerabilidades tecnicas de sus sistemas de información?	NO			
					SI	Con analisis de vulnerabilidades interno	☐ Casilla de	1
						Con analisis de vulnerabilidades externo	☐ Casilla de	1
						A realizado una evaluación del riesgo en base a la vulnerabilidades encontradas	☐ Casilla de	1
						Adoptado medidas para remediar la vulnerabilidad y reducir el riesgo	☐ Casilla de	2

Anexo 1: (Continuación)

Gestión de incidentes de seguridad	4	Notificación de eventos y puntos debiles de seguridad	76	¿Disponde de un procedimiento formal para la notificación de eventos de seguridad?	NO			
					SI		☐ Casilla de	1
			77	¿Están consientes los actores involucrados que deben notificar cualquier anomalia o sospecha de seguridad en los sistemas?	NO			
					SI		☐ Casilla de	1
	3	Responsabilidad y procedimientos ante eventos de seguridad	78	¿Cómo actua para gestionar un eventos de seguridad?	NO			
					SI	Adhoc-Toma acciones en el momento	◯ Botón de	1
						Existe un responsable	◯ Botón de	2
						Se tienen establecidos los pasos a seguir	◯ Botón de	3
	4	Valoración de incidentes de seguridad	79	¿Dispone de un mecanismo para cuantificar un incidente de seguridad?	NO			
					SI	Toma en cuenta los costos	☐ Casilla de	1
						Los clasifica por tipos	☐ Casilla de	1
						Determina la afectación	☐ Casilla de	2
	5	Recoplación de evidencias	80	¿Dispone usted de personal capacitado o contrata personal externo(forence o perito informatico) para buscar las evidencias que sustenten un evento de seguridad? (el objetivo es tomar acciones civiles o penales)	NO			
					SI		☐ Casilla de	5
Gestión de la continuidad del negocio	4	Plan de continuidad de negocio	81	¿Dispone de un plan de continuidad de negocio?	NO			
					SI	Adhoc - Verbal -Cuando sucede	◯ Botón de	1
						Se encuentra en desarrollo	◯ Botón de	2
						Se lo tiene implantado	◯ Botón de	3
			82	¿Ha identificado y avaluados los riesgos que pueden causar interrupciones a la contiuidad del negocio?	NO			
					SI			1
	5	Mantenimiento del plan de continuidad del negocio	83	¿Dispone de un único marco de referencia para asegurar que los planes de continudad sean coherentes?	NO			
					SI		☐ Casilla de	2
			84	¿Ha realizado revisiones a sus planes de continuidad?	NO			
					SI	Se han realizado simulacros	☐ Casilla de	1
						Se actualizan perdiodicamente	☐ Casilla de	1
						Mantiene indicadores de eficiencia plan	☐ Casilla de	1

Anexo 1: (Continuación)

Cumplimiento	4	Cumplimiento de requisitos legales	85	¿Ha identificado los requisitos legales de seguridad aplicables para los sistemas de su organización?	NO			
					SI		☐ Casilla de	0.5
			86	Se han identificado los requisistos legales sobre los derechos de propiedad intelectual y uso de productos de software(licencias)?	NO			
					SI		☐ Casilla de	0.5
			87	¿Protegen los documentos importantes de acuerdo a los requisitos legales, regularios, contractuales y empresariales que los rigen?	NO			
					SI		☐ Casilla de	0.5
			88	¿Aplica la legislación vigente referente a la protección de datos y privacidad de la información?	NO			
					SI		☐ Casilla de	1
			89	¿Ha sociabilizado las acciones y/o consecuencias del uso indebido de los recursos de tratamiento de información?	NO			
					SI		☐ Casilla de	1
			90	¿Se han validado los controles criptograficos utliazados en la organización de acuerdo a los contratos, leyes y regulaciones pertinentes?	NO			
					SI		☐ Casilla de	0.5
	5	Cumplimiento de política y normas de seguridad y Cumplimiento Técnico	91	¿Los directores de cada área hacen que se cumplan las polítcas y normas de seguridad?	NO			
					SI		☐ Casilla de	2.5
			92	¿Existen reuniones períodicas para el analális de resultados que indiquen el cumplimento tecnico de todos los sistemas de información respecto a las politicas y normas de seguridad?	NO			
					SI		☐ Casilla de	2.5
	3	Auditoria de los sistemas de información	93	¿Dispone de alguno de los siguientes procedimiento para las actividades de audirias?	NO			
					Son calendarizadas		☐ Casilla de	1
					Son planificadas para evitar el impacto técnico		☐ Casilla de	1
					Dispone de proteccion para el acceso o uso indebido de los logs de auditoria		☐ Casilla de	1

ANEXO 2

MODELO DE LA METODOLOGÍA

GUÍA DE OBSERVACIÓN

Variable	Inidcadores	Observación	Respuesta	Peso
Politica de Seguridad	Distribución,Publicación y Conocmimiento de la Politíca	Buscar evidencia de la publicacion de la Politica	☑ Casilla de	1
Gestion de Activos y clasificacion de la informacion	Inventario de Activos	Observar si los activos se encuentran identificados	☑ Casilla de	2
	Propiedad de los activos	Escoger una identificacion de activo y preguntar quien es el responsable	☑ Casilla de	2
	Directriz de clasificacion	Observar el procedimiento de etiquetado y manejo de la informacion	☑ Casilla de	2
Seguridad física y ambiental	Perímetros y controles de seguridad física	Dispone de barreras, muros o puestos de vigilacina	☐ Casilla de	1
		Dispone de controles de acceso a las instalaciones	☐ Casilla de	1
		Dispone de controles fisicos de entrada a las áreas críticas de tratamiento (ejemplo servidores)	☐ Casilla de	2
		Dispone de controles de seguridad fisicos a las oficinas o despachos	☐ Casilla de	1
	Areas de acceso publico	Buscar puntos de control desde las areas publicas hacias las areas privadas (ejemplo sala de servidores)	Dispone de puestos de vigilacia	☐ Casilla de	1
			Dispone de controles de acceso fisicos (puertas)	☐ Casilla de	1
			Dispone de controles de acces logico (tarjetas	☐ Casilla de	2
Control de accesos	Responsabilidades del usuario	Bucar si los equipos desatendidos se encuentran bloqueados	☐ Casilla de	1
		Verificar que los puestos de trabajo esten despejados y sin soportes de almacenamiento extraibles.	☐ Casilla de	1
Gestión de incidentes de seguridad	Notificación de eventos y puntos debiles de seguridad	Ir a una estacion de trabajo desocupada de algun colaborador, conectar una flash memory simular que se hace una copia de archivos y luego salir (nadie me conoce) ¿Se conocio el incidente?	☐ Casilla de	2