RESUMEN – TRABAJO DE GRADO

AUTORES	Claudia Yojana Figueroa Vergel
FACULTAD	Facultad de ingeniería
PLAN DE ESTUDIOS	Maestría en Gobierno de Tecnología de la Información
DIRECTOR	Andrés Mauricio Puentes Velásquez
TÍTULO DE LA TESIS	Modelo de gobierno de tecnologías de la información para la gestión de la seguridad de la información en las instituciones prestadoras de salud en el municipio de Ocaña
TITULO EN INGLES	Information technology governance model for information security management in health care institutions in the municipality of Ocaña

RESUMEN
(70 palabras)

El Objetivo el presente trabajo se centró en proponer un modelo de gobierno de tecnologías de la información para la gestión de la seguridad de información en las Instituciones Prestadoras de Salud en el Municipio de Ocaña. La gestión de la seguridad constituye un reto para las organizaciones en materia de implementación, las cuales deben dimensionar las implicaciones y el nivel de esfuerzo requerido, a partir de una correcta etapa de planeación.
.

RESUMEN EN INGLES

The Objective of this work focused on proposing an information technology governance model for the management of information security in the Health Providers Institutions in the Municipality of Ocaña. Security management constitutes a challenge for organizations in terms of implementation, which must measure the implications and the level of effort required, starting from a correct planning stage.

PALABRAS CLAVES	Tecnologías de la información, Modelo de gobernanza, Gestión de la seguridad, Salud, Ocaña
PALABRAS CLAVES EN INGLES	Information technology, Governance model, Security management, Health care, Ocaña

CARACTERÍSTICAS

PÁGINAS: 83	PLANOS:	ILUSTRACIONES:	CD-ROM:

Modelo de gobierno de tecnologías de la información para la gestión de la seguridad de la información en las instituciones prestadoras de salud en el Municipio de Ocaña

Claudia Yojana Figueroa Vergel

Facultad de ingenierías, Universidad Francisco de Paula Santander Ocaña

Maestría en gobierno de TI

Msc. Andrés Mauricio Puentes Velásquez

Noviembre, 2021

Índice

Listado de figuras

Listado de tablas

Capítulo 1. Modelo de Gobierno de tecnologías de la información para la gestión de la seguridad de la información en las instituciones prestadoras de salud en el Municipio de Ocaña

1.1 Planteamiento Del Problema

El Sistema Único de Acreditación en Salud en Colombia consiste en el conjunto de procesos, procedimientos y herramientas de implementación voluntaria y periódica por parte de instituciones prestadoras de servicios de salud y demás prestadores identificados por el Ministerio de Salud y Protección Social, mediante los cuales se busca comprobar el cumplimiento gradual de niveles de calidad que sobrepasen los requisitos mínimos obligatorios, para la atención en salud, bajo las directrices del Estado y la inspección, vigilancia y control de la Superintendencia Nacional de Salud (Funcion publica, 2014).

Este decreto es referente de la gestión del Gobierno de Colombia para establecer mecanismos que le permitan medir la calidad en la prestación del servicio de salud, considerado como ¨derecho fundamental¨ (Minsalud, 2015), lo cual tiene como base una estricta evolución jurídica frente a la acreditación para prestar todo servicio relacionado con la salud, razón por la que no toda persona natural o jurídica puede hacerlo, siendo válido en cuanto se perfila a la protección de la vida de los usuarios y al ¨goce efectivo del derecho a la salud¨ (Minsalud, Decreto 780 de 2016, 2016), artículo 2.1.1.1, que para el caso particular no se dispone de un modelo de gobierno de las tecnologías que oriente de forma específica a las Instituciones Prestadoras del Servicio de Salud para la acreditación en salud ambulatoria y hospitalaria en Colombia, con trabajo específico en

el grupo de estándares de apoyo administrativo que a su vez tiene el subgrupo de estándares de gerencia de información, situación que dificulta la comprensión y aplicación de la acreditación por parte de prestadores de servicios de salud en Colombia.

El despliegue institucional frente a la acreditación de salud ambulatoria y hospitalaria en IPS de Colombia ha ido mostrando cada vez la importancia de la información dentro de los procesos estratégicos, administrativos, técnicos y operativos, tal como lo indica el Ministerio de Salud y Protección Social (MSPS) ¨El primer tópico es la Información que la EPS brinda al ciudadano como pilar fundamental para la toma acertada de las decisiones del mismo¨ (Minsalud, 2006).

Mediante Decreto 1011 de 2006 se estableció el Sistema Obligatorio de Garantía de Calidad de la Atención de Salud del Sistema General de Seguridad Social en Salud, contemplando como componentes de éste, el Sistema Único de Habilitación, la Auditoría para el Mejoramiento de la Calidad de la Atención de Salud, el Sistema Único de Acreditación y el Sistema de Información para la Calidad. (Minsalud, Decreto 1011 de 2006, 2006).

De igual manera, el MSPS indica define el Sistema de Salud:

Es el conjunto articulado y armónico de principios y normas; políticas públicas; instituciones; competencias y procedimientos; facultades, obligaciones, derechos y deberes; financiamiento; controles; información y evaluación, que el Estado disponga para la garantía y materialización del derecho fundamental de la salud. (Minsalud, Ley 1751 de 2015, 2015), artículo 4.

Otra de las variables incidentes en el escenario de la acreditación es que la mayoría de los prestadores comparten la idea que estos estímulos deberían ser de tipo

económico. Por otro lado, la acreditación es un poderoso impulsador del mejoramiento continuo y de la calidad, fomenta una adecuada cultura organizacional envolviendo a todo el personal de la organización en el desarrollo de esta metodología, fomenta la satisfacción del usuario y la obtención de mejores resultados de salud (Henao, 2013).

Al tratarse de un proceso continuo y en el que solo llegan a percibirse en el largo plazo los resultados, puede suponerse que esta situación genera apatía por parte de las instituciones para iniciar la búsqueda de la acreditación. Una muestra de esto sería que, aunque en el país se está hablando de acreditación desde el año 1993, apenas en el año 2005 se acreditó la primera institución prestadora de servicios de salud: se erigió como precursor el "Instituto del Corazón de la Fundación Cardiovascular" de la Ciudad de Bucaramanga, Departamento de Santander. Esta distancia temporal y las pocas instituciones acreditadas en la actualidad, son un indicador contundente de la falta de interés en este proceso. En la actualidad en Colombia se encuentran 38 Instituciones Prestadoras de Servicios de Salud acreditas distribuidas en las ciudades Bogotá, Medellín, Cali, Barranquilla, Bucaramanga entre otras.

No disponer de un modelo de gobierno de las tecnologías que mediante estándares de gerencia de la información contribuya a la acreditación de salud ambulatoria y hospitalaria en Colombia, se considera como una debilidad contextual para aquellos prestadores de servicios de salud que aspiran a lograr cumplir con tales paràmetros de calidad, alejándose de la posibilidad de certificaciòn voluntaria y por ende el crecimiento de estas IPS, cuya función es esencial dentro del sistema de salud en Colombia.

1.2 Formulación Del Problema

¿Qué estándares se requieren para diseñar un modelo de gobierno de tecnologías para la gestión de la seguridad de información en las instituciones prestadoras de salud del Municipio de Ocaña?

1.3 Objetivos

1.3.1 Objetivo General

Proponer un modelo de Gobierno de tecnologías de la información para la gestión de la seguridad de información en las Instituciones Prestadoras de Salud en el Municipio de Ocaña.

1.3.2 Objetivos Específicos

Analizar los estándares de gobernanza corporativa de TI aplicables al sector salud.

Diagnosticar el nivel de seguridad y privacidad de la información en las Instituciones Prestadoras de Salud en el Municipio de Ocaña.

Estructurar los componentes del modelo de gestión de seguridad de la información.

1.4 Justificación

El Sistema Único de Habilitación se configura como la puerta de entrada al Sistema Obligatorio de Garantía de la Calidad de la Atención en Salud del Sistema General de Seguridad Social en Salud, es así como, la habilitación consiste en una evaluación externa, de carácter gubernamental y obligatoria, orientada a garantizar unas condiciones mínimas de seguridad, de manejo del riesgo y de dignidad para los usuarios, sin las cuales no se pueden ofrecer ni contratar servicios de salud, cuya vigilancia es de la competencia del Estado, específicamente de las Direcciones Territoriales de Salud (Ministerio de protección social, 2015).

Desde esta óptica, el sistema busca fortalecer la atención en salud para ofrecerle a la sociedad colombiana un mejor sistema de seguridad social en salud. Esto significa que las instituciones de salud promoverán mejores prácticas de atención y cuidado de los pacientes, luego de reformular estándares para alcanzar niveles superiores de calidad (Minsalud, 2017).

Por consiguiente, el sistema de información para la calidad, que permitirá estimular la competencia por calidad entre los agentes del sector y orientar a los usuarios en el conocimiento de las características del sistema, en el ejercicio de sus derechos y deberes, así como de los niveles de calidad de los prestadores de servicios de salud, las entidades promotoras de salud del régimen contributivo y subsidiado, las entidades adaptadas y las empresas de medicina preparada, para que puedan tomar decisiones informadas en el momento de ejercer sus derechos en el Sistema General de Seguridad Social en Salud (Ministerio de protección social, 2015).

Teniendo en cuenta la importancia de la información dentro de los procesos de acreditación para la prestación de servicios de salud, el presente modelo de gobierno de

las tecnologías para la gerencia de la información en IPS con enfoque a la acreditación en salud ambulatoria y hospitalaria, versión 3,1 (Minsalud, 2017) será una herramienta fundamental para aquellas empresas que aspiren a tales estándares de calidad, para lo cual se tendrá el estricto apego a la norma jurídica establecida por el gobierno colombiano, así como el ajuste específico a la figura de las IPS, lo cual redundará en eficiencia y eficacia en procesos enfocados a tal proceso de acreditación voluntaria, pero fundamental para consolidarse como entidades que garanticen la calidad en la oferta de servicios de salud.

De igual manera, algunos factores que llevan a las instituciones a buscar la acreditación es la existencia de estímulos concretos, que pueden brindarse como: facilidades para la contratación, mejora en las condiciones que imponen las aseguradoras, reducción en los aranceles de importación, Prestigio y reconocimiento al recibir el máximo sello de calidad del país y el de ISQua, inclusión de las instituciones acreditadas como cabeza del escalafón de instituciones de salud desarrollado por el Ministerio de Salud, Posibilidad de exportación de servicios de salud, Prioridades para el acceso a becas y créditos ofrecidos por el gobierno para el personal que labora en las instituciones, Beneficios del “Plan Vallejo”, al permitir la suspensión total o parcial de los derechos de aduana, diferir del pago del IVA y reducción al 0% del arancel aduanero para el uso de bienes de capital, importación de insumos, materia prima, dotación, maquinaria, y equipos de uso en la prestación del servicio, Condiciones especiales para el acceso a las zonas francas, Inclusión en las redes de servicios de las EPS que operen en la región.

1.5 Delimitaciones

1.5.1 Delimitación Operativa:

El proyecto de investigación adoptará los lineamientos metodológicos establecidos por la Universidad Francisco de Paula Santander Ocaña para la Maestría en Gobierno de Tecnología de la Información, bajo el trabajo mancomunado entre la maestrante y el director del proyecto, lo cual implica la toma de decisiones sobre el abordaje y la resolución de deficiencias que posiblemente se presenten durante la elaboración del mismo; tales como la necesidad de reajuste de técnicas de recopilación de información, no hallazgo de ciertas fuentes primarias de datos, así como manejo de plazos para la presentación del informe final.

1.5.2 Delimitación Conceptual:

El proyecto abordará conceptos asociados tales como: Buenas prácticas, Gobierno de TI, Gobernanza Corporativa, Información, seguridad de la información, acreditación en salud, salud ambulatoria y salud hospitalaria, Estándares de acreditación.

1.5.3 Delimitación Geográfica:

Actualmente en Colombia existen alrededor de 8.000 Instituciones Prestadoras de Salud, de las cuales solo 37 se encuentran acreditadas. La presente investigación está dirigida a las Instituciones prestadores de salud o IPS presentes en el municipio de Ocaña, Norte de Santander. Se tomará como referente el Centro de Eco Radio Diagnóstico S.A.S.

1.5.4 Delimitación temporal:

La revisión documental relacionará los parámetros de la temática, a partir de fuentes confiables y vigentes. En cuanto al tiempo que conlleva la realización de la investigación, se proyecta que esta sea realizada en un lapso de un año a partir de la aprobación de la presente propuesta de trabajo de grado.

Capítulo 2. Marco Referencial

2.1 Marco Histórico

Según datos históricos, en el siglo XIX se inició un proceso de ámbito mundial para dar procesamiento informático a la información, desde un contexto de gestión y comunicación, este hecho sencillo marcó el inicio de todos los procesos y procedimientos en la gestión de las TI del mundo; dicho procesamiento informático, se orienta en términos de análisis, diseño, desarrollo, mantenimiento y administración de la información por medio de sistemas informáticos. Para los años noventa, ya se había consolidado un conjunto de mecanismos que aseguraba lograr las capacidades de las TI necesarias para la óptima operación de los procesos de negocio (Weill & Ross, 2014).

En la actualidad, la gestión de TI en ámbitos internacionales está regida por sus requisitos funcionales (MinTic, 2008) donde se ha sofisticado el término (gestión de TI) a tal punto de establecer un modelo de negocio; este lineamiento permite cumplir con los requerimientos básicos planteados en las organizaciones, lo cual indica que el desarrollo tecnológico se presenta ante los ámbitos nacionales colombianos como herramientas ya ejecutadas y probadas. En los años setenta, en Colombia, se inició un proceso de importación de tecnologías informáticas, las cuales fueron aprovechadas por las instituciones para el mejoramiento de los procesos gerenciales, dando así comienzo a la gestión de las tecnologías de la información en el entorno nacional; es importante aclarar que los sistemas de información actuales, en ámbitos nacionales y locales, son herramientas construidas principalmente en el País, pero su base fundamental de desarrollo está guiada por lineamientos internacionales. Este rol fue vivido en varios países, de diversas formas y en acuerdo con su desarrollo cultural (Borrero, 2004).

2.1.1 Antecedentes.

Para (Yañez, 2017) en su investigación titulada “Sistema de gestión de seguridad de la información para la subsecretaria de economía y empresas de menor tamaño” de la universidad de Chile, Esta tesis propone que la metodología de implementación de SGSI se apoye en la gestión de riesgos, utilizando las guías y buenas prácticas de la norma ISO31000. Con ello los procesos estratégicos de la subsecretaría son clasificados por prioridad según su exposición a los riesgos y su impacto. De este modo se optimiza la asignación de recursos a los proyectos de seguridad de la información, se favorece el aprendizaje y la creación de equipos de trabajo orientados a los objetivos prioritarios, sin que ellos perdieran la visión de conjunto y objetivo final.

Como evaluación de la implementación del SGSI y de las políticas y procedimientos de seguridad de la información se realizaron dos auditorías, una interna y otra realizada por una empresa externa. Ambas auditorias fueron totalmente independientes al equipo que diseñó e implementó tanto el SGSI como las políticas y procedimientos de seguridad de la información. Ambas auditorias llegaron a la conclusión que el estado actual de seguridad de la información está en un nivel medio. Esto es un avance sustancial pues al inicio de la presente tesis no había un SGSI ni políticas y procedimientos efectivos para proteger la seguridad de la información. La principal recomendación entregada por las auditorías fue profundizar la difusión de las políticas y procedimientos de seguridad de la información, continuar con la implementación de los restantes 70 objetivos de control de la norma ISO27001:2013 y realizar una nueva evaluación durante el 2017 del funcionamiento del SGSI, es decir se

han implementado los restante objetivos de control y evaluar el grado de institucionalización de las políticas y procedimientos de seguridad de la información.

La metodología que se utiliza esta tesis, se centra en ciclos de aprobación que permitan establecer consensos y conciliar visiones en torno a un fuerte sentimiento de trabajo en equipo para facilitar la implementación de las políticas y procedimientos de seguridad de la información.

Este trabajo de investigación sirve como soporte para direccionar los objetivos de la presente investigación, ya contiene información relevante sobre los sistemas de gestión de la seguridad de la información que es el eje de desarrollo de la problemática planteada.

Por su parte, (Talabera, 2015), en su investigación "Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013" analizan como las instituciones públicas deben adaptarse a los nuevos cambios legislativos mediante la implementación, de manera complementaria con las nuevas normas que regulan los temas de privacidad y seguridad, de mecanismos de control y seguimiento de seguridad de la información. Sin embargo, como se mencionó previamente, la normativa aprobada si bien da recomendaciones a seguir para la Implementación de un SGSI, no indica exactamente la metodología o pasos a seguir para lograr este objetivo.

Donde se evidencia la necesidad de las instituciones públicas de contar con un análisis que les permita realizar el diseño de un SGSI, en conjunto con los controles correspondientes al mismo como respuesta a la exigencia legal establecida por las

normas previamente mencionadas, además de la falta de una guía que acompañe el proceso a seguir para realizar dicho diseño a medida según los requerimientos específicos de una entidad prestadora de salud como el INMP, constituyen la problemática que este Proyecto de Fin de Carrera pretende resolver siguiendo las buenas prácticas y estándares internacionales correspondientes que permitan realizar una identificación de la información crítica con la que trabaja la institución y en consecuencia definir los riesgos a los que se encuentra expuesta y los controles que deberían implementarse para garantizar su seguridad.

Concluyendo que se pudo verificar el gran retraso en el proceso de implementación, en comparación con la programación establecida por la ONGEI para todas las instituciones públicas, del INMP en cuanto a la Norma Técnica Peruana NTP ISO/IEC 27001:2008. No se ha gestionado actualmente el proyecto de implementación a pesar de que el plazo final previo a la fase regulatoria venció en el presente año. Es notorio que el principal interés de la institución es realizar inversiones relacionados a los servicios de salud.

Los resultados obtenidos por el autor, se aproximan a la situación objeto de estudio, las empresas de salud del municipio de Ocaña no poseen procesos estandarizados que cumplan con lo establecido por la ley según el Manual de Acreditación en Salud Ambulatorio y Hospitalario de Colombia, lo que se constituye en una deficiencia a solventar si se está en riesgo de una sanción.

De igual forma, (Lepage, 2014) en su trabajo de grado “Diseño de un modelo de gobierno de ti con enfoque de seguridad de información para empresas prestadoras de

servicios de salud bajo la óptica de COBIT 5.0" de la Pontificia Universidad Católica del Perú. Estudia como non la reciente publicación de la ley de protección de datos personales y la actualización de las dos (2) principales normas de la familia de la ISO 27000, se verifica la importancia de la información dentro de las organizaciones.

En el caso de las empresas prestadoras de servicios de salud, el sector ha ido creciendo tras la necesidad de los clientes por contar con un servicio de excelencia para toda la familia y detección de enfermedades, por ello se crean nuevos programas para tener acceso a estos servicios, teniendo como consecuencia el incremento de datos e información.

Por esa razón, se ven en la necesidad de incrementar y/o mejorar su infraestructura tecnológica para soportar sus procesos de negocio, mejorando la calidad y rapidez de sus servicios, integrando datos provistos por otras entidades y velando por la confidencialidad de la ellos de acuerdo al marco regulatorio al que están sujetas. No obstante, se debe garantizar el alineamiento estratégico y la correspondencia de esta tecnología con los objetivos de negocio que aseguren el retorno de la inversión.

A partir de lo expuesto, se plantea una solución integrada que brinde un enfoque estratégico y comprometa a la Alta Dirección para que participe del cambio que conlleve a que las empresas logren sus objetivos de la mano de tecnología correctamente gestionada. Esta solución es diseñar un Gobierno de Tecnología de Información con enfoque a seguridad de información, velando por el cumplimiento de los cinco (5) pilares que son el alineamiento estratégico, la entrega de valor o retorno de inversión, medición del desempeño de TI, gestión de riesgos y gestión de recursos.

Para el proyecto se empleará un marco de negocio mundialmente reconocido, COBIT 5.0, que brinda buenas prácticas para implementar esta solución dentro de cualquier organización según sea el contexto. Así mismo, integra una serie de marcos reconocidos y permite su uso desde una alta perspectiva de negocio y finalmente presentarse como una alternativa de solución ante una problemática generalizada a nivel estratégico y tecnológico en las empresas prestadoras de servicio de salud.

Los procesos de estandarización se deben soportar en la empresa no solo como un mecanismo de cumplimiento de normas, sino como un método de mejoramiento continuo, por lo tanto contar con estas herramientas en la organización la direcciona de forma correcta en la consecución de los objetivos, por lo tanto esta investigación propone uno de los sistemas que se pueden utilizar para el cumplimiento de lo establecido en la ley, el cual esta descrito en uno de los objetivos específicos de la presente investigación.

También (Marulanda, Lopez, & Valencia, 2017), en su investigación "Gobierno y gestión de ti en las entidades públicas" de la Universidad EAFIT de Colombia. Presentan los resultados del estudio sobre el estado y alcances del gobierno de TI y la gestión de TI en las entidades públicas de la ciudad de Manizales, departamento de Caldas, Colombia. Se realizó una evaluación por medio de encuesta, que se aplicó a 19 entidades públicas.

Se desarrolló la investigación desde una óptica inductiva y con un tipo de estudio descriptivo exploratorio y correlacional. Se concluyó que el gobierno de TI es

una realidad para una pequeña porción de dichas entidades. Se espera que con los resultados obtenidos se puedan desarrollar planes conjuntos entre universidades públicas y las entidades para generar un mayor desarrollo de su gobierno y la gestión de TI.

El gobierno y la gestión de TI han sido objeto de estudio en los últimos años por parte de la comunidad académica, en búsqueda de hacer de las mismas una parte integral de la estrategia de la organización, para lo cual se necesita no solo contemplarlas como recursos de hardware y software, sino establecer los factores que determinan la forma de liderar y controlar las TI por parte de la alta dirección para que su operación sea efectiva en el día a día de la organización.

El Gobierno colombiano viene desarrollando estrategias, planes, programas, proyectos y modelos relacionados con el gobierno de TI y con la estrategia correspondiente, condicionado a su aplicación de parte de las entidades públicas; en consecuencia, la idea con este artículo es mostrar, a partir de los resultados, el estado de su aplicación en las entidades estatales de Manizales, Caldas, Colombia.

Teniendo en cuenta los referentes de este artículo es importante conocer como es el manejo del gobierno TI en las entidades públicas, ya que estas se rigen a partir de una reglamentación diferente a las privadas, para la presente investigación estas deben regirse según la normatividad de salud vigente.

2.2 Marco Teórico

A continuación, se presentan algunas teorías que apoyan la presente investigación y hacen un aporte significativo para reflejar un resultado mucho más acertado

2.2.1 Gobierno de TI.

Como lo menciona Brisebois (s/f), en su artículo "What is IT Governance? and why

is it important for the IS auditor", apegándose a la definición brindada por el IT Governance Institute, El Gobierno de TI consiste en el liderazgo, estructuras organizativas y procesos que aseguren que la organización de TI pueda sostener y ampliar los objetivos y estrategias de la organización. Siendo esta, parte integral del gobierno empresarial y responsabilidad del consejo directivo y los ejecutivos de gestión.

Sus retos y preocupaciones a resolver son:

- Marco de trabajo de alto nivel
- Obtención de valor de negocio a través de TI
- Gestión de Recursos
- Gestión de Riesgos
- Alineamiento estratégico entre TI y Negocio
- Gestión del Rendimiento

Mediante el gobierno de TI se busca asegurar que las inversiones realizadas en tecnología otorguen el valor añadido esperado a la Organización y que puedan ser mitigados los riesgos asociados a TI. El gobierno de TI es un tema administrativo, sino un tema estratégico que debe de ser observado por la alta dirección. Brisebois (s/f) lo describe en su artículo "La gobernanza no es acerca de los que toman decisiones, eso es

la gestión de TI, el gobierno de TI se trata de quién toma las decisiones y cómo se hacen".

Por tanto en el gobierno de TI se construirá una estructura de relaciones y procesos que apoyen la alineación estratégica de TI con la organización de tal manera que se obtenga el valor máximo a través de controles efectivos en el mantenimiento y desarrollo efectivo de las tecnologías de información (Carrera, 2011).

2.2.2 Teoría Del Mejoramiento Continuo – Kaizen

El sistema al cual se hace referencia se denomina Kaizen, lo cual significa "mejora continua que involucra a todos". Es pues un sistema integral y sistémico destinado a mejorar tanto a las empresas, como a los procesos y actividades que las conforman, y a los individuos que son los que las hacen realidad. El objetivo primero y fundamental es mejorar para dar al cliente o consumidor el mayor valor agregado, mediante una mejora continua y sistemática de la calidad, los costes, los tiempos de respuestas, la variedad, y mayores niveles de satisfacción; esta teoría presenta 10 principios enfoque en el cliente, Realizar mejoras continuamente, Reconocer abiertamente los problemas, Promover la apertura, Crear equipos de trabajo, Manejar proyectos a través de equipos ínter funcionales, Desarrollar la autodisciplina, Información constante a los empleados, Fomentar el desarrollo de los empleados (Sanchez, 2012).

Esta teoría muestra la relación existente entre la innovación y la mejora continua y apoya el presente estudio desde el punto de vista que para contrarrestar las afectaciones que genera el no cumplimento de la norma se debe estar en un cambio

permanente y en disposición al cambio; de lo contario será tan traumático para las organizaciones que les costara hasta la continuidad del negocio, debido a las sanciones que estarán expuesta ante el Ministerio de salud.

2.2.3 Teoría de la información.

La Teoría de la Información nos muestra, entre otras cosas, el camino a seguir para determinar la cantidad de información útil a partir de unos datos. Y para comprimir la información de manera que los datos se representen de una manera eficiente. Nace de la necesidad de optimizar los contenidos de las informaciones, en una época histórica en la que la comunicación alcanzaba un destacado papel (Shannon, 1948), esto después del nacimiento del código binario (Hartley, 1927) y los primeros pasos de encriptación (Turing, 1936). En consecuencia, se debía encontrar una forma en la cual determinar "la cantidad de información" que entregaba un mensaje.

El mayor investigador de este tema fue Claude Shannon quién aportó el concepto de que la información debe dejar de verse como inmaterial y subjetiva, sino que como perfectamente material y cuantificable. Así pasó a considerarse de una manera independiente un dispositivo de representación y se dio la posibilidad de hablar de procesos de representación y manipulación de la información sin hacer énfasis si era el cerebro o un ordenador quien realizaba dichos procesos. Esto permitió, dar el primer paso para la cibernética: el control de las máquinas para realizar tareas humanas (Tomas, 2014).

2.2.4 Seguridad de la información desde la Teoría de las Limitaciones

El eslabón más débil de la cadena.

A cualquier profesional le suena: "La seguridad es como una cadena, es tan fuerte como el eslabón más débil". Esto se dice por varios motivos: Para enfatizar la naturaleza de seguridad como proceso, como sistema, pero también para entender que se trata de una posición de defensa débil, es decir, el defensor tiene que defender todos los puntos, mientras que al atacante le basta con encontrar un punto vulnerable para tener éxito en su ataque.

Sin embargo, aunque se está convencido de que esto es así, muy pocos (por no decir, ninguno) realiza la gestión de este proceso conforme a esta máxima. Porque si se gestionará la seguridad teniendo este paradigma en mente, lo mejor sería emplear la misma estrategia que cualquier otro sistema cuya producción esté gobernada por su factor limitante. Me explico, después de identificarlo, habría que hacer que este factor limitante produjese al máximo nivel.

Esta forma de gestionar la seguridad cambiaría sobremanera el enfoque actual del proceso de gestión. Si se sigue lo establecido en los estándares, por ejemplo, el estándar ISO/IEC 27001 que establece las pautas para montar un Sistema de Gestión de la Seguridad de la Información (SGSI) "certificable", tenemos que (como ya hemos comentado aquí anteriormente) llevar a cabo un análisis de riesgos que nos permita identificar el nivel de riesgo por cada área o dominio del alcance establecido y pasar a gestionar el riesgo en función de la estrategia definida.

Si se plantea la seguridad como un sistema en el que el output fuera el nivel de seguridad de la organización (parece obvio, ¿no?), el máximo nivel estaría marcado por el máximo caudal que pudiera gestionar el cuello de botella del sistema, es decir, el nivel de seguridad de la organización sería el del eslabón más débil de la cadena.

¿Cuál es la diferencia entre estas dos maneras de gestionar la seguridad? la diferencia es que no tendría tanto interés realizar un análisis de riesgos como el hecho de encontrar cuál es el factor limitante, cuál es el eslabón más débil, puesto que sería el que marcaría el nivel de seguridad de nuestra organización. A partir de ahí, si se quiere elevar el nivel de seguridad de nuestra organización, se debería gestionar esa limitación y eso, ya se sabe, hay que preguntarle a Goldratt el cómo (Ramos, 2016).

2.2.5 Teoría de la seguridad por oscuridad Gaming.

Shannon buscó la seguridad contra el atacante con poderes computacionales ilimitados: si la información transmite cierta información, a continuación, el atacante de Shannon seguramente va a extraer esa información. Diffie y Hellman refinaron el modelo atacante de Shannon al tener en cuenta el hecho de que los atacantes reales son computacionalmente limitados. Esta idea se convirtió en uno de los grandes nuevos paradigmas en ciencias de la computación, y condujo a la criptografía moderna.

Shannon también buscó la seguridad contra el atacante con poderes lógicos y observacionales ilimitadas, expresada a través de la máxima de que "el enemigo conoce el sistema". Este punto de vista todavía es refrendado de la criptografía. La formulación popular, que se remonta a Kerckhoffs, es que "no hay seguridad por oscuridad", lo que

significa que los algoritmos no se pueden mantener ocultos al atacante, y que la seguridad sólo debe confiar en las claves secretas. De hecho, la criptografía moderna va más allá de Shannon o Kerckhoffs en asumir tácitamente que si hay un algoritmo que puede romper el sistema, entonces el atacante seguramente encontrará ese algoritmo. El atacante no es visto como un equipo omnipotente más, pero él todavía se interpreta como un programador omnipotente (Meneses & Ramirez , 2016).

2.3 Marco Conceptual

La Seguridad de la Información es el conjunto de metodologías, prácticas y procedimientos que buscan proteger la información como activo valioso, con el fin de minimizar las amenazas y riesgos continuos a los que está expuesta, a efectos de asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de inversiones y las oportunidades del negocio. Y en el caso de cada individuo de proteger la identidad y la privacidad (Meneses & Ramirez , 2016).

Desde esta óptica, es importante conocer cada uno de los conceptos más relevantes que harán parte del fundamento de la presente investigación.

***2.3.1 Tecnologías de la Información*.** Son Aquéllas cuyo propósito es el manejo y tratamiento de la información, entendida ésta como conjunto de datos, señales o conocimientos, registrados o transportados sobre soportes físicos de muy diversos tipos. Las tecnologías de la información abarcan técnicas, dispositivos y métodos que permiten obtener, transmitir, reproducir, transformar y combinar dichos datos, señales o conocimientos (Esquivia, 2018).

2.3.2 Gobierno Corporativo. Es el sistema por el cual las sociedades son dirigidas y controladas. La estructura del gobierno corporativo especifica la distribución de los derechos y responsabilidades entre los diferentes participantes de la sociedad, tales como el directorio, los gerentes, los accionistas y otros agentes económicos que mantengan interés en la empresa (ODEC, 2010) Citado por (Muñoz & Ulloa, 2011).

2.3.3 Gobierno de Tecnologías de Información. El gobierno de las TI especifica los procedimientos de toma de decisiones y los esquemas de responsabilidad para alcanzar el comportamiento deseado en el uso de las TI (Weill & Ross, 2014).

2.3.4 Gestión de TI. La gestión de TI es responsabilidad de los ejecutivos y de la junta directiva y hacen parte de ella el liderazgo, las estructuras organizativas y los procesos para garantizar que las mencionadas tecnologías de la empresa sustenten y extiendan las estrategias y objetivos de la empresa (Brandis, 2014).

2.3.5 Entrega del valor. Se refiere a ejecutar la proposición de valor a través de todo el ciclo de entrega asegurando que las tecnologías de información otorguen los beneficios acordado alineados con la estrategia, concentrándose en la optimización de costos y demostrando el valor de las TI (Muñoz & Ulloa, 2011).

> Desde el aspecto de la seguridad de información, el manual del CISM[1] sostiene que la entrega de valor se produce cuando las inversiones en seguridad están optimizadas para apoyar a los objetivos de la organización. La entrega de valor es una función de alineación estratégica entre las estrategias de seguridad y

[1] CISM: *Certified Information Security Manager*

los objetivos de negocio. Es decir, cuando un caso de negocio puede ser realizado para todas las actividades de seguridad. Los niveles óptimos de inversión se producen cuando los objetivos estratégicos de seguridad se consiguen y se logra una postura de riesgo aceptable al menor costo posible (ISACA, 2012).

2.3.6 Administración de Riesgos. Se direcciona a salvaguardar los activos de TI y la recuperación de desastres. La administración de riesgos tiene como motor la necesidad de mostrar una buena gobernanza empresarial a los accionistas y clientes.

El riesgo empresarial no es solo a nivel financiero, también existen preocupaciones por el lado operacional y el riesgo sistémico, en el que la tecnología de riesgos y la seguridad de información se vuelven prominentes (Lepage, 2014).

2.3.7 Seguridad de la información. La seguridad de la información hace parte del gobierno corporativo y desde ahí se debe asegurar y establecer su manejo. Con la NTC-ISO/IEC 27001 (2006) el área de tecnología se puede apoyar para identificar los requisitos y establecer los controles requeridos en la gestión de la información (Paéz & Hernandez, 2015).

2.3.8 Gestión de riesgos. Aunque la NTC-ISO/IEC 38500 (2009) plantea que se debe realizar una gestión de riesgos sobre la información, los activos de TI y una valoración de los riesgos como parte de la evaluación de su principio de desempeño, COBIT 5-ISACA (2012) integra los principales marcos de gestión de riesgos y específicamente relacionado con el uso, propiedad, operación, involucramiento, influencia y adopción de la TI dentro de la compañía (RiskIT) QAEC (2015)

El resto de prácticas analizadas tratan de manera más específica la gestión y valoración de los riesgos en la continuidad de la operación del negocio, los proyectos y los activos de TI de la compañía (Paéz & Hernandez, 2015).

2.3.9 Sistema de Información de salud. Se considera así a cualquier sistema, repositorio o conjunto de datos – ya sean bases de datos, datawarehouse, etc. – que almacena información relevante sobre el cuidado de la salud de uno o más pacientes, y que se encuentra almacenada de tal forma que pueda ser transmitida de forma segura por parte de usuarios autorizados según su nivel de acceso a la misma. (ISO 27799, 2008).

2.3.10 Informática de salud. Es la disciplina científica que aplica la informática y tecnologías de comunicación para procesar la información médica necesaria que sirva de soporte a las operaciones de las instituciones del sector salud. En la actualidad constituye una de las más importantes herramientas utilizadas por las entidades prestadoras de salud dada la versatilidad y disponibilidad de la información que se logra mediante el uso de software especializado, permitiendo que la información de los pacientes se mantenga actualizada. (ISO 27799, 2008).

2.3.11 Información personal de salud. Este concepto se refiere a toda aquella información perteneciente a una persona usuaria de los servicios de salud y que describe sus características físicas o mentales, además de todo registro acerca de sus tratamientos, operaciones, medicaciones o servicios que ha recibido por parte de la institución médica correspondiente (Talabera, 2015).

2.3.12 Métodos de archivo de Historia Clínica. Se denomina así a las diferentes técnicas que se utilizan para organizar el Archivo Clínico de la organización prestadora de salud. Tiene por motivo mantener un orden que facilite el archivado y reconocimiento de las Historias Clínicas de los pacientes (Talabera, 2015).

2.4 Marco Legal

2.4.1 Decreto 2618 de 2012. "Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones y se dictan otras disposiciones".

2.4.2 Decreto 2693 de 2012. “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones”.

2.4.3 Ley Estatutaria 1266 Del 31 de diciembre De 2008. Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.17

2.4.4 Ley 1341 del 30 de julio de 2009. Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones

2.4.5 Ley estatutaria 1581 de 2012. Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional. Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

2.4.6 Ley 1712 De 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. 20

2.4.7 Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. 21

2.4.8 Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

***2.4.9 Norma ISO/IEC3850011*. Gobierno corporativo de la tecnología de la información 2009-12-16.** Esta norma es una adopción idéntica (IDT) por traducción, respecto a su documento de referencia, la norma ISO/IEC 38500:2008.

Esta norma proporciona un marco de principios para que los directores los utilicen al evaluar, dirigir y monitorear el uso de la tecnología de la información (TI) en sus organizaciones.

***2.4.10 Certificación del Sistema de Gestión de Seguridad de la Información con ISO/IEC 27001 – ICONTEC*.** El Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), es el Organismo Nacional de Normalización de Colombia. Entre sus labores se destaca la creación de normas técnicas y la certificación de normas de calidad para empresas y actividades profesionales. ICONTEC es el representante de la Organización Internacional para la Estandarización (ISO), en Colombia.

El estándar para la seguridad de la información ISO/IEC 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).

Capítulo 3. Diseño Metodológico

3.1 Tipo de investigación

La Investigación que se propone es de tipo descriptiva, la cual busca especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice. (Hernández, Fernández y Baptista, 2010).

De acuerdo con las características propias de la investigación a desarrollar se aplicara la Investigación con enfoque cuantitativo de tipo transversal descriptiva, que implica recolectar y analizar datos, buscando a través de ella profundizar en el conocimiento de las situaciones, con la finalidad de realizar inferencias sobre el cumplimiento de Estándares de Gerencia de la Información en las Instituciones prestadoras de servicios de salud, obtener mayor objetividad en el tema, diferentes puntos de vista, y lograr una perspectiva más amplia y profunda sobre el tema de estudio.

La técnica de investigación se validara a través de una entrevista semiestructurada la cual se aplicara al personal del área tecnológica, permitiendo conocer más afondo como es el manejo de la información y a los directivos de las Instituciones prestadoras de servicio de salud para saber cómo están frente al cumplimiento de los Estándares de Gerencia de la Información según lo establecido en el Manual de Acreditación en Salud Ambulatorio y Hospitalario de Colombia, ya que para (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014) “la entrevista no estructurada se adopta como entrevista en profundidad. Sus objetivos son comprender más que explicar, maximizar el significado, alcanzar una respuesta subjetivamente sincera más que objetivamente verdadera y captar emociones pasando por alto la racionalidad”.

3.2 Seguimiento metodológico del proyecto

Tabla 1.

Modelo Metodológico.

Objetivos de la investigación	Actividades por objetivo	Indicador por actividades
Obj. 1. Analizar los estándares de gobernanza corporativa de TI para la gestión de la seguridad de información aplicables al sector Salud.	Act. 1. Realizar estado del arte	Ind. 1 Recopilación de estándares identificados
	Act. 2. Analizar de los procesos organizacionales de seguridad de la información en el sector salud.	Ind 2. Caracterización de procesos
Obj. 2. Diagnosticar el nivel de seguridad y privacidad de la información en las Instituciones Prestadoras de Salud en el Municipio de Ocaña	Act. 1. Evaluar los elementos en materia de seguridad.	Ind. 1. Resultados de aplicación de herramienta de evaluación.
	Act. 2. Analizar el grado de seguridad con que cuenta la Entidad.	Ind. 2. Diagnóstico documentado.
Obj. 3. Estructurar los componentes del modelo de gestión de seguridad de la información .	Act. 1. Identificar los elementos que conformarán el modelo	Ind. 1, Elementos identificados
	Act. 2. Estructurar el modelo	Ind. 2. Modelo Estructurado
	Act. 3. Diseñar el modelo	

Fuente: Autora del proyecto.

3.3 Población

La población para la presente investigación incluirá las empresas prestadoras de servicios de salud (IPS) del casco urbano en la ciudad de Ocaña, la cual estuvo

conformada por las 20 Instituciones Prestadoras de Salud (I.P.S) existentes en la ciudad, información suministrada por la oficina de Desarrollo Humano de la Alcaldía de Ocaña. (Apéndice C.)

3.4 Muestra

En la investigación cuantitativa se parte del supuesto que en la mayoría de los casos no es posible medir cada uno de los individuos de la población, por lo tanto, se toma una muestra representativa de la misma. La muestra se justifica en que las partes representan el todo y como tal, refleja las características que definen la población de la cual fue extraída, lo cual es representativa. (Cerda Gutiérrez, 2013)

Para efectos de la recolección de la información se tomará como referente de aplicación de herramientas para la recolección de la información al Centro de Eco Radio Diagnóstico S.A.S.

3.5 Técnica e instrumento de recolección de la información

Desde este punto de vista de las técnicas de investigación, la observación es un procedimiento de recolección de datos e información que consiste en utilizar los sentidos para observar hechos y realidades sociales presentes y a la gente donde desarrolla normalmente sus actividades, para la presente investigación esta buscara identificar las características de la IPS frente a los estándares de gerencia de la información, así como la habilidad y la disposición que estos muestran ante la

implementación del estándar 146 “Existen mecanismos estandarizados, implementados y evaluados para garantizar la seguridad y confidencialidad de la información”.

Se complementara con la técnica de la entrevista, la cual tiene su fundamento teórico en la investigación, debido a que permite recoger información de primera mano y con la fuente principal, al igual que deja aclarar dudas y ver el impacto de las preguntas en los informantes claves; por tal motivo, el instrumento utilizado es el guion de preguntas la mayoría de ellas son de carácter abierto con la intención de poder recolectar la mayor información que permita establecer un resultado acertado a la presente investigación y que refleje el conocimiento de la normatividad de gerencia de la información, en lo concerniente a la seguridad de la información en la empresa.

3.6 Procesamiento y análisis de la información

La investigación se fundamentará con una base documental acerca de la literatura existente sobre los modelos de gobierno en TI y seguridad de la información.

Para el análisis de la información, se procederá a organizar la información recopilada mediante las técnicas de recolección descritas, para posteriormente analizarla y presentar los resultados arrojados por la misma.

La información obtenida a partir de la aplicación de la entrevista dirigida al Gerente de la IPS (Apéndice B), será el insumo que permita estructurar la herramienta de diagnóstico que fundamentará el desarrollo del proyecto.

Capítulo 4. Presentación de Resultados

4.1 Analizar los estándares de gobernanza corporativa de TI aplicables al sector salud.

Mediante la realización de un pertinente proceso de revisión literaria, se identifican los principales estándares de Gobierno asociados a la seguridad de la Información, aplicables a cualquier tipo de organización. La presente investigación, se enfoca hacia el sector salud, en el marco de los siguientes estándares: ISO 38500, COBIT 5.0, ISO 27000 e ITIL.

Tabla 2.

Síntesis de elementos de los Estándares de seguridad.

Nombre del Estándar	Propósito	Áreas/ Dominios	Principios
ISO 38500	1.Asegurar los beneficios para las partes interesadas. 2.Informar y orientar a Directivos que controlan el uso de TI. 3.Ofrecer bases para una evaluación objetiva de TI por parte de la Dirección.	1.Evaluar 2.Dirigir 3.Monitorizar	1.Responsabilidad. 2.Estrategia. 3.Adquisiciones. 4.Desempeño. 5.Conformidad. 6.Comportamiento Humano.
COBIT 5.0	Brindar un marco de trabajo integral orientado al Alcance de los objetivos para el gobierno y la gestión de las TI corporativas.	1.Alinear, Planificar, Organizar (APO). 2.Construir, Adquirir, Implementar (BAI). 3.Entregar, dar servicio y soporte (DSS). 4.Supervisar, evaluar y valorar (MEA). 5. Evaluar, Orientar y Supervisar (EDMO).	1.Satisfacer las necesidades de las partes interesadas. 2. Cubrir la empresa de extremo a extremo. 3. Aplicar un marco de referencia único e integrado. 4. Hacer posible un enfoque holístico. 5. Separar el Gobierno de la Gestión.
ISO 270000 *ISO 27001* *ISO 27002*	Conjunto de buenas prácticas orientadas a la seguridad de la información. Definir los requisitos necesarios para establecer, implementar, mantener y mejorar permanentemente un sistema de gestión de seguridad de la información. Determinar políticas, procedimientos y controles con el objeto de disminuir los riesgos.	1. Política de Seguridad. 2. Organización de Seguridad. 3. Administración de activos. 5.Seguridad de los Recursos Humanos. 6. Seguridad Física y Ambiental. 7.Gestión de Comunicaciones y Operaciones. 8.Sistema de Control de Accesos. 9.Adquisición, Desarrollo y Mantenimiento de Sistemas de Información. 10.Administración de Incidentes. 11. Plan de Continuidad de Negocio.	1.Confidencialidad. 2. Integridad. 3.Disponibilidad.
ITIL	Proporcionar a los administradores de sistemas de TI las mejores herramientas para mejorar la calidad de los servicios y la satisfacción de usuarios, alcanzando simultáneamente los objetivos misionales.	1.Estrategia del servicio. 2.Diseño del Servicio. 3.Trascición del Servicio. 4. Operación del Servicio. 5.Mejora continua del servicio.	1.Enfoque de Valor. 2. Iniciar donde se está. 3.Prograsar iterativamente con Retroalimentación. 4.Colaborar y promover visibilidad.

		5. Pensar y trabajar holísticamente. 6.Mantener lo simple y práctico. 7.Optimizar y Automatizar.

Fuente: Autora del Proyecto.

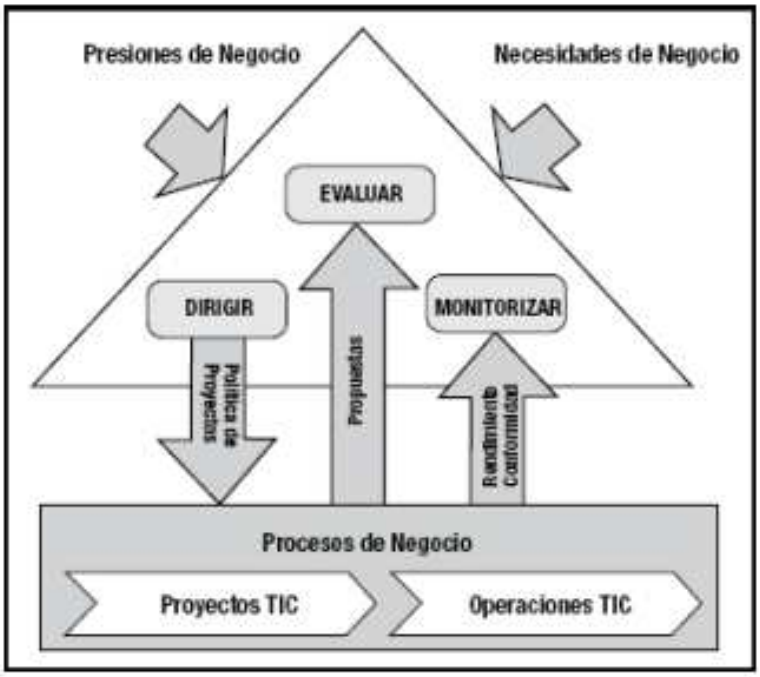
A continuación, se expone la representación gráfica de los elementos más relevantes de los estándares asociados a Gobierno de TI para la Gestión de la Seguridad de la Información:

La **norma ISO 38500** corresponde a un estándar diseñado por la International Organization for Standardization (ISO), cuya orientación tiende al Gobierno Corporativo y de las Tecnologías de la Información para apoyar a las organizaciones en la gobernanza de sus procesos y la toma de decisiones sobre todo en materia de administración de servicios de TI y demás unidades de negocio.

Para dar cumplimiento a los objetivos propuestos, la norma ISO 38500 ofrece un modelo de Gobierno de TI soportado en el desarrollo de la Evaluación, Dirección y Monitorización. De acuerdo con ello, se presenta el modelo de gobierno corporativo y de TI planteado por dicha norma:

Figura 1.

Modelo de Gobierno Corporativo de TI.



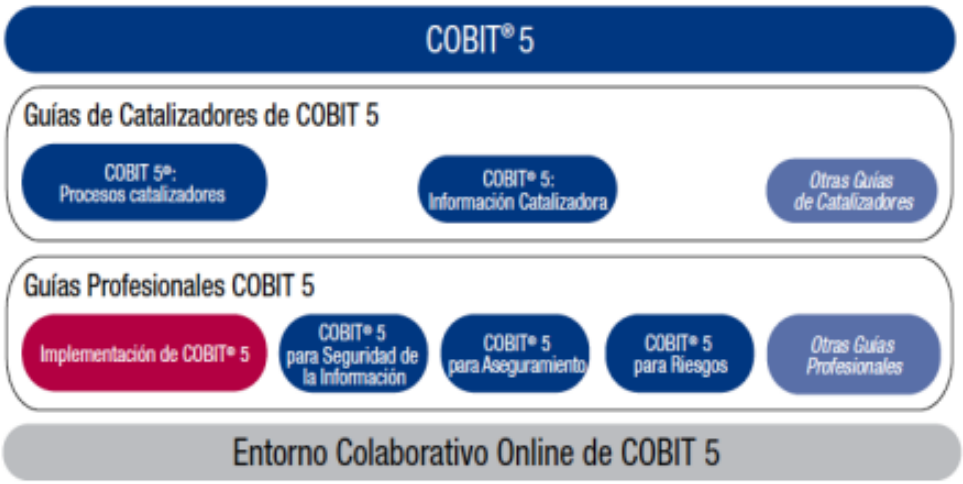
Fuente: ISO 38500.

El estándar **COBIT**, debe su nombre a sus siglas en inglés, (Control Objetives for Information and Related Technology) según ISACA (Information Systems Audit an Control Association), es conocido como el marco líder para el Gobierno y la Gestión de las tecnologías de la información en las organizaciones. En su versión 5.0, este estándar ha incorporado cambios significativos en lo que respecta a Gobierno de TI, además del componente de Gestión abordado en anteriores versiones, estructurado mediante la integración de la siguiente familia de productos:

- Guía de Catalizadores, compuesta por procesos catalizadores, información catalizadora y demás guías.
- Guías Profesionales, que apoyan la implementación de COBIT, la seguridad de la información, las buenas prácticas de aseguramiento en materia de riesgos, entre otras guías profesionales.
- Entorno Colaborativo en Línea.

Figura 2.

Familia de productos de COBIT 5.0.

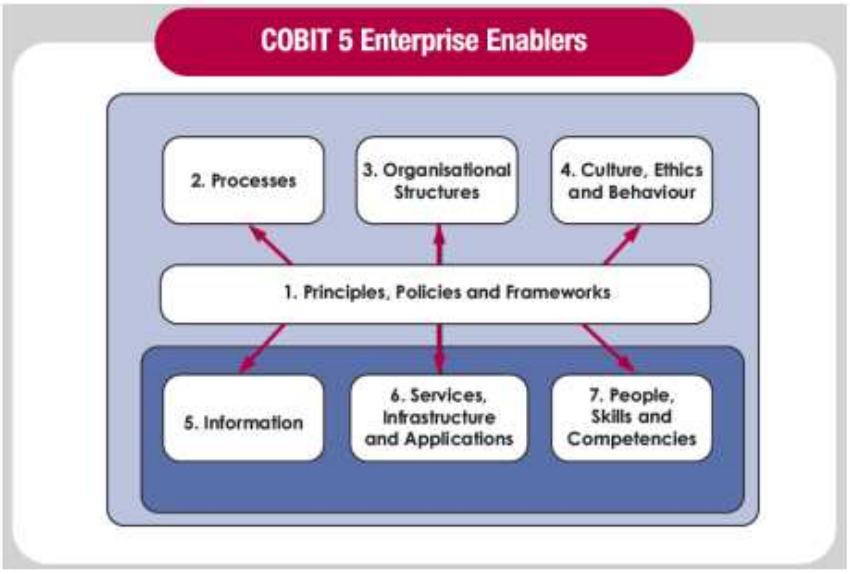


Fuente: COBIT 5.0 (ISACA).

Se encuentra además una serie de habilitadores para el Gobierno y la Gestión en la organización, representados en la siguiente figura:

Figura 3.

Habilitadores de COBIT 5.0.

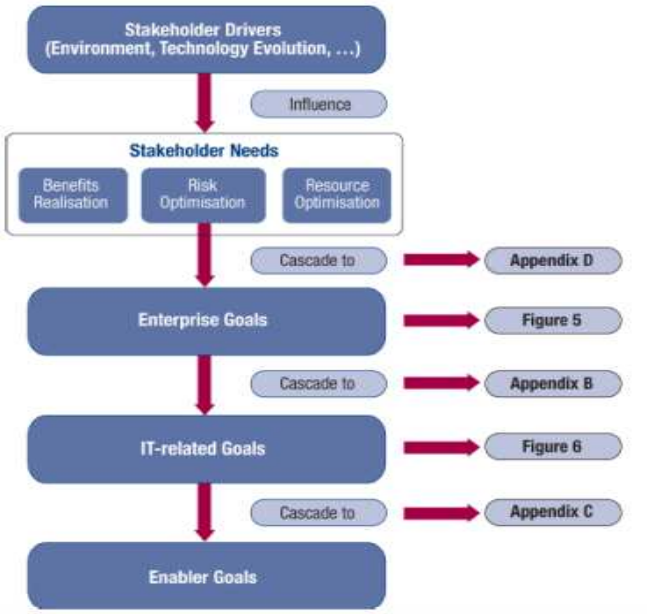


Fuente: COBIT 5.0 (ISACA).

Por otra parte, COBIT establece una cascada de metas, cuyo propósito es identificar las necesidades de los stakeholders con miras a la optimización de beneficios, riesgos y recursos; señalando las metas empresariales, metas relacionadas TI y las metas de los habilitadores, manteniendo como prioridad la creación de valor para la organización.

Figura 4.

Cascada de Metas COBIT 5.0.



Fuente: COBIT 5.0 (ISACA).

La **norma ISO 27001** desarrollada por la International Organization for Standardization (ISO), cuyo objeto hace referencia a la emisión de los lineamientos como apoyo a las organizaciones, que garanticen la seguridad de la información. La implementación de este estándar contribuirá a la protección de los activos con relación a la información financiera, recursos humanos, propiedad intelectual, información dada a terceros, entre otro tipo de información propia de las compañías. Las siguientes fases constituyen el proceso de implementación de la norma:

Figura 5.

Fases de implementación de la Norma ISO 27001.

Fuente: AC Consultores (2021).

La última versión de la norma adaptada por ICONTEC para Colombia, data del año 2013 y se encuentra estructurada mediante un ciclo PHVA (P: Planificación, H: Operación, V: Evaluación y Desempeño y A: Mejora), considerando el contexto de la organización y el liderazgo como uno de los factores más relevantes en pro del compromiso de parte de la Alta Dirección en la organización sobre el SGSI, además, la norma dispone de un Anexo A asociado con Dominios y Controles de Seguridad de la Información como buenas prácticas, estas a su vez se desarrollan a partir de la norma Técnica ISO 27002.

La norma ISO 27002 (anteriormente denominada ISO 17799) es el estándar de seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. Su versión más reciente de la norma ISO 27002:2013.

Esta norma proporciona diversas recomendaciones sobre las mejores prácticas para las partes interesadas, con el fin de iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. A continuación, se presenta gráficamente un modelo de gestión basado en la norma ISO 27002:

Figura 6.

Modelo de Gestión basado en ISO 27002.

Fuente: ISO 27002:2013.

Information Technology Infraestructure Library **ITIL**, es una metodología enfocada en la calidad de servicio y el desarrollo eficaz y eficiente de los procesos que cubren las actividades más representativas de las organizaciones en cuanto a Sistemas y Tecnologías de la Información.

Figura 7.

Modelo ITIL.

Fuente: Biblioteca ITIL.

4.2 Diagnosticar el nivel de seguridad y privacidad de la información en las instituciones prestadoras de salud en la ciudad de Ocaña.

Con el fin de realizar el diagnóstico de la seguridad y privacidad de la información en las intuiciones prestadoras del servicio de salud de la ciudad de Ocaña, se tomó como referente el Centro Eco-Radiodiagnósticos S.A.S., donde se aplicó la herramienta de diagnóstico diseñada por el Ministerio de Tecnologías de la Información para tal fin, teniendo en cuenta que es una herramienta robusta diseñada teniendo en cuenta la realidad de las instituciones colombianas.

Como principal referente para la evaluación del nivel de seguridad y privacidad de la información se cuenta con los controles de la norma ISO 27001:2013 en su Anexo A, teniendo en cuenta pruebas previamente definidas, teniendo en cuenta las mejores prácticas nacionales e internacionales; Con el fin de proveer a las instituciones prestadoras de salud en la ciudad de Ocaña un mecanismo de aprovechamiento de las tecnologías de la información basado en las necesidades y objetivos, los requisitos de seguridad y los procesos misionales de la institución.

Evaluación de controles ISO 27001

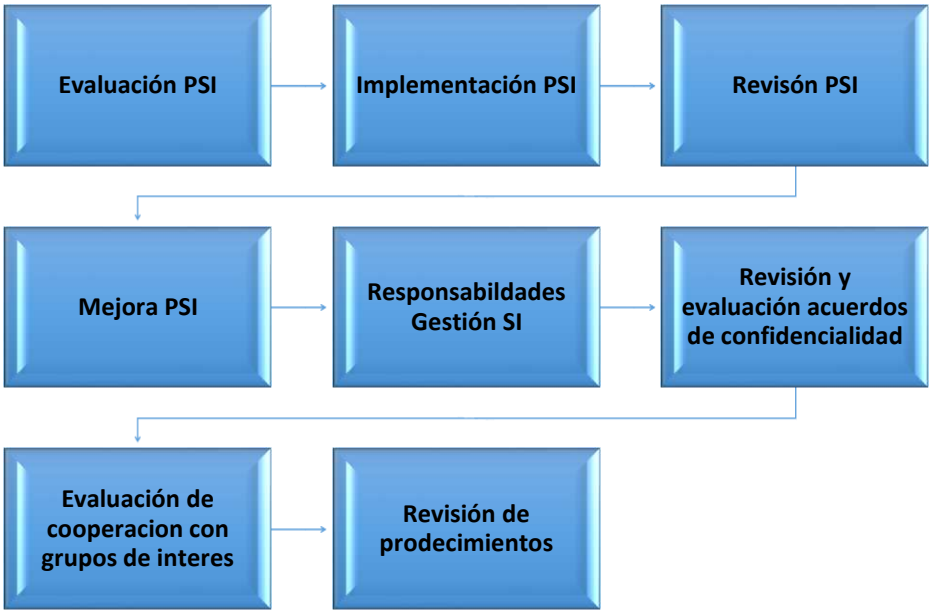
La evaluación planteada califica cada dominio de la norma frente a una escala previamente definida, identificando la brecha existente entre la realidad y la proyección; mediante pruebas de diferente tipo, clasificadas como Administrativas, Técnicas, entre otras:

Pruebas Administrativas

Las pruebas administrativas están diseñadas para abordar temáticas relacionadas a seguridad de la información que no se encuentran directamente relacionadas con las áreas tecnológicas de la organización, abarcan:

Figura 8.

Etapas de las Pruebas Administrativas.



Fuente: Autora del Proyecto.

Al interior del Centro Eco radiodiagnósticos IPS, se ha implementado un plan de calidad que tiene como objetivo principal "*Ofrecer servicios confiables seguros y oportunos con alta y centrada atención en el usuario ofreciendo un trato amable, digno y respetuoso. Soportado por profesionales cálidos y competentes, equipos de última tecnología y mejoramiento continuo de los procesos*", de igual manera se implementó la Política de la Gestión de la Tecnología la cual busca: "*Generar un compromiso para realizar una adecuada gestión de la tecnología y los dispositivos médicos en la compra, renovación, reposición y su uso, apoyada en conceptos técnicos, de tal manera que se*

disminuya el riesgo para el paciente, su familia, el trabajador y el medio ambiente durante su vida útil, cumpliendo los requisitos de ley y partes interesadas."

En el marco de estas políticas se diseñó la política de seguridad de la información como primer paso para el diseño del Sistema de Gestión de Seguridad para la entidad, es necesario resaltar que la PSI se encuentra documentada y aprobada por parte de la gerencia general pero no se ha socializado con las partes interesadas.

Para evaluar las temáticas administrativas de la organización, y tomando como referencia la herramienta de diagnóstico diseñada por MinTic, se toman en cuenta treinta y seis pruebas que fueron analizadas con el gerente general quien ofreció una amplia visión de la entidad, los resultados de estas pruebas se resumen en la tabla a continuación y se pueden ver en detalle en el Anexo A (archivo adjunto en PDF.)

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN					
AD.1	**Responsable de SI**	**POLITICAS DE SEGURIDAD DE LA INFORMACIÓN**	**Orientación de la dirección para gestión de la seguridad de la información**	**A.5**	**20**
RESPONSABILIDADES Y ORGANIZACIÓN SEGURIDAD INFORMACIÓN					
A2	**Responsable de SI**	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización** **Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles**	**A.6**	**12**
AD.2.1	Responsable de SI	Organización Interna	Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización	A.6.1	4
AD.2.2	Responsable de SI	Dispositivos Móviles y Teletrabajo	Garantizar la seguridad del teletrabajo y uso de dispositivos móviles	A.6.2	20

SEGURIDAD DE LOS RECURSOS HUMANOS					
AD.3	**Responsable de SI/Gestión Humana/Líderes de los procesos**	**SEGURIDAD DE LOS RECURSOS HUMANOS**		**A.7**	**21**
AD.3.1	Responsable de SI	Antes de asumir el empleo	Asegurar que el personal y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que son considerados.	A.7.1	30
AD.3.2	Responsable de SI/Líderes de los procesos	Durante la ejecución del empleo	Asegurar que los funcionarios y contratistas tomen consciencia de sus responsabilidades sobre la seguridad de la información y las cumplan. Proteger los intereses de la Entidad como parte del proceso de cambio o terminación de empleo.	A.7.1.2	13
AD.3.3	Responsable de SI	Terminación y cambio de empleo		A.7.3	20

GESTIÓN DE ACTIVOS					
AD.4	**Responsable de SI**	**GESTIÓN DE ACTIVOS**		**A.8**	**25**
AD.4.1	Responsable de SI	Responsabilidad de los activos	Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.	A.8.1	20
AD.4.2	Responsable de SI	Clasificación de información	Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la Entidad.	A.8.2	27
AD.4.3	Responsable de TICs	Manejo de medios	Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de la información almacenada en los medios.	A.8.3	27
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO					
AD.5	**Responsable de la Continuidad**	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		**A.17**	**6,5**
AD.5.1	Responsable de la Continuidad	Continuidad de la seguridad de la información	La continuidad de la seguridad de la información debe incluir en los sistemas de	A.17.1	13

			gestión de la continuidad del negocio de la Entidad.		
AD.5.2	Responsable de la Continuidad	Redundancias	Asegurar la disponibilidad de las instalaciones de procesamiento de la información.	A.17.2	0
CUMPLIMIENTO					
AD.6	**Responsable de SI/Responsable de TICs/Control Interno**	**CUMPLIMIENTO**		**A.18**	**32,5**
AD.6.1	Responsable de SI	Cumplimiento de requisitos legales y contractuales	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.	A.18.1	45
AD.6.1.5	n/a	Reglamentación de controles criptográficos.		A.18.1.5	n/a
AD.6.2	Control interno	Revisiones de seguridad de la información		A.18.2	20
RELACIONES CON LOS PROVEEDORES					
AD.7	**Responsable de compras y adquisiciones**	**RELACIONES CON LOS PROVEEDORES**		**A.15**	**20**

La anterior evaluación deja ver un bajo cumplimiento de los controles asociados a la norma, lo que se traduce en una evaluación de efectividad de controles **inicial.**

Pruebas Técnicas

Continuando con la evaluación se aplicaron las pruebas orientadas a las áreas técnicas de la entidad, las cuales constan de setenta pruebas orientadas específicamente a la revisión de los componentes tecnológicos de la organización, los resultados de este análisis se resumen a continuación:

Tabla 3.

Pruebas técnicas.

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001
CONTROL DE ACCESO						
T.1	**Responsable de SI/Responsable de TICs**	**CONTROL DE ACCESO**		**A.9**	**Componente planificación y modelo de madurez nivel gestionado**	**15**

T.1.1	Responsable de SI	REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	Se debe limitar el acceso a información y a instalaciones de procesamiento de información.	A.9.1	Modelo de madurez definido	30
T.1.2	Responsable de SI	GESTIÓN DE ACCESO DE USUARIOS	Se debe asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.	A.9.2	Modelo de madurez gestionado cuantitativamente	10
T.1.3	Responsable de SI	RESPONSABILIDADES DE LOS USUARIOS	Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.	A.9.3	Modelo de madurez definido	0
T.1.4	Responsable de SI	CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	Se debe evitar el acceso no autorizado a sistemas y aplicaciones.	A.9.4	Modelo de madurez gestionado cuantitativamente	20
CRIPTOGRAFÍA						
T.2	**Responsable de SI**	**CRIPTOGRAFÍA**	**Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización**	**A.10**		**10**

			Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles			
T.2.1	Responsable de SI	CONTROLES CRIPTOGRÁFICOS	Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.	A.10.1	Modelo de madurez gestionado cuantitativamente	10
SEGURIDAD FÍSICA Y DEL ENTORNO						
T.3	**Responsable de la seguridad física/Responsable de SI/Líderes de los procesos**	**SEGURIDAD FÍSICA Y DEL ENTORNO**		**A.11**		24
T.3.1	Responsable de la seguridad física	ÁREAS SEGURAS	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de	A.11.1	Modelo de madurez definido	20

			información de la organización.			
T.3.2	Responsable de SI	EQUIPOS	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	A.11.2	Modelo de madurez definido	27
SEGURIDAD DE LAS OPERACIONES						
T.4	**Responsable de TICs/Responsable de SI**	**SEGURIDAD DE LAS OPERACIONES**		**A.12**		14
T.4.1	Responsable de TICs	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	A.12.1	Modelo de madurez definido	15

T.4.2	Responsable de SI	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.	A.12.2		20
T.4.3	Responsable de TICs	COPIAS DE RESPALDO	Proteger contra la pérdida de datos.	A.12.3	Modelo de madurez gestionado	40
T.4.4	Responsable de SI	REGISTRO Y SEGUIMIENTO	Registrar eventos y generar evidencia.	A.12.4	Modelo de madurez gestionado cuantitativamente	5
T.4.5	Responsable de TICs	CONTROL DE SOFTWARE OPERACIONAL	Asegurar la integridad de los sistemas operacionales.	A.12.5	Modelo de madurez definido	20
T.4.6	Responsable de SI	GESTIÓN DE LA VULNERABILIDAD TÉCNICA	Prevenir el aprovechamiento de las vulnerabilidades técnicas.	A.12.6	Modelo de madurez gestionado	0
SEGURIDAD DE LAS COMUNICACIONES						
T.5	**Responsable de TICs/Responsable de SI**	**SEGURIDAD DE LAS COMUNICACIONES**		**A.13**		14
T.5.1	Responsable de TICs	GESTIÓN DE LA SEGURIDAD DE LAS REDES	Asegurar la protección de la información en las redes, y sus instalaciones de	A.13.1	Modelo de madurez definido	13

			procesamiento de información de soporte.			
T.5.2	Responsable de TICs	TRANSFERENCIA DE INFORMACIÓN	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	A.13.2	Modelo de madurez definido	15
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS						
T.6	**Responsable de SI/Responsable de TICs**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**		**A.14**		12

T.6.1	Responsable de SI	REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.	A.14.1	Modelo de madurez definido	10
T.6.2	Responsable de SI	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	A.14.2	Modelo de madurez definido	25
T.6.3	Responsable de SI	DATOS DE PRUEBA	Asegurar la protección de los datos usados para pruebas.	A.14.3	Modelo de madurez definido	0

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

T.7.	**Responsable de SI/Responsable de TICs**	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**		**A.16**	11
T.7.1	Responsable de SI	GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.	A.16.1	11

Continuando con la tendencia anteriormente descrita, la evaluación aplicada al área técnica muestra un bajo nivel de cumplimiento, generando una evaluación de efectividad de controles **inicial** o **repetible.**

Como resumen del proceso de evaluación de efectividad de los controles aplicables a la organización podemos observar la siguiente tabla, la cual muestra una comparación sobre el estado actual y el deseado para cada dominio analizado y el nivel de efectividad del control aplicable:

Tabla 4.

Evaluación de Efectividad de controles.

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	100	**INICIAL**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	12	100	**INICIAL**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	21	100	**REPETIBLE**
A.8	GESTIÓN DE ACTIVOS	25	100	**REPETIBLE**
A.9	CONTROL DE ACCESO	15	100	**INICIAL**
A.10	CRIPTOGRAFÍA	10	100	**INICIAL**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	24	100	**REPETIBLE**
A.12	SEGURIDAD DE LAS OPERACIONES	14	100	**INICIAL**
A.13	SEGURIDAD DE LAS COMUNICACIONES	14	100	**INICIAL**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	12	100	**INICIAL**
A.15	RELACIONES CON LOS PROVEEDORES	20	100	**INICIAL**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	11	100	**INICIAL**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	7	100	**INICIAL**
A.18	CUMPLIMIENTO	32,5	100	**REPETIBLE**
	PROMEDIO EVALUACIÓN DE CONTROLES	**17**	**100**	**INICIAL**

Igualmente se puede apreciar una gráfica comparativa entre la calificación actual y la deseada, generando una amplia brecha de cumplimiento de controles, tal como se observa a continuación:

Figura 9.

Brecha cumplimiento de controles.

Se hace notorio que la institución se encuentra en un punto muy básico frente al desarrollo e implementación del Sistema de Gestión de Seguridad de la Información, con un porcentaje de desarrollo mínimo de sus componentes, de esta manera:

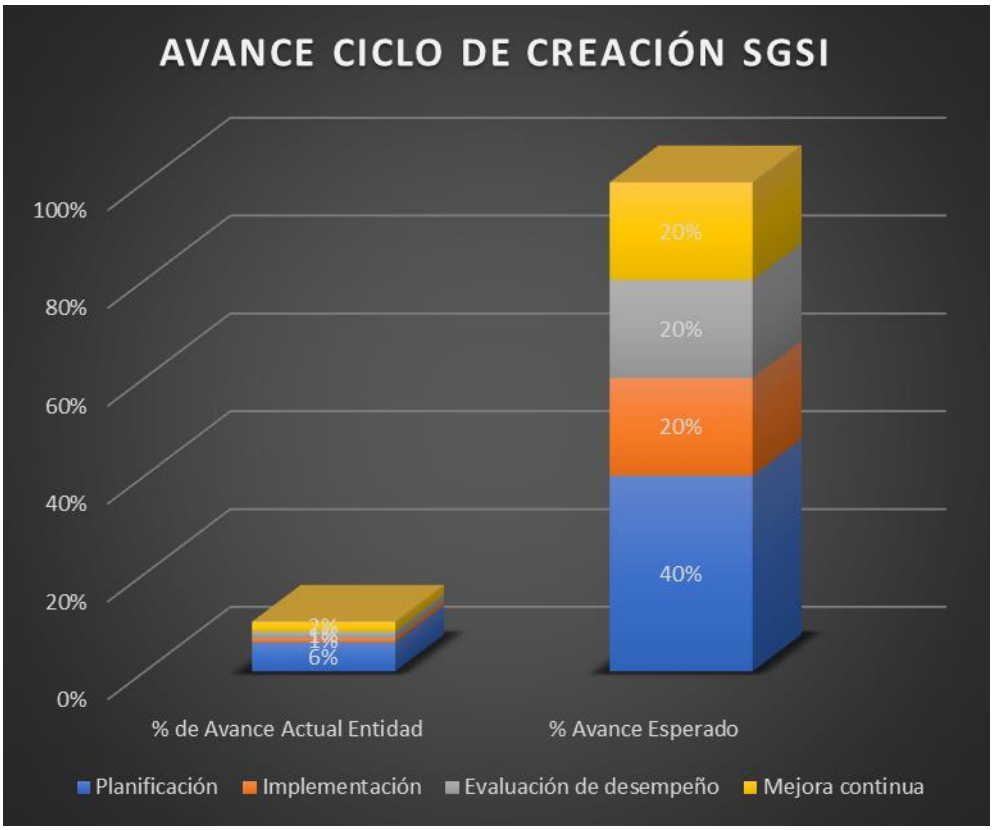
Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2021	Planificación	6%	40%
	Implementación	1%	20%

	Evaluación de desempeño	1%	20%
	Mejora continua	2%	20%
TOTAL		**10%**	**100%**

Analizando gráficamente el avance del ciclo de creación del Sistema de Gestión de Seguridad de la Información, se puede ver como el porcentaje de avance es casi nulo en las etapas de implementación, evaluación de desempleo y mejora continua; mientras que en el caso de planificación se muestra que la entidad comenzó a dar pasos para avanzar en el ciclo:

Figura 10.

Avance ciclo de creación SGSI



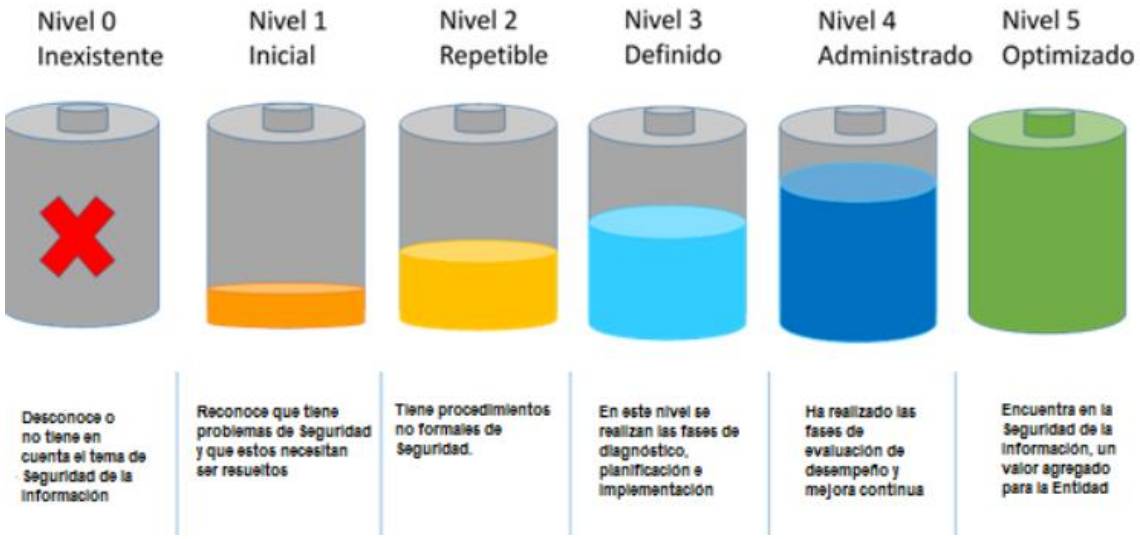
:

Nivel de Madurez de la Seguridad y Privacidad de la Información

Con el fin de diagnosticar el nivel de madurez de la seguridad y privacidad de la información en el Centro Eco radiodiagnósticos IPS, se aplicó el instrumento anexo del MinTic, el cual identifica cada uno de los requisitos para cumplir los diferentes niveles de madurez así:

Figura 11.

Niveles de madurez.



Nota. Niveles de madures, Mintic. (https://mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf)

Con base en las evaluaciones realizadas y teniendo en cuenta las pruebas que se aplicaron para validar el cumplimiento de cada uno de los dominios y el avance en la creación e implementación del Modelo de Seguridad de la Información, se logró obtener el nivel de madurez de los procesos asociados a la seguridad de la información:

	NIVEL DE CUMPLIMIENTO
Inicial	SUFICIENTE
Repetible	CRÍTICO

Definido	CRÍTICO
Administrado	CRÍTICO
Optimizado	CRÍTICO

La determinación de un nivel de madurez inicial, permite evidenciar que la entidad no aplica controles alineados con la confidencialidad, integridad, disponibilidad y privacidad de la información, no se identifica la información como un activo valioso para la consecución de los objetivos del negocio; esto se ve reflejado en la inconciencia sobre la seguridad de la información de la institución.

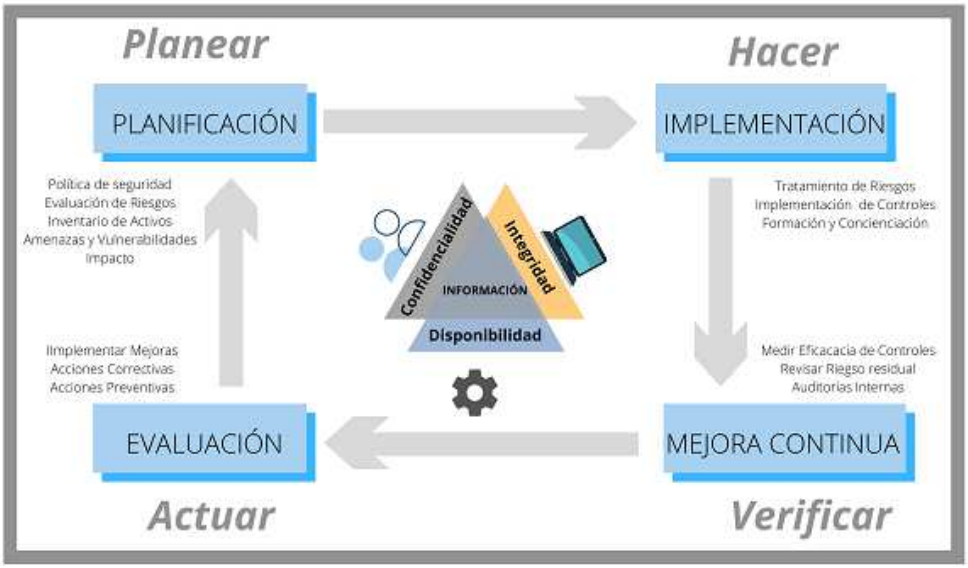
4.3 Estructurar los componentes del modelo de gestión de seguridad de la información.

El modelo de gestión de seguridad de la Información para las entidades prestadoras de salud del municipio de Ocaña fue estructurado teniendo en cuenta la necesidad de mantener una hoja de ruta que permita aplicar las actividades propias de un Sistema de Gestión de Seguridad de la Información soportado en el ciclo PHVA y su metodología.

Figura 12.

Modelo diseñado.

MODELO DE GOBIERNO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN EN LAS INSTITUCIONES PRESTADORAS DE SALUD EN EL MUNICIPIO DE OCAÑA.



Fuente: Autora del proyecto.

Planear:

En la etapa de planificación del modelo propuesto es necesario definir con claridad los activos de información con los que cuenta la entidad, los cuales deben ser valorados y clasificados mediante un sistema de clasificación.

De igual manera se debe definir la metodología por la cual se identificarán, evaluarán y tratarán los riesgos, medición de impacto, y establecer el plan de tratamiento de riesgos.

Adicionalmente se determinarán lineamientos para la gestión oportuna de incidentes, clasificándolos y definiendo indicadores para este.

Finalmente se deben implementar estrategias para la gestión del cambio y la creación de conciencia de seguridad de la información.

Hacer:

En este punto se debe realizar el levantamiento de la información correspondiente a los activos de información y aplicar la metodología de clasificación previamente definida, Determinar la ocurrencia y probabilidad del riesgo, además de definir el impacto que generaría la ocurrencia del riesgo sobre los recursos de la entidad.

De igual forma dentro de la gestión de incidentes se deberán detectar y analizar cada uno de ellos a fines de contener y recuperarse del mismo, siempre documentando cada acción realizada y caracterizando uno a uno los incidentes hallados.

Es de vital importancia involucrar la implementación de controles jurídicos para el tratamiento de riesgo, definir e implementar los planes de continuidad y recuperación soportados en una adecuada infraestructura de TI y capacitando el personal para el desarrollo y mantenimiento de estos planes.

Verificar:

Se deberá realizar una revisión de la información consignada en el inventario de activos, auditorias para la verificación del cumplimiento de la metodología de clasificación de activos; diseñar un cronograma de seguimiento al desarrollo de los planes de tratamiento de riesgo, revisando si los niveles de riesgo son aceptables.

Además, debe diseñarse un plan de auditorías internas aplicables a los procedimientos internos de gestión de incidentes de seguridad y adicionalmente auditar y

revisar mediante la aplicación de pruebas los planes de continuidad y recuperación definidos, con el fin de realizar medición a la efectividad de dichos planes.

Como un producto adicional al proceso de auditoría interna, se debe revisar el cumplimiento de los objetivos de seguridad de la información y resultados de las pruebas aplicadas en auditorias.

Actuar:

El inventario de activos debe mantenerse en constante actualización de acuerdo a los cambios producidos sobre la entidad teniendo en cuenta las recomendaciones que surgen del proceso de auditoria; de igual manera la evaluación de riesgos debe ser un proceso recurrente, que permita determinar las acciones que actualizaran el plan de tratamiento a riesgos.

Frente a los incidentes de seguridad de la información se debe establecer un conjunto de acciones preventivas y correctivas acordes a la gestión e identificación realizada previamente.

Los planes de continuidad y recuperación estarán en constante actualización, reforzando las debilidades halladas en las auditorias.

Conclusiones

La gestión de la seguridad constituye un reto para las organizaciones en materia de implementación, las cuales deben dimensionar las implicaciones y el nivel de esfuerzo requerido, a partir de una correcta etapa de planeación que apunte hacia una estrategia de adaptación exitosa.

Es necesario que la implementación de modelos de Seguridad sea una iniciativa abordada por la alta dirección de las organizaciones, bajo la que se gestionará la seguridad de la información para asumir o mitigar los riesgos inherentes a la naturaleza de cualquier negocio.

Tras analizar los estándares de gobernanza de TI aplicables, es posible concluir que existe una amplia gama de estos, cuyo propósito consiste en brindar un compendio de buenas prácticas que garanticen la alineación de sus objetivos misionales con los recursos disponibles en pro de beneficios para las partes interesadas. Para la presente investigación, se seleccionó los marcos de referencia asociados a la seguridad de la información, en el ámbito de la salud, tomando como insumo primario la Norma ISO 27000 para la evaluación del nivel de seguridad y privacidad.

El diagnóstico del estado actual del activo de información en las Instituciones Prestadoras de Salud en el Municipio de Ocaña pone en evidencia la amplia brecha existente en las organizaciones en materia de seguridad, demostrando que dichas entidades son aun incipientes en la correcta implementación de estándares y buenas prácticas de Gobierno y Gestión de las Tecnologías de la Información.

El modelo de gestión de seguridad de la Información propuesta para las entidades del sector de la salud de Ocaña ha sido diseñado con el objeto de dar respuesta a una necesidad latente presente en el medio. El modelo proporciona una herramienta para la

aplicación de las actividades propias de un Sistema de Gestión de Seguridad de la Información en el marco del ciclo PHVA.

Recomendaciones

Con el propósito de lograr resultados favorables para las partes interesadas en la organización objeto del presente estudio se plantean las siguientes recomendaciones:

1. Socializar e involucrar a todas las partes que integran las diferentes áreas de la organización, haciéndoles partícipes desde sus diferentes roles en todas las fases del proceso, desde la Planeación hasta la implementación del mismo.

2. Garantizar el acompañamiento continuo de la alta Dirección en la adopción de las políticas de seguridad existentes.

3. Ofrecer capacitación permanente al personal de las instituciones en materia de seguridad de la Información.

4. Revisar y adoptar el Modelo propuesto en pro del mejoramiento continuo de la Organización y sus Stakeholders.

5. Promover entre las demás entidades del sector, mediante resultados positivos de su proceso como un caso de éxito para ser replicado en la implementación del modelo de Gobierno de TI para la Gestión de la seguridad.

Referencias

Behar Rivero, D. S. (2008). *Metodología de la Investigación.* Editorial Shalom.

Borrero, C. (2004). Simposio Permanente sobre la Universidad. *Conferencia XXXIII La Tecnología* (pág. 25). Bogota: Colombia.

Brandis, K. (2014). Towards a framework for governance architecture management in cloud environments: A semantic perspective. *Future Generation Computer Systems*, 32.

Carrera, H. (2011). *MODELO DE GOBIERNO DE TI. CASO CENTRO DE COMPETENCIAS DE BUSINESS INTELLIGENCE.* Obtenido de http://www.bib.uia.mx/tesis/pdf/015355/015355.pdf

Cerda Gutiérrez, H. (2013). *Los elementos de la Investigación.* Bogotá: El Buho Ltda.

Esquivia, S. (2018). *Diseño de una estrategia de Gobierno y Gestión de TI para sistemas integrados de transporte masivo: caso Transmetro.* Obtenido de http://manglar.uninorte.edu.co/bitstream/handle/10584/8319/133656.pdf?sequence=1&isAllowed=y

Funcion publica. (2014). *Decreto 903 de 2014*. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=57358

Henao, A. (2013). *Beneficios resultantes del proceso de acreditación de la calidad en Salud.* Obtenido de http://catalogo.econo.unlp.edu.ar/meran/opac-detail.pl?id1=16975#.XTSMxI5KgdU

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación* (Sexta ed.). México: McGraw-Hill. Recuperado el Febrero de 2018

ISACA. (2012). COBIT 5.0: A Business Framework for the Governance and Management of Enterprise IT. *Management of Enterprise* , 35.

Lepage, G. (2014). *DISEÑO DE UN MODELO DE GOBIERNO DE TI CON ENFOQUE DE SEGURIDAD DE INFORMACIÓN PARA EMPRESAS PRESTADORAS DE SERVICIOS DE SALUD BAJO LA ÓPTICA DE COBIT 5.0.* Obtenido de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/5384/LEPAGE_

DIANA_MODELO_GOBIERNO_TI_SEGURIDAD_INFORMACION_EMPRESAS_PRESTADORAS_SERVICIOS_SALUD_COBIT_5.0.pdf?sequence=1&isAllowed=y

Marulanda, C., Lopez, M., & Valencia, F. (2017). *GOBIERNO Y GESTIÓN DE TI EN LAS ENTIDADES PÚBLICAS.* Obtenido de publicaciones.eafit.edu.co/index.php/administer/article/download/4614/4064/

Meneses, A., & Ramirez , E. (2016). *DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI BASADO EN EL ESTÁNDAR ISO 27001, PARA LOS PROCESOS SOPORTADOS POR EL AREA DE SISTEMAS EN LA CÁMARA DE COMERCIO DE AGUACHICA.* Obtenido de http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/1434/1/29635.pdf

Minsalud. (2006). *Decreto 1011 de 2006*. Obtenido de https://www.minsalud.gov.co/Normatividad_Nuevo/DECRETO%201011%20DE%202006.pdf

Minsalud. (2006). *Resolución 1445 de 2006, anexo tecnico*. Obtenido de https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/VS/PSA/Manual-Estandares-Sistema-Acreditacion-Resolucion-1445-2006.pdf

Minsalud. (2015). *Ley 1751 de 2015*. Obtenido de https://www.minsalud.gov.co/Normatividad_Nuevo/Ley%201751%20de%202015.pdf

Minsalud. (2016). *Decreto 780 de 2016*. Obtenido de https://www.minsalud.gov.co/Normatividad_Nuevo/Decreto%200780%20de%202016.pdf

MinTic. (2008). *Plan Nacional de Tecnologías de la Información.* Obtenido de https://www.mintic.gov.co/portal/604/w3-propertyvalue-544.html

Muñoz, I., & Ulloa, G. (2011). Gobierno de TI – Estado del Arte. *S&T*, 69.

Paéz, A., & Hernandez, F. (2015). *Modelo para la definición e implementación de procesos de gobierno de tecnologías de la información aplicado a CENIT Transporte y Logística de Hidrocarburos S.A.S.* Obtenido de http://repository.urosario.edu.co/handle/10336/11836

Ramos, A. (2016). *El eslabón más débil de la cadena.* Obtenido de http://www.antonio ramos.es/2007/06/el eslabn ms dbil de lacadena.html

Sanchez, H. (2012). Diseño del proceso de evaluación del desempeño del personal y las principales tendencias que afectan su auditoría. *Innovación*, 35.

Talabera, V. (2015). *DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA ENTIDAD ESTATAL DE SALUD DE ACUERDO A LA ISO/IEC 27001:2013.* Obtenido de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/6092/TALAVERA_VASCO_DISE%c3%91O_SISTEMA_GESTION.pdf?sequence=1&isAllowed=y

Tomas, A. (2014). *Shannon, padre de la Teoría de la Información.* Obtenido de http://bituchile.com/2011/05/teoria de la informacion concepto

Weill, P., & Ross, J. (2014). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. *Harvard Business School*, 269.

Yañez, M. (2017). *SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA SUBSECRETARIA DE ECONOMÍA Y EMPRESAS DE MENOR TAMAÑO.* Obtenido de http://repositorio.uchile.cl/bitstream/handle/2250/147976/Sistema-de-gestion-de-seguridad-de-la-informacion-para-la-Subsecretaria-de-Economia-y-Empresas.pdf?sequence=1&isAllowed=y

Apendice

Apéndice A. Matriz de Operacionalización de variables

Propósito	Conceptualización	Dimensiones	Subdimensiones	Ítems
Proponer un Modelo de gobierno de las tecnologías para la gestión de la seguridad de información en las instituciones prestadoras de salud en el Municipio de Ocaña.	La gobernanza corporativa puede referirse a cualquiera de las políticas y procesos que controlan una empresa. Son las acciones que ayudan a la corporación a avanzar hacia sus objetivos, evitando conflictos y crisis, con miras al crecimiento y al desarrollo de nuevas oportunidades de negocio que lo diferencien de la competencia y mantengan la reputación de la organización. (México) Se entiende por Gobierno TI, el conjunto de acciones que realiza el área de TI en coordinación con la alta dirección para movilizar sus recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o del negocio. (TCP, 2014)	Cobit 5	Procesos catalizadores para la Gestión de TI Empresarial APO13 (alinear, planificar y organizar) gestionar la seguridad DSS05(entregar, dar servicio, dar soporte) gestionar los servicios de seguridad. MEA01(supervisar, evaluar y valorar). rendimiento y conformidad; MEA02(supervisar, evaluar y valorar). servicio, dar soporte) el sistema de control interno; MEA03(supervisar, evaluar y valorar).la conformidad con los requerimientos externos. Dominios	**45**

	El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001. (ISO 27001) Sistema Único de Acreditación en Salud, es el conjunto de procesos, procedimientos y herramientas de implementación voluntaria y periódica por parte de las entidades, los cuales están destinados a comprobar el cumplimiento gradual de niveles de calidad superiores a los requisitos mínimos obligatorios, para la atención en salud, bajo la dirección del Estado y la inspección, vigilancia y control de la Superintendencia Nacional de Salud. (Social)	ISO/IEC 27002:2013 Manual de Acreditación en Salud ambulatorio y	políticas de seguridad. aspectos organizativos de la seguridad de la información. seguridad ligada a los recursos humanos. gestión de activos. control de accesos. cifrado. seguridad física y ambiental. seguridad en la operativa seguridad en las telecomunicaciones adquisición, desarrollo y mantenimiento de los sistemas de información. relaciones con suministradores gestión de incidentes en la seguridad de la información. aspectos de seguridad de la	

		hospitalario de Colombia versión 3.1	informacion en la gestión de la continuidad del negocio cumplimiento Grupo de estandares de gerencia de la Información	

Fuente: Autora del proyecto

Apéndice B. Entrevista dirigida al gerente de la IPS

Objetivo: Conocer cómo se encuentra la IPS frente a los componentes de la COBIT y la ISO 27002, los cuales están distribuidos en secciones, que corresponden a controles de seguridad de la información.

1. ¿Está en marcha un sistema que considera y trata efectivamente los requerimientos de seguridad de la información de la empresa?

2. ¿Se ha establecido, aceptado y comunicado por toda la empresa un plan de seguridad?

3. ¿Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en toda la empresa?

4. ¿La seguridad de las redes y las comunicaciones cumple con las necesidades del negocio?

5. ¿La información procesada, almacenada y transmitida en los dispositivos de usuario final está protegida?

6. ¿Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en el negocio?

7. ¿Se han implantado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida?

8. ¿La información electrónica tiene las medidas de seguridad apropiadas mientras está almacenada, transmitida o destruida?

9. ¿Los Objetivos y métricas son aprobadas por las partes interesadas?

10. ¿Son los procesos medidos acorde a las métricas y objetivos acordados?

11. ¿La monitorización, evaluación y generación de información es efectiva y operativa?

12. Los objetivos y métricas están integradas dentro de los sistemas de supervisión de la empresa?

13. ¿Los informes acerca del rendimiento y conformidad de los procesos son útil y a tiempo?

14. ¿Los procesos, recursos e información cumplen con los requisitos del sistema de control interno de la empresa?

15. ¿Todas las iniciativas de aseguramiento se planean y ejecutan de forma efectiva?

16. ¿Se proporciona aseguramiento independiente de que el sistema de control interno es operativo y efectivo?

17. ¿El control interno está establecido y las deficiencias son identificadas y comunicadas?

18. ¿La totalidad de los requisitos externos de cumplimiento se han identificado?

19. ¿La empresa trata adecuadamente los requisitos externos de cumplimiento?

20. ¿Posee la IPS un documento sobre la política de seguridad de la información de la empresa, que contenga los conceptos de seguridad de la información?

21. ¿Las actividades de seguridad de la información están coordinadas por representantes de la IPS, con las responsabilidades bien definidas los cuales protegen las informaciones de carácter confidencial?

22. ¿Están los activos identificados y clasificados, de modo que un inventario pueda ser estructurado y posteriormente mantenido? ¿Siguiendo reglas documentadas, que definen qué tipo de uso se permite hacer con dichos activos?

23. ¿Cuándo se contrata un empleado o proveedor es debidamente analizado, principalmente si se trata de información de carácter confidencial, con el ánimo de mitigar el riesgo de robo, fraude o mal uso de los recursos?

24. ¿Los equipos e instalaciones de procesamiento de información crítica o sensible están ubicados en áreas seguras, con niveles y controles de acceso apropiados, incluyendo protección contra amenazas físicas y ambientales?

25. ¿Están definidos los procedimientos y responsabilidades por la gestión y operación de todos los recursos de procesamiento de la información?

26. ¿El acceso a la información, así como a los recursos de procesamiento de la información y los procesos de negocios, son controlados con base en los requisitos de negocio y en la seguridad de la información?

27. ¿Los requisitos de seguridad de los sistemas de información son identificados y acordados antes de su desarrollo y/o de su implementación, para que así puedan ser protegidos para el mantenimiento de su confidencialidad, autenticidad o integridad por medios criptográficos?

28. ¿Los procedimientos formales de registro y escalonamiento están siendo establecidos y los empleados, proveedores y terceros son conscientes de los procedimientos

para notificar los eventos de seguridad de la información para asegurar que se comuniquen lo más rápido posible y corregidos en tiempo hábil?

29. ¿Los planes de continuidad del negocio están desarrollados e implementados, con el fin de impedir la interrupción de las actividades del negocio y asegurar que las operaciones esenciales sean rápidamente recuperadas?

30. ¿La empresa tiene contratada una consultoría especializada, para que se verifique su conformidad y adherencia a los requisitos legales y reglamentarios?

31. ¿Existen procesos para identificar, responder a las necesidades y evaluar la efectividad de información de los usuarios y sus familias, los colaboradores, y todos los procesos de la organización?

32. ¿Existe un proceso para planificar la gestión de la información en la organización; este proceso está documentado, implementado y evaluado en un plan de gerencia de la información?

33. ¿Cuándo el análisis periódico de la información detecta variaciones no esperadas o no deseables en el desempeño de los procesos, la organización realiza análisis de causas y genera acciones de mejoramiento continuo?

34. ¿La adopción de tecnologías de la información y comunicaciones tendrá en cuenta? ¿Los costos asociados, el entrenamiento al personal, los aspectos éticos, la relación existente entre tecnología y personal (número de equipos, cobertura, etc.)?

35. ¿Existen mecanismos estandarizados, implementados y evaluados para garantizar la seguridad y confidencialidad de la información?

36. ¿Existe un mecanismo definido implementado, evaluado y formal para transmitir los datos y la información? La transmisión garantiza. ¿Oportunidad, facilidad de acceso, confiabilidad y validez de la información, seguridad, veracidad?

37. ¿Existen procesos para la gestión y minería de los datos, que permitan obtener la información en forma oportuna, veraz, clara y conciliada?

38. ¿Existe un mecanismo formal para consolidar e integrar la información asistencial y administrativa? ¿La información asistencial es aquella generada de los procesos de atención a los pacientes y su familia?

39. ¿La gestión de la información relacionada con los registros clínicos, sea en medio físico o electrónico, garantiza la calidad, la seguridad y la accesibilidad de los mismos?

40. ¿Existe un plan de contingencia diseñado, implementado y evaluado que garantice el normal funcionamiento de los sistemas de información de la organización, sean manuales, automatizados, o ambos? Cualquier disfunción en el sistema es recolectada, analizada y

resuelta. ¿Lo anterior incluye mecanismos para prevenir eventos adversos relacionados con el manejo de los sistemas de información en especial alarmas en historia clínica?

41. ¿Le corresponde a la gerencia de la información incorporar en los sistemas informáticos o computarizados los contenidos de los registros definidos por la organización en los procesos de atención médica, así como en la gestión de medicamentos? ¿Esto incluye mecanismos para garantizar que se previenen eventos adversos asociados al uso de siglas o por confusión en las órdenes médicas?

42. ¿La toma de decisiones en todos los procesos de la organización se fundamenta en la información recolectada, analizada, validada y procesada a partir de la gerencia de la información?

43. ¿Existen procesos diseñados, implementados y evaluados de educación y comunicación orientados a desplegar información a clientes internos y externos?

44. ¿Cuentan con un procedimiento de realización de copias de seguridad?

45. ¿Se desarrolla la gestión de las oportunidades de mejora consideradas en el proceso organizacional de mejoramiento continuo, que apliquen al grupo de estándares?

Apéndice C. IPS localizadas en Ocaña

ESE HOSPITAL EMIRO QUINTERO CAÑIZAREZ	CALLE 7 3 29-144
AMBULANCIAS MEDICAS DE OCAÑA LIMITADA- AMBUMED LTDA	CALLE 12 Nº13-20
CENTRO DE ECO-RADIODIAGNOSTICOS S.A.S	CALLE 12 Nº13-20
CENTRO DE IMÁGENES MÉDICAS DE ALTA TECNOLOGÍA CIMAT S.A.C.	KR 14 NO. 10 - 31 / 25
CENTRO DE REHABILITACION FISICA Y ASESORIA SEXUAL- CERAS	CALLE 11 NO.16A-65
CENTRO DE SALUD SAN FRANCISCO DE ASIS LTDA	CLL11 9-14
CENTRO REHABILITAR SAS	CALLE 12 14-68
CLINICA INTEGRAL OFTALMOQUIRURGICA CIO LTDA	CALLE 11 N 16 A 34
CLINICA Y DROGUERIA NTRA SRA DE TORCOROMA LTDA	CRA 14 # 11-81
CONFESALUD IPS LTDA.	KRA. 16A NO. 11-45 B./SAN AGUSTIN
CONSULTORIO ODONTOLÓGICO INTEGRAL ROLANDO RINCON E.U.	CALLE 11 NO. 12-48 LOCAL 4 2 PISO
COOPERATIVA DE TRABAJDORES DE LA SALUD CAPITULO ORIENTE - COOMED CAPITULO ORIENTE	CL 32 NO. 32-64 OF 2
DASALUD S.A.	CRA 11 # 11-53 OCAÑA
I.P.S. CLINICA DIVINO NIÑO	CALLE 11 # 14-64 CENTRO
IN LINE CENTRO DE FISIOTERAPIA Y ESTETICA OCAÑA E.U.	CARRERA 11 NUMERO 12-47
LABORATORIO CLINICO ESPECIALIZADO LTDA	CALLE 10 # 14-34
LIGA NORTE SANTANDEREANA DELUCHA CONTRA EL CANCER CAPITULO OCAÑA	KR 12 # 9-56

MEDI-CARE LIMITADA	CALLE 7 NO 30-25 LOCAL 4
SALUD & ESTETICA CLINICA ODONTOLOGICA IPS LIMITADA	CARRERA 12 NO 8-89 B./ EL TORITO
UNIDAD MEDICA INTEGRAL MISION VISION LTDA-UMIVIS	CR 13 N. 9-13 LOCAL 104 CENTRO COMERCIAL ALMACENTRO