RESUMEN – TRABAJO DE GRADO

AUTORES	**Jenis del Carmen Sagbini Echávez**
FACULTAD	**Ingeniería**
PLAN DE ESTUDIOS	**Maestría en Gobierno TI**
DIRECTOR	**Torcoroma Velásquez Pérez - Edwin Edgardo Espinel Blanco**
TÍTULO DE LA TESIS	**Modelo de seguridad de la información bajo los principios de Gobierno TI para el sector industrial manufacturero**
TITULO EN INGLES	**Information security model under the principles of IT Governance for the industrial manufacturing sector**

RESUMEN
(70 palabras)

El presente proyecto de investigación propone un Modelo de Seguridad de la Información basado en los principios de Gobierno TI para el Sector Industrial Manufacturero. El desarrollo de este proyecto inicia con el análisis de los diferentes procesos en las empresas caracterizadas, luego se hizo una comparación de los estándares de buenas prácticas de seguridad de la información, para posteriormente, proponer un modelo que termina con la validación por expertos.

RESUMEN EN INGLES

This research project proposes an Information Security Model based on the principles of IT Governance for the Industrial Manufacturing Sector. The development of this project begins with the analysis of the different processes in the characterized companies, then a comparison of the standards of good information security practices was made, to later propose a model that ends with the validation by experts.

PALABRAS CLAVES	Gobierno TI, Industria, Información, Seguridad, Tecnología
PALABRAS CLAVES EN INGLES	IT Government, Industry, Information, Security, Technology

CARACTERÍSTICAS			
PÁGINAS: 120	PLANOS:	ILUSTRACIONES:41	CD-ROM:1

Modelo de seguridad de la información bajo los principios de Gobierno TI para el sector industrial manufacturero

Jenis del Carmen Sagbini Echávez

Facultad de Ingeniería, Universidad Francisco de Paula Santander Ocaña

Ingeniería de Sistemas

Phd. Torcoroma Velasquez Pérez

Phd. Edwin Edgardo Espinel Blanco

1 de junio de 2022

Agradecimientos

A Dios quien fue mi creador y alimenta mi ser diariamente de sabiduría.

A mis padres quienes estuvieron dispuestos a dar lo mejor para mi formación y desarrollo.

A mi directora de proyecto, la doctora Torcoroma Velásquez Pérez por su gran compromiso y dedicación para culminar satisfactoriamente este proceso.

Dedicatoria

A mis hijos; Alexandra y Andrés Felipe, quienes fueron mi inspiracion para el logro de este objetivo.

Indice

Lista de figuras

Lista de tablas

Lista de apéndices

Introducción

La tendencia hacia una creciente madurez global de los mercados y sus correspondientes desafíos hace que muchas organizaciones, especialmente en lo referido a sus sistemas de información y redes de trabajo, se vean enfrentadas a continuas amenazas de seguridad, incluyendo fraudes informáticos, espionaje, sabotaje, vandalismo, fuego o inundaciones. Igualmente, se viven otros tipos de amenazas como son los virus informáticos, ataques de cracker informáticos y demás riesgos eludibles. La dependencia que tienen actualmente los negocios de las tecnologías de la información y de las comunicaciones (TIC), especialmente de Internet, obliga a la búsqueda de métodos, técnicas y medios que ayuden a mantener la seguridad de funcionamiento correcto de los sistemas de información (SI) utilizadores de tales tecnologías. (Pablos Heredero L. H.-R., 2019)

Partiendo de allí, en el interior de las organizaciones, la seguridad de los sistemas de información, ha cobrado mucha importancia debido a que está basada en establecer procedimientos y estrategias para mantener la confidencialidad, integridad y disponibilidad de un núcleo fundamental como es la información, y lograr un desarrollo evolutivo de sus actividades y del crecimiento institucional.

Esta investigación pretende diseñar un modelo de seguridad de la información bajo los principios de gobierno de TI aplicado al sector industrial manufacturero de la ciudad de Barranquilla, Atlántico, Colombia. Inicialmente se tomarán los estándares requeridos para poder alinear la tecnología de la Información al direccionamiento estratégico de la empresa,

verificando cuáles son los estándares más aplicables para la estructuración del modelo para este sector productivo.

En el primer capítulo se encuentra el problema, los objetivos, la justificación y las delimitaciones. En el segundo capítulo se encontrarán todos los referentes teóricos, conceptuales, históricos y legales necesarios para conducir la investigación. El seguimiento metodológico se encuentra en el capítulo tres en donde se define el tipo, enfoque y alcance la investigación, la matriz de objetivos, la población objetivo, así como, las técnicas de instrumentos y su respectiva evaluación. Por último, en el capítulo cuarto, se muestran los resultados de la investigación, así como también la validación del modelo propuesto.

Resumen

En el presente proyecto, se establece el contenido de los elementos esenciales del Modelo de Seguridad de la Información para Empresas Manufactureras tomando como referentes metodologías y estándares, entre ellos: el Balance Score Card, COBIT 5.0 y la ISO 27002:20013, con el gran objetivo de lograr controlar efectivamente todos los procesos organizacionales y garantizando una confidencialidad, integridad y disponibilidad de la información.

Capítulo 1. Modelo de seguridad de la información bajo los principios de Gobierno TI para el sector industrial manufacturero

1.1. Planteamiento del problema

El uso de las TIC en las empresas industriales manufactureras ha generado transformación de los procesos: mejor planificación de los recursos, disminución de costos, aumento de movilidad y hay rapidez en la prestación de servicios logrando una facilidad en la inserción de una economía dinámica y cambiante. Lo anterior, ha permitido una mayor dependencia de las TIC (Tecnologías de la Información y las Comunicaciones) en el interior de todos sus procesos.

En Colombia, existe una gran preocupación de los empresarios dedicados a actividades manufactureras que utilizan las TIC en sus actividades cotidianas y es todo lo referente a los lineamientos establecidos y a la seguridad de la información. Los propietarios y directivos deben tomar decisiones de implementar TI en el interior de sus instituciones, sin embargo, existe una creciente preocupación en la toma de decisiones correctas. Chavarro y Hoyos[1] establecen que un problema de gran importancia que se ha podido observar debido a estudios realizados anteriormente acerca de Gobierno TI en empresas privadas, es la falta de conocimiento de estas políticas por parte de los gerentes y demás encargados de tomar decisiones de TI en las organizaciones. (Reales, 2014)

[1] TORO, Iván, VILLEGAS, Dora. Las PYMES: Una mirada a partir de la Experiencia Académica del MBA. (documento en línea: **http://www.eafit.edu.co/revistas/revistamba/Documents/pymes-mirada-a-partir-experiencia-academica-mba.pdf**) citado el 14 octubre de 2019

La MiPyme en Colombia generalmente inicia sus procesos administrativos y a medida que sus operaciones van creciendo, se generan procesos aislados, lo cual no constituyen integridad de la información. Esto genera decisiones gerenciales erróneas pues no se analizan todas las alternativas posibles como un sistema en conjunto. Esto obviamente no cumple con lineamientos lo que conlleva a toma de decisiones no adecuadas.

Diseñar un modelo de seguridad de la información teniendo como marco el Gobierno TI, permitirá aportar una gran mejora en la gestión adecuada de la información en una MiPymes, haciendo que todos los procesos resulten eficientes, ésto ayudará a cumplir todas la normatividad vigente legal colombiana, controlará múltiples plataformas tecnológicas de manera efectiva, evitará una cantidad considerada de fallas que puedan surgir en la institución que puedan afectar a la entidad, permitirá a ser menos vulnerable a los ciberataque y manejará de forma responsable la información con una mayor seguridad.

1.2. Formulación del problema

¿Cuáles son los componentes que integrarían un modelo de seguridad de la información bajo los principios de Gobierno de TI, para MiPymes industriales manufactureras?

1.3. Objetivos

1.3.1. General.

Formular un Modelo de Seguridad de la Información enmarcado en Gobierno de TI para el sector industrial manufacturero.

1.3.2. Objetivos específicos

- Diagnosticar el cumplimiento de los estándares de gobierno de TI requeridos para la gestión de la seguridad de la información aplicable al sector de la industria manufacturera.

- Estructurar los componentes enmarcados en Gobierno de TI en el diseño de un modelo de seguridad de la información para el sector industrial manufacturero.

- Validar el modelo planteado.

1.4 Justificación

Las empresas industriales manufactureras colombianas crecen de manera vertiginosa e incorporan a través del tiempo a las TI para generar un mayor valor en su negocio hasta el punto de que se vuelven tan dependientes en los procesos productivos, administrativos, recursos humanos, logísticos y de servicio al cliente que olvidan replantearse profundamente la importancia de alinear sus procesos de TI con las estrategias organizacionales. Teniendo en cuenta que los sectores manufactureros difieren de los sectores comerciales, este gremio se vuelve muy dependiente de los sistemas de información y esto hace que exista una creciente preocupación por la necesidad de proteger la información, manteniendo su integridad, disponibilidad y confidencialidad. Entones, aparecen las intimidaciones a la seguridad de lo más valioso en una organización: la información, aterrando a los empresarios de manera catastrófica a tal punto que cada día se extienden y fortalecen desde las cuentas bancarias hasta los servicios de fidelización. (Revista Semana, 2020) Es una realidad, las empresas manufactureras son

vulnerables a esto aún con la modernización de herramientas tecnológicas conectadas a internet. (Carolina Masso, 2018)

Según el DANE, en el último informe técnico de los resultados de la Encuesta Anual Manufacturera (EAM) que analizó 7.256 empresas manufactureras colombianas en el año 2018 y comparándolo con el año inmediatamente anterior, el 2017, el porcentaje de personal ocupado que usó internet pasó de 48,1% en 2017 a 52,8% en 2018 evidenciando un incremento considerable (DANE, 2019) Este crecimiento vertiginoso demuestra una vez más que la preocupación de los empresarios va en aumento, por lo que establecer e implementar estándares que permitan generar beneficios de negocio mediante el empleo de tecnologías de la información, asegurar una utilización óptima de los recursos tecnológicos y optimizar los niveles de riesgo de negocio relacionado con la tecnología de información, permitirá que estas empresas busquen eficacia en los procesos, compatibilidad con sus clientes, sus proveedores y con el mundo en general debido a la globalización de los negocios. (RSM, 2017)

Según (Ross, 2004) la Gobernanza de TI "es el marco que permite definir responsabilidades y tomar decisiones correctas para impulsar los comportamientos deseables en el uso de la TI en las organizaciones." Es por ello que se afirma que el Gobierno de TI, hace parte del gobierno corporativo y en las empresas industriales manufactureras logra un gran aporte debido a que su uso efectivo e innovador genera valor en el negocio, busca fortalecer la atención a los clientes y estimula la competitividad con elementos como calidad, eficiencia, efectividad, ejercicio de deberes y derechos. Un modelo de seguridad de la información enmarcado en Gobierno TI permite ser una herramienta fundamental para todas aquellas

empresas que aspiren a tener estándares de calidad en la industria lo cual redundará en una productividad, eficiencia y eficacia en los procesos.

1.5. Delimitaciones

1.5.1 Geográficas.

Este proyecto está enmarcado en las empresas del sector industrial manufacturero ubicadas en Barranquilla cuyas actividades centrales son la transformación de materias primas en bienes terminados para ser distribuidos y consumidos.

1.5.2 Temporales.

Para el desarrollo de investigación se proyecta un tiempo de 12 meses iniciando en el mes de junio 2020 a junio 2021 con base a la planificación de la Universidad Francisco de Paula Santander sede Ocaña.

1.5.3 Conceptuales.

En la investigación se tendrán en cuenta conceptos como seguridad de la información, Gobierno de TI, normas ISO 270001, normas ISO 270002 y las empresas del sector industrial manufacturero ubicadas en la ciudad de Barranquilla.

1.5.4 Operativa.

Para el presente proyecto se delimitarán un marco compuesto por las empresas categorizadas en el sector industrial manufacturero y los estándares de gobierno de TI.

Capítulo 2. Marco referencial

2.1 Marco histórico

Las Tecnologías de la Información y la Comunicación (TIC) han aportado grandes beneficios a las empresas y hoy en día existe una creciente necesidad de ellas para volverlas más competitivas y llegar a nuevos mercados. A través del tiempo se puede analizar la evolución que indiscutiblemente han tenido las TIC en las empresas y todos los componentes que involucran en su desarrollo.

2.1.1 Antecedentes

El sector industrial manufacturero se dedica a establecer procesos donde transfoman una materia con el fin de producir unos bienes que serán consumidos. Estos productos no requieren de un comercializador intermediario porque generalmente son negociados de forma directa (cvn.com.co, 2020). En Colombia, el 45% de las MiPymes pertenecen a este sector y son actores estratégicos en el crecimiento de la economía, la transformación del aparato productivo nacional y el mejoramiento de la posición competitiva del país (businesscol, 2016) (DNP,2018).

El sector manufacturero genera un gran número de empleos especialmente urbano debido a los procesos y procedimientos que realiza. Su comportamiento ha dependido siempre por una demanda interna y externa. A enero 2019, la demanda interna de productos de la industria manufacturera registró un crecimiento del 3,5%, lo que refleja una mejor dinámica de sus ventas reales. (cvn.com.co, 2020)

En cuanto a uso de tecnologías de la información en la industria manufacturea, en 2018, el 40,2% usaron internet dentro de sus instalaciones y lo hicieron principalmente con un ancho de banda entre 2.048 y 10.239 kbps, y el 27,0% tuvieron acceso a internet con un ancho de banda entre 10.240 y 30.719 kbps. (DANE, 2019)

En 2018, el 99,9% de las empresas industriales manufactureras que utilizaron internet lo hicieron para enviar y recibir correos electrónicos, el 97,8% lo utilizó para búsqueda de información y el 96,6% lo usó para realizar operaciones de banca electrónica. En 2018, el 30,1% de las empresas industriales manufactureras que usaron internet, vendieron sus productos a través de plataforma electrónica. Igualmente, el 33,9% de las empresas industriales informaron que utilizan una plataforma electrónica para la adquisición de insumos generando valor agregado a los procesos internos de las empresas. (DANE, 2019)

El Gobierno de TI se define como la estructura de relaciones y procesos para dirigir y controlar la empresa hacia el logro de sus objetivos, por medio de agregar valor, al tiempo que se obtiene un balance entre el riesgo y el retorno sobre las TI y sus procesos. (Muñóz, 2011). También se podría definir como: “es el uso eficiente de los recursos de TI para apoyar el cumplimiento de los objetivos del negocio” (ITGIRolling Meadows, 2008).

Estas dos definiciones, en la evolución sobre el Gobierno TI, invitan a tener en cuenta que existe una seria relación con los dos conceptos conocidos como: gobierno corporativo y gobierno de negocio. Si bien, el gobierno corporativo es la estructura más grande que permite dar reportes acerca de un determinado manejo económico, pero a su vez, es muy necesario poder controlar

procesos en el interior de la organización por lo que el gobierno de negocio ejecuta esos procesos y es allí donde se incluye allí el gobierno de TI.

El Gobierno de TI trabaja en cuatro ámbitos esenciales y estructurales: el primero, llamado Cumplimiento y Alineación que se encarga de la entrega de valor de los proyectos de TI, el segundo llamado Esquema de Gobierno TI cuyos objetivos son agrupar los factores necesarios de los procesos de gobernanza, el tercero llamado Gestión Integral de Proyectos de TI que adecúa la gestión de programas y proyectos asociados a TI, y por último y no menos importante, aquel que busca la adecuada planeación, ejecución, monitoreo y mejora de la prestación de los servicios de TI, por lo que se llama Gestión de la Operación de TI. (MINTIC, 2020)

La seguridad de la información es el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información. Es un concepto amplio que engloba medidas de seguridad que afectan a la información independientemente del tipo de esta, soporte en el que se almacene, forma en que se transmita, etc. Importante entender que esta definición no puede confundirse con la definición de seguridad informática. Esta es una rama de la seguridad de la información y busca de protegerla haciendo uso de una infraestructura informática y de telecomunicaciones para ser almacenada o transmitida. (Escrivá Gascó, 2013)

El radio de acción de la seguridad de la información cubre análisis de riesgos, seguridad del personal, seguridad física y del entorno, gestión de comunicaciones, desarrollo y mantenimiento de sistemas (de acuerdo a la ISO 27000). (Camelo, 2010)

2.2 Marco conceptual

2.2.1. Gobierno TI.

Es el sistema a través del cual se dirige y controla la utilización de las TI actuales y futuras. Supone la dirección y evaluación de los planes de utilización de las TI que den soporte a la organización y la monitorización de dicho uso para alcanzar lo establecido en los planes de la organización. Incluye las estrategias y políticas de uso de las TI dentro de la organización según (ISO IEC38500:2008 Corporate Governance of Information Technology).

2.2.2. Seguridad de la Información.

Son normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta. Esta definición se puede complementar señalando que en caso de que una amenaza a la seguridad se haga efectiva, debe procurar recuperar la información dañada o robada. Muchos investigadores y autores especializados en el tema de la seguridad informática por lo común se centran sólo en las tres características de la información mencionadas; no obstante, de acuerdo con el marco de gestión y de negocio global para el gobierno y la gestión de las TI (Tecnología Informática) de la empresa (COBIT por sus siglas en inglés), las características que debe poseer la información son: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, apego a los estándares y confiabilidad. (Baca Urbina, Introducción a la seguridad informática, 2016)

2.2.3. Sector Industrial Manufacturero.

Se refiere al conjunto de actividades que llevan como fin la transformación de materiales en nuevos productos. Se caracteriza porque estas labores se pueden hacer manualmente o con ayuda de máquinas o líneas de producción industrializadas que funcionan bajo la supervisión de una mano de obra que se convierte en vital. Estos nuevos productos pueden llegar a ser distribuidos directamente desde el punto de fábrica o en su defecto, a través de intermediarios. Las empresas del sector manufacturero pertenecen al llamado sector secundario de la economía colombiana y su razón es porque transforma a la materia prima que fue generada desde el sector primario.

Toda la labora que esta actividad económica despliega es posible por la intervención de tres pilares fundamentales como son: la fuerza del trabajo, las máquinas y las herramientas, que justamente posibilitan la producción en cuestión (https://www.definicionabc.com, 2020). Este sector se reúne u organiza en compañías diversas; que pueden ser pequeñas, medianas o grandes de acuerdo a los productos que elaboran.

2.3 Marco contextual

Barranquilla está ubicada al norte de Colombia, es la capital del departamento del Atlántico. Es un Distrito Especial, Industrial y Portuario ubicado en el lado occidental del río Magdalena 7,5 kilómetros de su desembocadura en el mar. En la Región Caribe Colombiana, es el centro económico más importante y desarrolla diferentes actividades como el comercio y la

industria.[2] (https://es.wikipedia.org/, 2019) También es conocida como “La Puerta de Oro de Colombia” o “Curramba la Bella” o “La Arenosa”. Es una de las principales ciudades de Colombia y también, se considera un destino turístico que sirve de referencias para personas locales y para extranjeros. (Procolombia, 2020)

Barranquilla tiene una población de 1.274.250 personas, convirtiéndola en la cuarta ciudad más poblada del Colombia. La ciudad es el núcleo del Área Metropolitana de Barranquilla, la cual está constituida además por los municipios de Soledad, Malambo, Galapa y Puerto Colombia. Por lo anterior, todo este sector alberga a un total de 2.199.507 habitantes, ocupando así, la cuarta posición entre las conurbaciones del país.[3] Barranquilla es la capital del departamento del Atlántico ubicándose allí la sede de la Gobernación, de la Asamblea Departamental y del Tribunal Superior, máximo órgano judicial del departamento. En Barranquilla se celebra el carnaval, festividad folclórica y culturale importante en Colombia, y fue declarado Patrimonio Cultural de la Nación por el Congreso de Colombia en 2001 y Patrimonio Oral e Inmaterial de la Humanidad por la Unesco en 2003. [4] La ciudad fue designada Capital Americana de la Cultura en 2013. [5] (https://es.wikipedia.org/, 2019)

La economía en Barranquilla se desarrolla principalmente en los sectores industria, comercio y servicios. De acuerdo al DANE (2015), el 12% de los establecimientos en Barranquilla se dedican a la industria, el 45.2% al comercio, 41.3% a servicios y el 1.4% a otra

[2] **«Composición de la economía de la región Caribe de Colombia»**. *Banco de la República (banco central de Colombia)*. 22 de mayo de 2013. Consultado el 21 de noviembre de 2017.

[3] «Censo DANE 2005». Consultado el 29 mayo 2020.
[4] «Proclamación 2003: "El carnaval de Barranquilla"». Sector de la Cultura de la Unesco.
[5] Lina Robles Luján - El Heraldo. «Barranquilla, elegida Capital de la Cultura 2013». Archivado desde el original el 24 de diciembre de 2012.

actividad. Los sectores que mayor concentran empleo en la ciudad son el comercio, restaurantes, hoteles y servicios comunales, con una proporción mayor al nacional. La industria manufacturera tiene una proporción menor a la nacional. En la ciudad se ha dado una desindustrialización del aparato productivo, la cual ha estado acompañada de un aumento del sector servicio que demanda mano de obra no calificada. Las empresas más importantes de Barranquilla son: Cementos Argos, Monómeros Colombo Venezolanos, Gases del Caribe, Cervecería Águila y Acesco. Se destaca la concentración de pequeñas empresas en la Zona Franca de Barranquilla y en el Parque Industrial Malambo. Las otras empresas pequeñas se especializan en la elaboración de productos farmacéuticos, industriales, químicos, grasas vegetales y aceites, calzado, bebidas, jabones, ladrillos, prendas de vestir y embarcaciones. El sector de la construcción experimenta desde hace algunos años una reactivación importante en Barranquilla, siendo inclusive sobresaliente a nivel nacional. La mayor proporción de los metros cuadrados construidos en los dos últimos años corresponden a proyectos de vivienda en todos los estratos. El resto corresponde principalmente a la construcción de almacenes de grandes superficies tales como Éxito, Carrefour y Centros Comerciales. (Alvarado Ortega, 2016)

Según la Encuesta Mensual Manufacturera con Enfoque Regional (EMMET)[6] Entre enero-diciembre de 2019 frente al mismo periodo de 2018, el índice de la producción real y ventas reales, por departamentos y clases industriales de la región Caribe, registró crecimiento en Atlántico y Bolívar, y descenso en Córdoba. En Atlántico el índice de producción y ventas fue impulsado principalmente por alimentos y bebidas; sustancias y productos químicos; y minerales

[6] ANDI (2020) Informe de la Encuesta de Opinión Industrial Conjunta, disponible en: **http://www.andi.com.co/Uploads/Informe%20%20EOIC%20Diciembre%202019%20VF.pdf** consultado el 26 febrero de 2020.

no metálicos. En el orden nacional, el desempeño de la actividad manufacturera entre enero y diciembre de 2019 fue de crecimiento. (Banco de la República, 2019)

De acuerdo a su categoría, existe un total de 6.158 empresas registradas al 2020. (informacolombia.com, 2020). En la Tabla 1 se observa la clasificación de ellas.

Tabla 1.

Empresas del sector industrial manufacturero de Barranquilla dedicadas a la producción de "otros tipos electrónicos"

CODIGO Y CATEGORÍA EMPRESAS	CANT
330 - Instalación, mantenimiento y reparación especializado de maquinaria y equipo.	1137
250 - Fabricación de productos elaborados de metal, excepto maquinaria y equipo.	976
100 - Elaboración de productos alimenticios.	720
140 - Confección de prendas de vestir.	673
310 - Fabricación de muebles, colchones y somieres.	362
200 - Fabricación de sustancias y productos químicos.	291
180 - Actividades de impresión y de producción de copias a partir de grabaciones originales.	283
160 - Transformación de la madera y fabricación de productos de madera y de corcho, excepto muebles; fabricación de artículos de cestería y espartería.	218
220 - Fabricación de productos farmacéuticos, sustancias químicas medicinales y productos botánicos de uso farmacéutico	179
320 - Otras industrias manufactureras.	179
130 - Fabricación de productos textiles.	158
230 - Fabricación de otros productos minerales no metálicos.	150
150 - Curtido y recurtido de cueros; fabricación de calzado; artículos de viaje, maletas, bolsos de mano y artículos similares, y artículos de talabartería y guarnicionería; adobo y teñido de pieles.	149
280 - Fabricación de maquinaria y equipo n.c.p.	140
240 - Fabricación de productos metalúrgicos básicos.	93
270 - Fabricación de aparatos y equipo eléctrico.	85
110 - Elaboración de bebidas	72
290 - Fabricación de vehículos automotores, remolques y semirremolques.	72
210 - Fabricación de productos farmacéuticos, sustancias químicas medicinales y productos botánicos de uso farmacéutico.	68
300 - Fabricación de otros tipos de equipo de transporte.	54
170 - Fabricación de papel, cartón y productos de papel y cartón.	44
260 - Fabricación de productos informáticos, electrónicos y ópticos.	35
190 - Coquización, fabricación de productos de la refinación del petróleo y actividad de mezcla de combustibles.	20
TOTAL EMPRESAS	**6158**

Fuente: https://www.informacolombia.com/directorio-empresas/actividad/2790_FABRICACION-DE-OTROS-TIPOS-DE-EQUIPO-ELECTRICO-N-C-P/localidad_barranquilla

De ese total, el 16% (10 empresas) corresponden a empresas del sector industrial manufacturero dedicadas a la producción de otros tipos electrónicos que es el clúster a estudiar en el presente proyecto.

Según el DANE, durante el cuarto trimestre de 2018, de las 9 actividades fabriles analizadas para Barranquilla, Soledad, Malambo, Cartagena y Santa Marta, 5 presentaron aumento en la producción y sumaron 5,6 puntos porcentuales a la variación total. La producción

industrial manufacturera de Barranquilla, Soledad, Malambo, Cartagena y Santa Marta presentó una variación de 7,0%, explicada principalmente por el aumento de Químicas básicas; Otras manufacturas y Otros productos químicos. (DANE, 2019)

Continuando con el entorno central del presente proyecto, y tomando una empresa del sector industrial manufacturera donde se toma como referencia principal para analizar y diseñar el modelo, a continuación se da a conocer los elementos esenciales de ésta: Ultraline Electrónica S.A.S., que está dedicada a la fabricación y comercialización de equipos de protección de voltajes para electrodomésticos, equipos de oficina, médicos e industriales, llamada anteriormente Ultraline de la Costa S.A., es una empresa industrial tipo pyme, inscrita en la cámara de comercio de Barranquilla con NIT N° 9004116093 y cuya matrícula mercantil es 514719-03, con forma jurídica de sociedad por acciones simplificada, cuyas operaciones comerciales iniciaron en el año 1999. En este sentido, Ultraline Electrónica S.A.S. se dedica a producir y comercializar equipos electrónicos tipo reguladores, elevadores de voltajes, multitomas, protectores de neveras, inversores, convertidores, transformadores de aislamientos, ups, baterías para ups, cargadores de baterías, entre otros.

En este orden de ideas, la empresa Ultraline Electrónica S.A.S. se encuentra ubicada con su centro de operaciones en la ciudad de Barranquilla, en el departamento de Atlántico, con domicilio social en la carrera 45 N° 60-37 en el Barrio Boston. Desde su fundación, los procesos de Ultraline Electrónica S.A.S., fueron crecido de forma consistente obligando ampliar sus operaciones productivas, comerciales y administrativas posicionándose en un mercado dinámico y competitivo. Con esto, cabe mencionar que de 5 personas que iniciaron laborando y 15 clientes

comercializando sus productos; hoy, 20 años después, se pueden calcular 250 clientes y 20 empleados directos. Por tanto, sus productos son conocidos en toda la Costa Atlántica de Colombia generando ingresos y recursos para muchas familias de la región norte colombiana. (Farello&Sagbini, 2019)

2.4 Marco teórico

La Teoría General de Sistemas (TGS), es una poderosa herramienta que permite la explicación de los fenómenos o una parte de ella (sistemas) que se suceden en la realidad y hace posible la predicción de la conducta futura de esa realidad. Es claro que un sistema está definido como conjunto de partes coordinadas para alcanzar ciertos objetivos, también es un enfoque interdisciplinario y dicho concepto fue discutido por perspectivas diferentes: la primera es la TGS (Teoría de Sistemas Generales), corriente iniciada por Von Bertalanffy y continuada por Boulding[7] y otros. El verdadero sentido de este enfoque es alcanzar la integración de las ciencias. El segundo enfoque se conoce como más práctico, cuyo nombre es "Ingeniería de Sistemas" o "Ciencias de Sistemas" iniciada por la investigación de Operaciones y seguida por la Administración Científica (Management Sciences) y finalmente por el Análisis de Sistemas.[8] (Johansen, 2000)

Una empresa es un sistema y como ello, permite interactuar con su entorno, está en una dinámica constante donde capta muchos datos, algunos que no tienen significación para ella, existen otros datos que le sirven permitiéndole tener mayor conocimiento de su entorno y de sus

[7] Es el enfoque de TGS (Teoría de General de Sistema) y el segundo enfoque que es el de Ciencias Aplicadas.
[8] Un interesante análisis de valor de esta rama del pensamiento sistemático se puede encontrar en J.R. Emshoff "Analysis of Behavioral Systems" (N. York, The Macmillan Co., 1971, pp823)

operaciones. A ello se le llama *información*, con la cual, se toman las decisiones más convenientes para la consecusión de objetivos dentro de las organizaciones. Así pues, la información a tiempo y en la cantidad precisa, es un factor clave para toda organización. En cualquier empresa, los directivos toman decisiones, preparan planes y controlan las actividades utilizando la información que pueden obtener, ya sea de fuentes formales o por medio de canales informales, tales como conversaciones cara a cara, llamadas telefónicas, contactos sociales, etc. Los directivos afrontan un entorno que se caracteriza por una creciente complejidad e incertidumbre. En estas circunstancias, y en teoría, el directivo debería ser capaz de definir el tipo de información que requiere y obtenerla. Sin embargo, en la práctica no ocurre de esta forma, sino que los directivos realizan su labor en función de la información disponible y accesible. Así, la mayoría de las decisiones son tomadas sin disponer de un conocimiento absoluto, ya sea porque la información no está disponible o por- que supondría un coste muy elevado el adquirirla. (Lapiedra Alcamí R. D., 2016)

La información, así como los procesos y sistemas que hacen uso de ella, son activos que toman mayor reelevancia en las organizaciones. La integridad, confidencialidad, y disponibilidad de ella, son fundamentales para perseverar los niveles de rentabilidad, competitividad, legalidad e imagen corporativa necesarios para lograr los objetivos de la organización y asegurar la creación de valor. En las organizaciones es necesario comprobar si se está siguiendo una buena política de gestión de seguridad de la información, incluyendo cualquier tipo de información que se procese en la misma, ya sea información digital o información en papel. Para gestionar la seguridad de la información, ésta se logra a través de procedimientos sistemáticos, documentados y conocidos dentro de la organización por el personal que lo tiene que aplicar y recogidos en un

Sistema de Gestión de la Seguridad de la Información (SGSI), o ISMS en inglés. Un SGSI tiene como objetivo final no garantizar la seguridad, sino garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (Pablos Heredero C. D.-R., 2019)

De acuerdo con (Coyle y Bardi,14), un sistema de información es una estructura interactiva de personas, equipo y procedimientos que hacen que la información relevante dentro de una organización esté disponible para planear, controlar e implementar con más facilidad cualquier tipo de innovación. (Baca Urbina, Proyectos de sistemas de información, 2016). Estos autores, logran dar la apertura a esa relación de los sistemas de información con las organizaciones.

Dado que la empresa se comporta como un sistema, es posible fragmentar sus partes en subsistemas. Según la literatura de teoría de la organización, se puede dividir la empresa en los siguientes sistemas: comercial, de operaciones, financiero, de personal, y de información. El sistema de información se relaciona con el resto de los sistemas y con el entorno. Un sistema de información en la empresa debe servir para captar la información que esta necesite y ponerla, con las transformaciones necesarias, en poder de aquellos miembros de la empresa que la requieran, bien sea para la toma de decisiones, bien sea para el control estratégico, o para la puesta en práctica de las decisiones adoptadas (Meguzzato y Renau, 1991). De ahí que el desempeño de un directivo dependa de su habilidad para explotar las capacidades de los sistemas de información para obtener unos positivos resultados empresariales. (Lapiedra Alcamí R. D.-U., 2016)

2.5 Marco Legal

2.5.1. CPC (Constitución Política de Colombia de 1991).

Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. (CorteConstitucional, 2016)

Artículo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura. (CorteConstitucional, 2016)

2.5.2. Ley 1266 de 2008.

"Por la cual se dictan las disposiciones generales del Habeas 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". (CongresodelaRepública, 2019)

2.5.3. Ley 1341 de 2009.

Por la cual se definen 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 de Espectro y se dictan otras disposiciones.

2.5.4. Ley 1581 de 2012.

Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. En ella, se establecen disposiciones generales para la protección de datos personales.

2.5.5.Decreto 1377 de 2013.

Reglamentando de forma parcial la Ley 158 de 2012 donde se expidió el Régimen General de Protección de Datos Personales, el cual, de conformidad con su artículo 1°, 15 y 20 de la constitución Política de Colombia de 1991.

2.5.6. ISO/IEC 17799:2005.

Esta norma establece un esquema sobre la definición de políticas, metodologías, o pautas técnicas que pueden ser utilizadas en el manejo de la seguridad de la información. Los beneficios que suman a las organizaciones que implementen estas normas, estarán basados en decisiones que poseen un marco referencial de la seguridad, asegurando de esta manera el desarrollo apropiado y generando mayor eficiencia y rentabilidad.

2.5.7. ISO/IEC 27000:2017.

Son guías de referencias que otorgan una manera de gestionar todo lo pertinente a la seguridad de la información. Ellas pueden ser utilizadas por las diferentes instituciones sin importar su tamaño, sector o tipo de capital económico. Puesto que la información es considerado un activo dentro de las organizaciones, el buen manejo de ella ocasionará el éxito, la

competitividad y su continuidad en un mercado cambiante y dinámico. Teniendo en cuenta eso, toda organización se preocupa por el aseguramiento de su información y sus sistemas, lo que conlleva a establecerlo como un objetivo de primer nivel.

2.5.8. NTC-ISO/IEC 27001:2013.

Brinda un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI).

2.5.9. NTC-ISO/IEC 27002:2013. Basado en BS 7799-1:1999 à ISO 17799:2005.

Provee un conjunto de controles de seguridad proporcionando recomendaciones de las mejores prácticas en la gestión de la seguridad de la información. Es por ello que todos los responsables que deseen iniciar o implantar o mantener un SGSI (sistema de gestión de seguridad de la información), le será de gran utilidad.

2.5.10. NTC-ISO/IEC 27005:2011.

Proporciona directrices para la gestión del riesgo en la seguridad de la información en una organización, dando soporte particular a los requisitos de un sistema de gestión de seguridad de la información (SGSI) de acuerdo con la norma NTC-ISO/IEC 27001. Sin embargo, esta norma

no brinda ninguna metodología específica para la gestión del riesgo en la seguridad de la información.

2.5.11. ITILV3 (Information Technology Infrastructure Library).

Es un conjunto de publicaciones de las mejores prácticas para la gestión del servicio de TI. ITIL®v3 proporciona guías de calidad para la prestación de servicios de TI y los procesos, funciones y otras competencias necesarias para sustentarlas.

2.5.12. COBIT 5. Objetivos de Control para Información y Tecnologías Relacionadas (Control Objectives for Information and related Technology)

Provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin mínimo de lucro o del sector público.

2.5.13. ISO/IEC 19941:2017(Information technology, Cloud computing, Interoperability and portability).

Establece un entendimiento común de interoperabilidad y portabilidad computación en la nube.

Capítulo 3. Diseño metodológico

3.1. Tipo de investigación

En este proyecto tendrá una investigación de tipo cuantitativo. La investigación cuantitativa es aquella que utiliza datos cuantitativos para recopilar información concreta, como cifras. Estos datos son estructurados y estadísticos. Brindan el respaldo necesario para llegar a conclusiones generales de la investigación. (surveymonkey, 2016) las técnicas cuantitativas emplean el método inductivo para producir conocimiento, ya que a partir de una cantidad de casos observados, con sus regularidades o puntos en común, se establecen generalizaciones confiables. (Ackerman, 2013)

El alcance de la investigación será descriptivo, debido a que describirá la realidad de situaciones, eventos, personas, grupos o comunidades que se estén abordando y que se pretenda analizar. En este tipo de investigación la cuestión no va mucho más allá del nivel descriptivo; ya que consiste en plantear lo más relevante de un hecho o situación concreta pero el investigador debe definir su análisis y los procesos que involucrará el mismo. (universia, 2017)

3.2. Seguimiento metodológico del proyecto

A continuación, se describe en una matriz de objetivos, todas las actividades que corresponden a cada objetivo que se desarrollará, incluyendo los respectivos indicadores. Todo esto permitirá hacer el diseño del modelo de seguridad de la información basado en Gobierno TI aplicable en empresas del sector industrial manufacturero.

Tabla 2.

Modelo Metodológico de la Investigación

OBJETIVOS DE LA INVESTIGACIÓN	ACTIVIDADES POR OBJETIVO	INDICADOR POR ACTIVIDAD
Obj 1. Diagnosticar el cumplimiento de los estándares de gobierno de TI requeridos para la gestión de la seguridad de la información en el sector de la industria manufacturera.	Act 1. Seleccionar los elementos requeridos de estándares asociados con seguridad de la información aplicables al sector manufacturero	Indicador 1. Elementos de los estándares identificados
	Act 2. Diseñar instrumento	Indicador 2. Instrumento
	Act 3. Aplicar el instrumento	Indicador 3. Información sistematizada
	Act 4. Análisis de información	Indicador 4. Diagnóstico
Obj 2. Estructurar los componentes enmarcados en Gobierno de TI diseñando un modelo de seguridad de la información para el sector industrial manufacturero.	Act 1. Identificar los componentes que pueden integrar el modelo	Indicador 4. Componentes identificados
	Act 2. Elaborar un documento que permita la estructuración de los componentes y la explicación del mismo	Indicador 5. Modelo diseñado
Obj 3. Diseñar la estrategia de valoración del Modelo de Gestión de Gobierno TI para las empresas manufactureras utilizando un panel de expertos	Act 1. Seleccionar la metodología a utilizar	Indicador 5. Método seleccionado
	Act 2. Diseñar y aplicar los instrumentos de la valoración por expertos	Indicador 6. Instrumentos de la valoración
	Act 3. Analizar los resultados de valoración por expertos	Indicador 7. Conclusiones de la valoración por expertos

Fuente: Autora

3.3. Población

La población o universo es el conjunto de objetos, sujetos o unidades que comparten la característica que estudio y a la que se pueden generalizar los hallazgos encontrados en la muestra (aquellos elementos del universo seleccionados) para ser sometidos a la observación. La definición de la población para un proyecto de investigación responde a la necesidad de especificar el grupo al cual son aplicables los resultados del estudio. Cuando el universo está compuesto por un número relativamente alto de unidades resulta imposible o innecesario examinar cada una de las unidades que lo componen. En tal caso, se procede a extraer una muestra, o sea, un conjunto de unidades, una porción del total que represente la conducta del universo total. Al emplear una muestra se busca lograr que, observando una porción relativamente reducida de unidades, se pueden obtener conclusiones semejantes a las que se lograría si se estudiará el universo total. (Monje, 2011)

En la presente investigación, se identificarán todas las empresas del sector industrial manufacturero tipo MiPyme ubicadas en la ciudad de Barranquilla que se dedican a la producción de artículos eléctricos y electrónicos, categorizados según la DIAN con el código 270 – Fabricación de aparatos y equipo eléctrico que tienen varias subcategorías donde se selecciona la subcategoría 2790 - Fabricación de otros tipos de equipo eléctrico n c p debido a que especifica de esta forma aquellas empresas que producen los bienes a que está direccionada la presente investigación. Es cuando se encuentran un total de 10 empresas, considerada la población a analizar. A continuación, se describen los nombres de estas MiPyme:

Tabla 3.

Empresas del Sector Manufacturero en Barranquilla a encuestar en el presente proyecto

NOMBRE DE LA EMPRESA	CIUDAD	TELÉFONO	PERSONAS QUE LABORAN EN EL DPTO DETI	PERSONAS A ENCUESTAR (LÍDER DE TI)
Compañía General de Mantenimiento y Montajes S.A.	Barranquilla	53608835	3	1
E.I.S. Colombia S.A.	Barranquilla	53417621	4	1
Sodinel S.A.S. administrativo@sodinel.com Adriana	Barranquilla	53049924	2	1
Ultraline Electrónica S.A.S.	Barranquilla	53638880	1	1
Lifeproof AP S.A.S.	Barranquilla	53049270	1	1
Consultoriía e Ingeniería de la Costa S.A.S.	Barranquilla	53242113	5	1
Iluminación Ecológica S.A.	Barranquilla	53602211	3	1
Metelectricos de la Costa Ltda.	Barranquilla	53709571	1	1
Cooperativa de Trabajo Asociado de Gestión y Desarrollo	Barranquilla	53693807	1	1
Divices y Technology S.A.S.	Barranquilla	53451341	1	1

Fuente:https://www.informacolombia.com/directorioempresas/actividad/C_INDUSTRIASMANUFACTURERAS/localidad_barranquilla (www.informacolombia.com, 2020) y Autora

3.4. Muestra

Según María Antonieta Tapia B. , la muestra es un subconjunto de la población o parte representativa. Una unidad de muestra está constituida por uno o varios de los elementos de la población y que dentro de ella se delimitan con precisión. Para que una muestra posea validez técnico estadística es necesario que cumpla con los siguientes requisitos: ser representativa o reflejo general del conjunto o universo que se va a estudiar, reproduciendo de la manera más exacta posible las característica de éste; que su tamaño sea estadísticamente proporcional al tamaño de la población y que el error muestral se mantengan dentro de límites aceptables. (TapiaB., 2000) El diseño de la muestra es una tarea específica, de implicaciones

metodológicas y requerimientos técnicos, destinada a elegir una representación adecuada de unidades de una población objeto de estudio. (López-RoldánPedro&FachelliSandra, 2017)

En tal sentido, esta investigación será de tipo cuantitativa por lo que se realizarán las técnicas adecuadas de recolección de información para lo cual, se tomará una representación significativa que consiste en todos aquellos líderes del área de TI de las empresas categorizadas como MiPymes cuyas actividades pertenecen al sector industrial manufactureras de la ciudad de Barranquilla.

3.5. Técnicas de recolección de la información

Las técnicas se vuelven respuestas al "*cómo hacer*" y permiten la aplicación del método en el ámbito donde se aplica. Los instrumentos son los apoyos que se tienen para que las técnicas cumplan su propósito. (Baena Paz, 2017)

Para el desarrollo de esta investigación se utilizarán instrumentos como la entrevista y el cuestionario. Para obtener información detallada, las entrevistas resultan siendo una herramienta muy valiosa y a través del tiempo, han demostrado ser unas herramientas populares en el ámbito investigativo. En lo que se refiere a las encuestas, se utilizarán en formato digital, debidamente diseñadas, que permitirán mayor confianza y lograrán legitimar de manera confidencial el comportamiento de las personas a encuestar. El enlace para realizar la encuesta es (Apéndice A) : **https://forms.gle/CSrqSbGw9wJYBeYa8**.

Para el logro del objetivo de diagnosticar el cumplimiento de los estándares de Gobierno de TI requeridos para gestionar la seguridad de la información aplicable al sector

manufacturero, se realizará una investigación documental considerada la búsqueda de una respuesta específica a partir de la indagación en documentos. En efecto, Maurice Duverger, se refiere a documento como todo aquello donde ha dejado huella el hombre en su paso por el planeta. (Baena Paz, 2017)

En lo que tiene que ver, a estructurar los componentes enmarcado en Gobierno de TI en el diseño de un modelo de seguridad de la información para el sector industrial manufacturero, se utilizará como prueba piloto el instrumento y será validado por personas expertas en la temática.

3.6. Analisis de la información

El vocablo “Análisis” proviene del griego “*analusis*” (disolución) derivada, a su vez de “*analuein*” (desatar, soltar). Por su parte, el Diccionario de la Real Academia Española (edición de 1992) define el término “*análisis*” como “*distinción y separación de las partes de un todo hasta llegar a conocer sus principios o elementos*” (Lopez, 2002)

Para la realización del análisis en esta investigación, se tomarán a cada uno de los objetivos, así, para el objetivo número uno planteado, se realizará un cuadro comparativo de los diferentes estándares y esto permitirá dar respuesta a partir de los datos encontrados. En cuanto al objetivo número dos que tiene que ver con estructurar los componentes del diseño del sistema de un modelo se seguridad de la información enmarcado en Gobierno TI, hace referencia a la tabulación de los datos hallados, así como también a la exploración de los datos ordenadamente.

Capítulo 4. Resultados

En el presente capítulo se plasman los resultados de la investigación realizada. Estos resultados fueron obtenidos basados en los objetivos planteados inicialmente en el proyecto y se comienza con una identificación de los estándares existentes en cuanto a prácticas de seguridad de la información, se hace una comparación y luego se analizan los procesos organizacionales de seguridad de la información en las instituciones manufactureras de la ciudad de Barranquilla. Por último, se estructuran los componentes del modelo de seguridad de la información para la Industria Manufacturera.

4.1. Identificación de los estándares de prácticas de seguridad de la información existentes

Se considera estándares a aquellas especificaciones de cómo se debe desarrollar una tarea o función determinada. Ellos están basados en unos acuerdos realizados entre una o más entidades o también, en un determinado grupo de personas. En este orden de ideas, aquí se plantea iniciar un análisis de todos aquellos estándares que hacen relación a las prácticas de seguridad de la información y en este punto de la investigación, se inició la labor de la búsqueda de ellos.

Para obtener un análisis de los estándares de prácticas de seguridad de la información existentes, fue necesario hacer una búsqueda metodológica basado en datos bibliográficos de ellos, con el objetivo de estudiarlos, analizarlos y lograr hacer un cuadro comparativo representativo que permitiera sacar las conclusiones ilustrativas.

Es por ello que, el análisis se basó en el estudio de la familia de normas ISO (27000, 27001, 27002, 27005), ITIL V3 2011 y el COBIT 5, que son considerados los estándares más importantes para las prácticas en la seguridad de la información.

4.1.1. ISO (27000, 27001, 27002, 27005)

Se denomina ISO a la Organización Internacional para la Estandarización, la cual se trata de una federación cuyo alcance es de carácter mundial, ya que está integrada por cuerpos de estandarización de 162 países. Esta organización se estableció en 1947, como un organismo no gubernamental, cuya misión es promover a nivel mundial el desarrollo de las actividades de estandarización. La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) han desarrollado una serie de normas internacionales de amplísima difusión a nivel mundial al respecto de esta problemática. Mediante el uso de la familia de normas UNIT-ISO/IEC 27000, las organizaciones pueden desarrollar e implantar un marco para la gestión de la seguridad de sus activos de información, incluyendo información financiera, propiedad intelectual y detalles de sus empleados, o información confiada a la organización por sus clientes o terceras partes. (Pineda, 2016)

La ISO 27001 está alineado con ISO 9001 e ISO 14001, a su vez contiene las mejores prácticas que especifican el desarrollo e implementación de los Sistemas de Gestión de la Información (SGSI); esta norma se compone de 11 secciones y el anexo A que contiene los 114 controles , donde las tres primeras secciones(0 - 3) son introductorias lo que significa que no son obligatorias para la implementación, de la sección 4 al 10 son de

obligatoria implementación en una organización; la norma es certificable. (QUINTERO, 2018)

Esta norma adopta el modelo de procesos “Planificar-Hacer-Verificar-Actuar”. Esto reflejará los principios establecidos en las Directrices OCDE (2002) que controlan la seguridad de sistemas y redes de información. También brinda un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad. ((ICONTEC), 2006)

Por consiguiente, la ISO/IEC 27002, logra entregar directrices de los controles y la aplicación para una seguridad de la información en un código de buenas prácticas para la gestión de la información. El principal objetivo de la ISO 27002 es establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. (https://ostec.blog/, 2018) La diferencia entre la ISO 27001 y 27002 se basa en el nivel de detalle pues la ISO 27002 explica un control en una página entera mientas que la ISO27001 dedica solo una frase a cada control. (https://advisera.com/, 2016)

En ISO/IEC 27005 proporciona directrices y está orientado a los procesos para la implementación y cumplimiento de la gestión del riesgo de la seguridad de la información tratando la gestión de riesgo en la seguridad de la información. (QUINTERO, 2018)

4.1.2. ITIL

Sus siglas en inglés ITIL (Information Technology Infraestructure Libraly) se refiere a la Biblioteca de Infraestructura de Tecnologías de Información, que es un conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. (https://www.servicetonic.com/, 2019). Resumiendo, ITIL es un marco de referencia mundial de la gestión de servicios de TI.

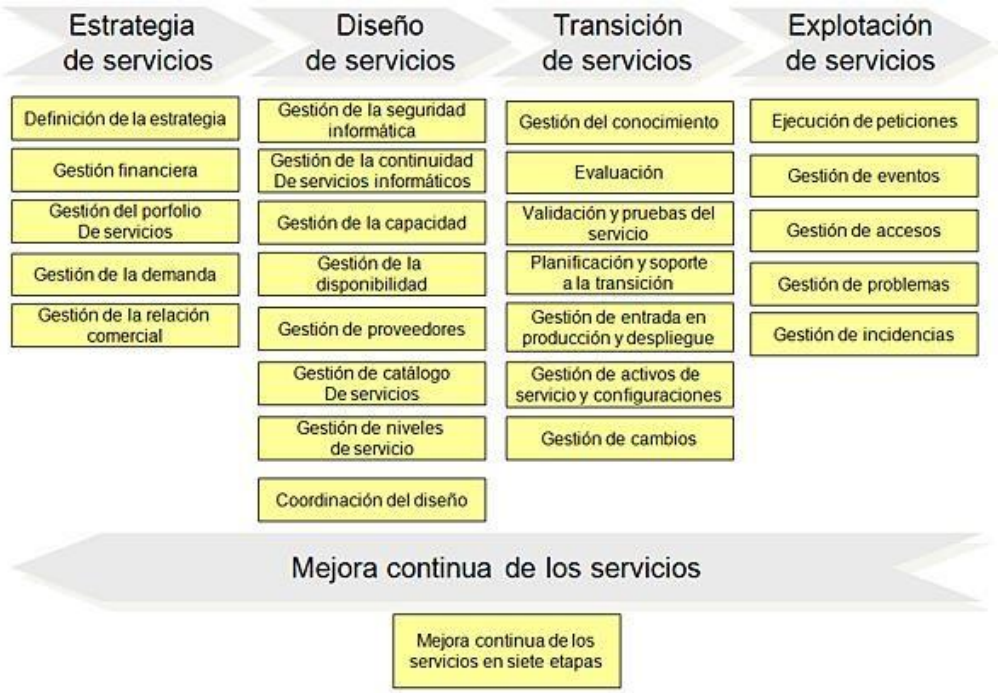
Aunque se desarrolló durante los años 1980, ITIL no fue ampliamente adoptada hasta mediados de los años 1990. Esta mayor adopción y conocimiento ha llevado a varios estándares, incluyendo ISO/IEC 20000, que es una norma internacional cubriendo los elementos de gestión de servicios de TI. (https://nextech.pe/, 2018)

Si bien ITIL se fundamenta en el establecimiento de un “Ciclo de Vida del Servicio” ampliado por subprocesos tan especificados que se convierten en procesos especializados. La evolución de las versiones de ITIL han sido muy reconocidas, pero en el presente proyecto, se estudiará la V3 de 2011, porque adiciona un proceso que permite esclarecer el como fluyen las actividades en el ciclo de vida del diseño del servicio.

ITIL V3 se sustenta en 26 procesos establecidos en cuatro funciones que se esquematizan en la siguiente gráfica dando a conocer las fases del ciclo de vida de los servicios y los procesos asociados:

Figura 1.

Procesos del ITIL V3



Fuente: ITIL V3-2011 – Preparación para la Certificación ITIL Foundation V3

4.1.3. COBIT 5.0

A propósito de COBIT 5 (Control Objetives for Information and Related Technologies); es un marco de trabajo que permite comprender el gobierno y la gestión de las tecnologías de información (TI) de una organización, así como evaluar el estado en que se encuentran las TI en la empresa. También se puede definir como un conjunto de herramientas de soporte empleadas por los gerentes para reducir la brecha entre los requerimientos de control, los temas técnicos y los riesgos del negocio. (https://www.esan.edu.pe/, 2016)

Tabla 4.

Cuadro comparativo de Estándares de Seguridad de la Información

ESPECIFICACIONES	ISO 27000:2017	ISO 27001:2013	ISO27002:2013	ISO 27005:2011	ITILV3 2011	COBIT 5
Definición	Marco de referencia de seguridad de la Información	Marco de Seguridad de la Información	Marco de referencia buenas prácticas de seguridad de la Información	Marco de Referencia de gestión del riesgo Seguridad de la Información	Mapeo de la Gestión de Niveles de Servicio de IT	Marco de Referencia de Gestión de Procesos - Mapeo de Procesos TI
Concepto	Entrega una visión general de los SGSI, términos y definiciones de uso común	Proporciona los requisitos necesarios para establecer, implantar, mantener y mejorar un SGSI	Es un estándar de Buenas Prácticas que permite describir los objetivos y controles en Seguridad de la Información	Contiene directrices para la gestión del riesgo de Seguridad de la Información.	Marco de trabajo de Buenas Prácticas dirigida a facilitar la entrega de servicios de Tecnologías de la Información. Son procedimientos de gestión que ayuda a las empresas a alcanzar la calidad en la operaciones de TI.	Compendio de mejores prácticas para el manejo de la información. Creado por ISACA y el ITGI
Areas de Aplicación	10 dominios	14 dominios, 10 procesos	14 dominios	N/A	26 procesos, 5 fases	37 procesos, 7 facilitadores, 2 dominios, 5 principios
Controles	N/A	114	114	N/A	N/A	N/A
Enfoque	Procesos	Procesos	Procesos	Riesgos	Procesos	Procesos
Finalidad de la Implementación	Cumplir el estándar de seguridad de la información	Evaluar el riesgo de la información	Definición de directrices para implementar controles	Gestionar los riesgos de la SI	Gestiónar niveles del servicio	Auditar los SI
Es Certificable?	No	Sí	No	No	No	No

Fuente: Autora

Teniendo en cuenta que el presente proyecto está orientado hacia el desarrollo de un modelo de seguridad de la información bajo los principios de Gobierno TI para el sector industrial manufacturero y revisada toda la bibliografía de los diferentes estándares; se llegó a la conclusión que se tomarán como referentes dos estándares: la norma ISO 20001 y escenario de trabajo integral denominado COBIT 5 para la gobernaza y gestión de TI.

En este orden de ideas, se hace necesario explicar que en el interior de las instituciones, los sistemas de gestión establecen estructuras que garantizan la ejecución correcta de las actividades. La norma técnica colombiana NTC ISO IEC 27001 del año 2013, suministra los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información. Se conoce entonces, que con ello se busca preservar la confidencialidad, la integridad y la disponibilidad de la información, haciendo uso de una adecuada gestión y tratamiento de los riesgos. (ICONTEC, 2013)

Esta norma contiene información del modelo PDCA y explica detalladamente los requerimientos de cada parte. Está conformada de 11 secciones, donde algunas son obligatorias y otros no lo son, como también, contiene 114 controles que son implementados siempre que la Organización considere importantes para poder certificarse. Las secciones obligatorias que contiene la norma inician de la 4 a la 10, debido a que las no obligatorias corresponden de la 0 a la 3. Estas secciones obligatorias, siempre deberán implementar todos los requerimientos de la norma. A continuación, se hacer una breve descripción de estas secciones:

Tabla 5.

Secciones de la Norma ISO IEC 27001 del año 2013

· Sección 0 Introducción. Explica el objetivo de la norma y su compatibilidad con otras normas.
· Sección 1 Objeto y campo de aplicación. La norma da orientaciones sobre el uso, finalidad y aplicabilidad a cualquier tipo de organización, además también menciona sobre los requisitos para la valoración y tratamiento del riego.
· Sección 2 Referencias normativas. Hace referencia a la norma ISO/IEC 27000 estándar que proporciona términos y definiciones.
· Sección 3 Términos y definiciones. Describe los términos y definiciones aplicable al estándar.
· Sección 4 Contextos de la organización. Define los requerimientos, partes interesadas, requisitos, contexto y alcance del SGSI de la organización
· Sección 5 Liderazgo. Se define la responsabilidad y compromiso de la dirección, establecimiento de roles, responsabilidades y la política de seguridad de la información.
· Sección 6 Planificación. Detalla los requerimientos para la evaluación, tratamiento y plan de tratamiento del riesgo, declaración de aplicabilidad y determinación de los objetivos de seguridad de la información.
· Sección 7 Soporte. En esta sección la norma especifica sobre la disponibilidad de recursos, competencias, conciencia, comunicación, documentación, control de documentos y registros del SGSI.
· Sección 8 Operación. En esta sección se formula e implementa el plan de tratamiento de riegos , implementación de controles y valoración del riesgo.
· Sección 9 Evaluación del desempeño. Se define los requerimientos de seguimiento, monitorización, medición, análisis, evaluación, auditoria interna y revisión de la dirección del SGSI
· Sección 10 Mejora. Se determina la mejora continua y eficacia del SGSI de la organización, además establece requerimientos para el tratamiento de las no conformidades.

Fuente: Norma ISO IEC 27001 del año 2013

Igualmente, el Anexo A, establece 114 controles distribuidos en 14 dominios, los cuales se describen a continuación:

Tabla 6.

Dominios ISO/IEC 27001:2013

Dominios ISO/IEC 27001:2013
A.5 Políticas de la seguridad de la información. Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes. Cuenta con 2 controles relacionadas con la política de seguridad de la información.
A.6 Organización de la seguridad de la información. Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización. Este dominio establece 5 controles donde define la asignación de responsabilidades, la seguridad de la información en la gestión de proyectos, teletrabajo y dispositivos móviles.
A.7 Seguridad de los recursos humanos. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran, además tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan. Para el dominio de la seguridad de los recursos humanos 6 controles que tratan del proceso de selección de candidato, contratación y terminación o cambio de actividades.
A.8 Gestión de activos. Identificar los activos organizacionales defiendo responsabilidades que permitan asegurar que la información recibe protección; evitando la divulgación, la modificación, el retiro o la destrucción de la misma. En este dominio se encuentran 11 controles relacionados al inventario, propiedad, uso, manejo, devolución y clasificación de activos, clasificación y etiquetado de la información y manejo de medios de almacenamiento de la información.
A.9 Control de acceso. Asegurar el acceso de los usuarios autorizados y evitar el acceso de usuarios no autorizado a sistemas y servicios. Para el dominio de control de acceso están definidos 14 controles específicamente para el requisito de política de control de acceso, gestión de control de acceso y responsabilidad de los usuarios, control de acceso a sistemas y aplicaciones.
A10 Criptografía. Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información. En este dominio están descritos 2 controles criptográficos.
A.11 Seguridad física y del entorno. Prevenir el acceso físico no autorizado, la perdida, el daño, robo e interferencia de la información. En la seguridad física y del entorno se encuentran 15 controles que están relacionados con la definición de áreas seguras y protección de los equipos contra perdida, daño o robo.
A12 Seguridad de las operaciones. Asegurar que la información y las instalaciones de procesamiento de información estén protegidas y las operaciones sean seguras y correctas. Los controles relacionados con este dominio son 14 donde se definen controles de gestión de cambio, capacidad y vulnerabilidad, contra códigos maliciosos, protección y respaldo de la información, registros de eventos, sincronización de relojes.
A13 Seguridad de las comunicaciones. Asegurar y mantener la seguridad y protección de la información. En este dominio se definieron 7 controles relacionados con la gestión de la seguridad de las redes y transferencia de la información.
A14 Adquisición, desarrollo y mantenimiento de sistemas. Asegurar la protección de los datos y que la seguridad de la información sea parte integral sea parte integral de los sistemas. Este dominio contiene 13 controles que definen la seguridad de la información y la protección de los datos de prueba.
A15 Relaciones con los proveedores. Asegurar y mantener la seguridad de la información de acuerdo con los acuerdos con los proveedores. Este dominio contiene 5 controles que determinan la política, tratamiento y cadena de suministro de los proveedores y a su vez el seguimiento, revisión y gestión de cambio de los mismo.
A16 Gestión de incidentes de 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. Este dominio contiene 7 controles de reporte de eventos y debilidades, evaluación de eventos, respuesta de incidentes y recolección de evidencia.
A17 Aspectos de seguridad de la información de la gestión de continuidad de negocio. Asegurar la disponibilidad y continuidad de la información. Aquí se encuentran 4 controles para la continuidad de la seguridad de la información y las redundancias.
A18 Cumplimiento. Asegurar que la seguridad de la información se implemente y opere de acuerdo a las obligaciones legales, estatutarias o contractuales. Para el cumplimiento del dominio se identifican 8 controles que se requieren para el cumplimiento de los requisitos legales y contractuales y revisiones de la seguridad de la información (ISO, 2013)

Fuente: (ISO, 2012)

COBIT fue creado para ayudar a las organizaciones a obtener el valor óptimo de TI manteniendo un balance entre la realización de beneficios, la utilización de recursos y los niveles de riesgo asumidos. COBIT 5 posibilita que TI sea gobernada y gestionada en forma holística para toda la organización, tomando en consideración el negocio y áreas funcionales de punta a punta, así como los interesados internos y externos. COBIT 5 se puede aplicar a organizaciones de todos los tamaños, tanto en el sector privado, público o entidades sin fines de lucro. (https://geniusitt.com/, 2018)

COBIT, lanzado en 1996, es una herramienta de gobierno de Tl que ha cambiado la forma en que trabajan los profesionales de Tl. Vinculando tecnología informática y prácticas de control, COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores. COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, minicomputadoras y ambientes distribuidos. Está basado en la filosofía de que los recursos de Tl necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos. Misión: Investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes y auditores. (Rojas Córsico, 2009)

COBIT establece que el Gobierno Corporativo de TI tiene 5 áreas clave de atención que en su conjunto aseguran la creación de valor de TI y evitan que se pierda el valor ya creado. Estos cinco dominios son:

Figura 2.

Componentes COBIT de un sistema de Gobierno TI

Fuente: Marco de Referencia COBIT 5.0 (ISACA, Marco de Referencia COBIT:2019 Objetivos de Gobierno TI, 2019)

COBIT 5 está basado en los siguientes cinco principios:

1. COBIT 5 es un modelo integrador. Dentro de este principio, incluye material previo de COBIT y de ISACA, como también de terceros. Posee una estructura muy sencilla que permite ser integrador de cualquier otra norma razonable. Por proponer un modelo de

referencia de procesos, no es prescriptivo, lo cual conlleva a una gran ventaja para su aplicación.

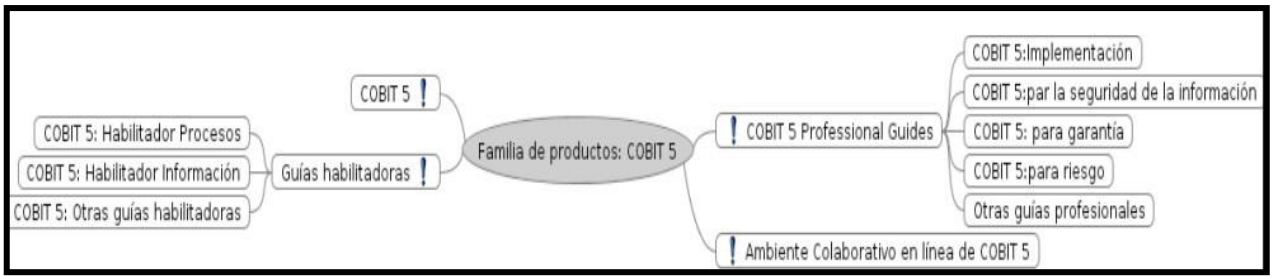
2. COBIT 5 está regido por la persecución del valor de todas las partes interesadas llamadas también, *stakeholders*.
3. Está orientado al negocio, lo que quiere decir que tiene la facultad de encontrar oportunidades para establecer nuevos productos y servicios en su actuación, no está demás, afirmar, que en un sentido genérico, pues también incluye a las administraciones públicas o entidades sin ánimo de lugro como las ONGs, entre otras.
4. El COBIT 5.0 está basado en los 7 habilitadores. Ver Figura 2. Componentes COBIT de un sistema de Gobierno TI
5. Está estructurado en procesos de Gobierno Corporativo y de Gestión [Administración] diferenciados, pero interrelacionados.

COBIT 5 establece una distinción con claridad entre los objetivos de gobierno y los objetivos de Gestión. El primero, que busca encontrar el logro de los objetivos empresariales evaluando las necesidades de todos los accionistas y que incluye también las condiciones existentes. El segundo, está relacionado directamente con un proceso explícito de gestión. Es por ello, que en los procesos de gestión, están involucrados componente del dominio de la media y alta gerencia. Si estos objetivos no están bien definidos, muy difícilmente se lograrán los objetivos de gobierno pues deberán estar alineados para compararlos y encaminarlo a la consecución de los objetivos de toda empresa que desee tener liderazgo y mantener un dinamismo empresarial.

También es importante conocer, que, COBIT 5 está estructurado por un grupo de prospectos llamadas “Familia de Productos COBIT 5”, la cual, se muestra a continuación.

Figura 3.

Familia de productos COBIT 5



Fuente: Marco de Referencia COBIT 5.0 (ISACA, Marco de Referencia COBIT:2019 Objetivos de Gobierno TI, 2019)

Se trata de un conjunto de Guías Profesionales utilizadas para las actividades prácticas de Implementación del modelo (COBIT 5 Implementación), seguridad de la información (COBIT 5 for information security), auditoría (COBIT 5 for assurance) y gestión de riesgos (COBIT 5 for risk), además de otras guías profesionales relacionadas (Other Professional Guides), que serán desarrolladas por ISACA en el futuro. En síntesis, la familia de COBIT 5 tiene como principales objetivos (Reis, 2015):

- Reunir las publicaciones COBIT 4.1, Val IT 2.0, RiskIT y BMIS de ISACA en una estructura única.

- Ampliar las áreas de TI que necesitan de contenidos más elaborados y actualizados

- Alinearse con otras normas y principales estructuras de mercado

- Definir un conjunto de habilitadores de gobernanza y gestión a partir de una estructura básica

- Posibilitar la inclusión de nuevos contenidos a base de conocimiento definidos en COBIT

- Ofrecer una sólida y abarcadora base de referencia de buenas prácticas en TI (Reis, 2015)

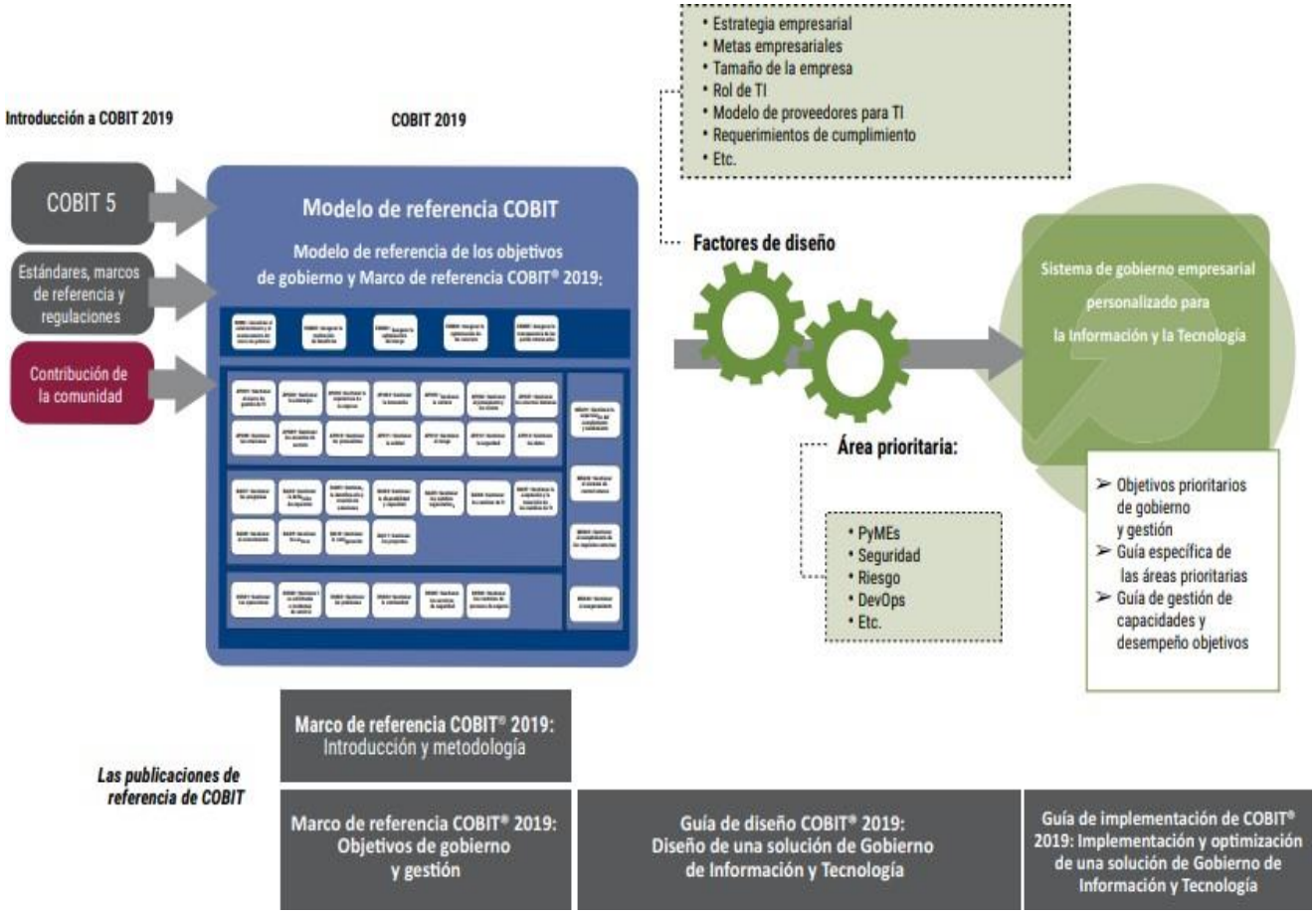
Los objetivos de gobierno y gestión de COBIT están organizados en los llamados dominios, los cuales son cinco. Ellos son clasificados a través de verbos los cuales expresan el objetivo principal y los sectores de actividad que los contienen:

• Los dominios Evaluar, Dirigir y Monitorizar (EDM en inglés) hacen parte del Objetivo de Gobierno. Aquí, en este dominio, el órgano de gobierno determina las opciones estratégicas, orienta a la alta gerencia acerca de las opciones estratégicas elegidas y hace control el logro de la estrategia.

• Los cuatro dominios: Alinear, Planificar y Organizar (APO), Consturir, Adquirir e Implementar (BAI), Entregar, Dar Servicio y Soporte (DSS) y Monitorizar, Evaluar y Valorar (MEA) forman parte de los Objetivos de Gestión.

Figura 4.

Visión General del COBIT 5.0 – 2019



Fuente: Marco de referencia COBIT® 2019: Objetivos de Gobierno y Gestión

COBIT 5:2019 tiene establecida una organización de los objetivos de gobierno y los objetivos de gestión. De esta manera, entrega toda la información pertinente que hace referencia a cada uno de los integrantes facilitando su entendimiento y aplicación. A continuación, en la Tabla 6, se puede aprecia la distribución.

Tabla 7.

Estructura de objetivos de gobierno y gestión COBIT 5.0:2019

1.Procesos	2.Estructuras organizativas
3.Flujos y elementos de información	4.Personas, habilidades y competencias
5.Políticas y procedimientos	6.Cultura, ética y comportamiento
7.Servicios, infraestructura y aplicaciones	

Fuente: (ISACA, Marco de Referencia COBIT5.0:2019, 2019)

Esta estructura mencionada, también es llamada catalizadores de COBIT 5, posee una agrupación de dimensiones comunes permitiendo a una entidad, lograr interactuar y manejar sus complejas interacciones y de esta manera, facilitar los resultados exitosos.

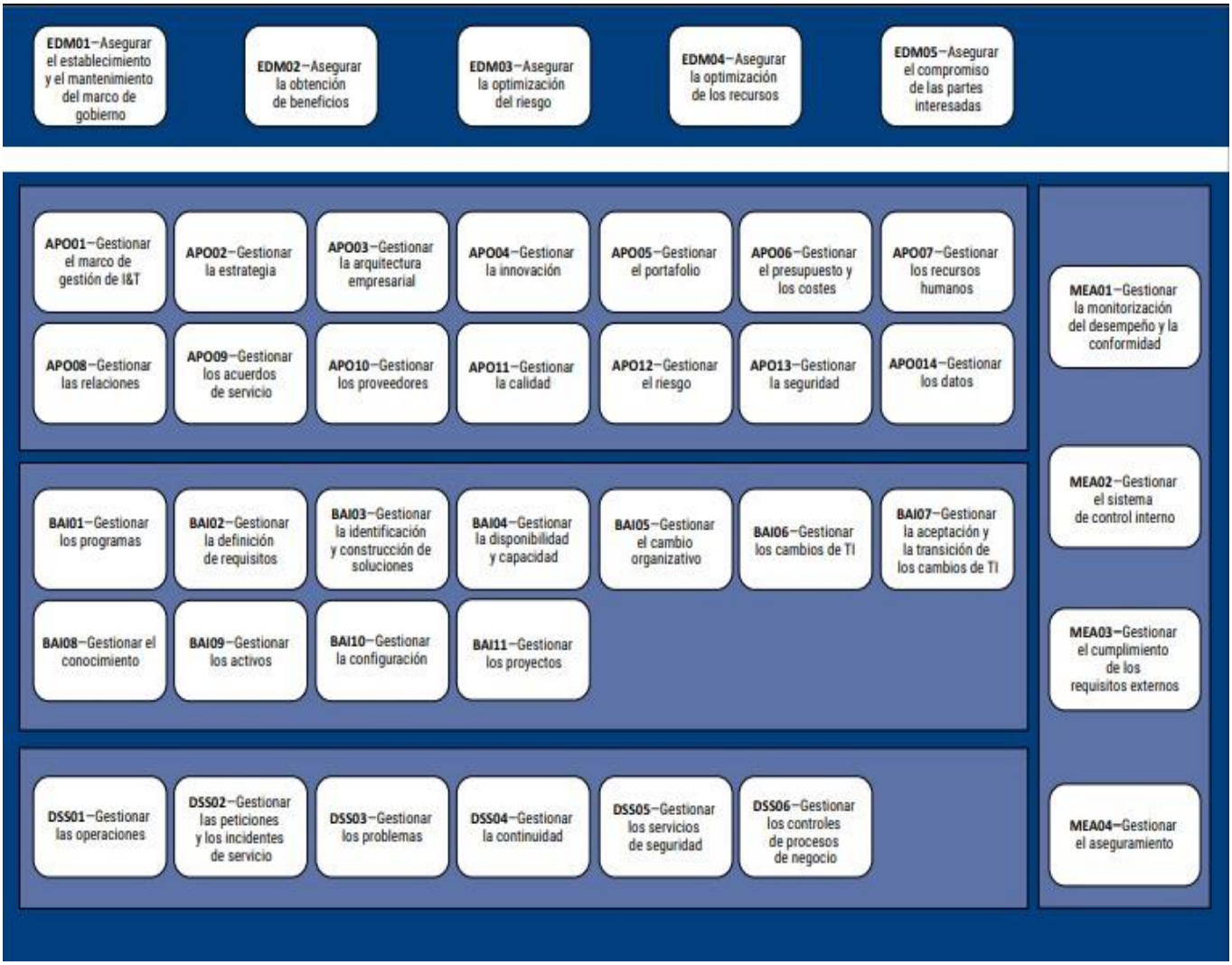
Los catalizadores poseen unas dimensiones comunes clasificadas en dos grandes elementos:

Grupos de interés : son las partes que están involucradas y poseen un interés especial en el catalizador

Metas : son los resultados esperados del catalizador

Figura 5.

Visión General del COBIT 5.0 – 2019



Fuente: Marco de referencia COBIT® 2019: objetivos de gobierno y gestión

El stándar COBIT 5.0 2019, incluye un total de 40 objetivos de gobierno y gestión, mediante los componentes. Cada objetivo de gobierno o gestión es la base del logro de metas de alineamiento que están relacionadas con metas empresariales más importantes. (ISACA, Framework-Governance-and-Management-Objectives, 2019)

4.2.Análisis de los procesos organizacionales en las empresas manufactureras de la ciudad de Barranquilla

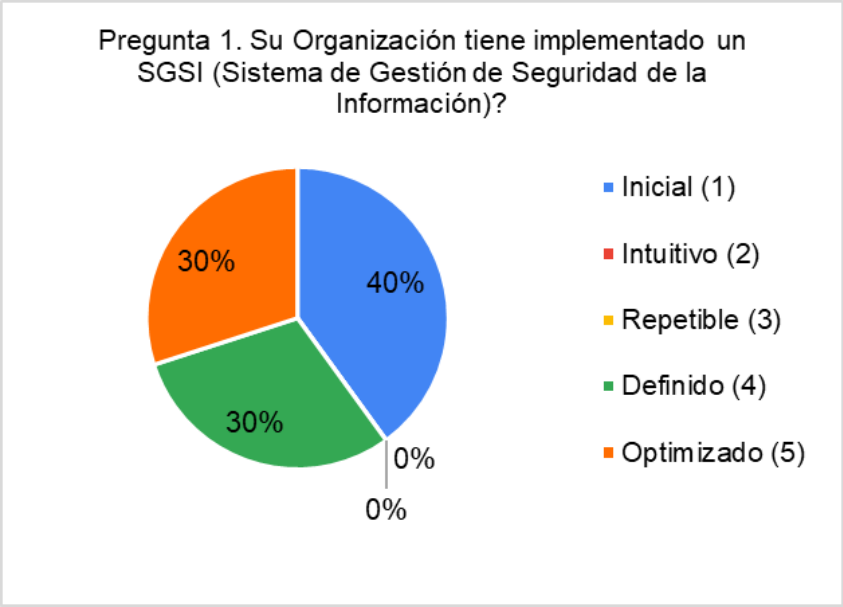
Un proceso es una secuencia de tareas que se realizan de forma concatenada, es decir de forma seguida una detrás de la otra para alcanzar un objetivo o un fin concreto. En una organización, la suma de muchos procesos tendrá como resultado la entrega de un producto o servicio al cliente. Los procesos de una empresa representan un know-how importantísimo dentro de la calidad del producto o servicio que entregan al mercado y por lo tanto del éxito y permanencia a lo largo de los años en el mercado. (https://iveconsultores.com/, 2020)

En este orden de ideas, la presente investigación diseñó un instrumento para recoger información teniendo como base, el análisis expuesto de los diferentes estándares de Seguridad de la Información. En ese sentido, se tomaron fundamentalmente la norma ISO 27001 y los procesos APO12, APO13 y APO14 del Estándar COBIT 5, después de analizar la aplicabilidad en el tema de estudio, que en este caso, son las empresas manufactureras del sector electrónico en la ciudad de Barranquilla.

El instrumento diseñado y revisado, fue aplicado a las personas que manejan los procesos de TI en las empresas del sector manufacturero de la ciudad de Barranquilla que se dedican a la producción de artículos eléctricos y electrónicos, establecida como muestra de la presente investigación (Ver Apéndice A). Cabe destacar que este modelo fue diseñado de manera digital y se tomó como referencia el establecido en la investigación Modelo de Seguridad de la Información para Instituciones de Educación Superior, de la autora Norly Alejandra Aguilar Quintero. A continuación, se dan a conocer los resultados más representativos obtenidos de esta investigación:

Figura 6.

Análisis de la Pregunta No.1:Su Organización tiene implementado un SGSI?



Concepto	Cant	%
Inicial (1)	4	40%
Intuitivo (2)	0	0%
Repetible (3)	0	0%
Definido (4)	3	30%
Optimizado (5)	3	30%
Total	**10**	**100%**

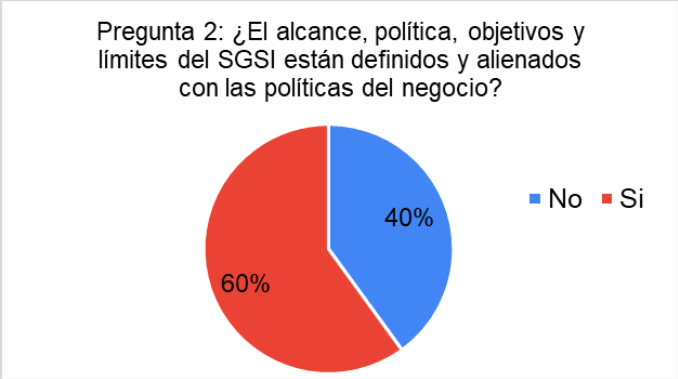
Fuente: Autora

En la Figura 6 se puede apreciar, los diferentes niveles de madurez de la muestra observada, donde el 40% de las empresas manufactureras dedicadas a la producción y comercialización de productos eléctricos y electrónicos de la ciudad de Barranquilla encuestadas, no tienen establecido el Sistema de Gestión de la Seguridad de la Información.

En ese mismo orden de ideas, el 30% de las empresas encuestadas lo tienen definido, por lo que es posible generar actividades de monitoreo y control en el cumplimiento de él, mientras que el otro, 30% respondió que tienen un Sistema de Gestión de Seguridad de la Información optimizado permitiendo generar acciones de mejoramiento continuo.

Figura 7.

Análisis de la Pregunta No.2: El alcance política, objetivos y límites del SGSI están definidos y alineados con las políticas del negocio?



Concepto	Cant	%
No	4	40%
Si	6	60%
Total	**10**	**100%**

Fuente: Autora

El 60% de las empresas encuestadas tienen tiene alineado el Alcance, las Políticas, los Objetivos y Límites del SGSI con las políticas del negocio, mientras que el 40% no lo tienen.

Figura 8.

Análisis de la Pregunta No.3: Se realizan revisiones a la política, objetivos, alcance, procedimientos, controles, valoración y tratamiento de riesgos del SGSI del negocio con el fin de garantizar que sigan siendo adecuados?

Concepto	Cant	%
Si	6	60%
No	4	40%
Total	**10**	**100%**

Fuente: Autora

El 60% de las empresas encuestadas realizan revisiones periódicas a los factores fundamentales como Alcance, Objetivos, Procedimiento, Controles, entre otros, del SGSI del

negocio con el fin de perfeccionarlos o sustituirlos por aquellos que brinden la respuesta adecuada y garanticen la efectividad de gestionar los riesgos en la seguridad de la información. El 40% no realizan revisiones, por lo que no permiten una mejora continua al proceso.

Figura 9.

Análisis de la Pregunta No.4: Los procedimientos de seguridad de la información brindan apoyo a los requisitos del negocio?

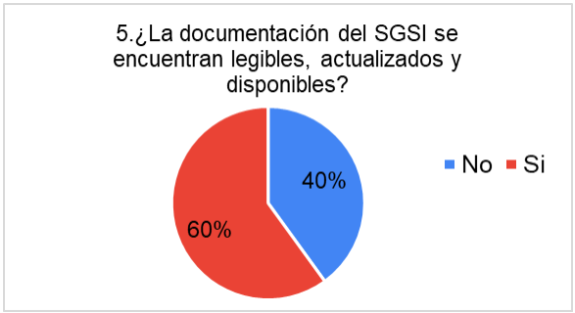
Concepto	Cant	%
Si	6	60%
No	4	40%
Total	**10**	**100%**

Fuente: Autora

En la Figura 9 se aprecia que el 60% de las empresas manufactureras encuestadas afirman que la actuación de Seguridad de la Información otorga una base a las necesidades del negocio y delinea los pasos que se deben seguir. El 40% de las empresas no realizan estas acciones.

Figura 10.

Análisis de la Pregunta No.5: La documentación del SGSI se encuentran legibles, actualizados y disponibles?



Concepto	Cant	%
Si	6	60%
No	4	40%
Total	**10**	**100%**

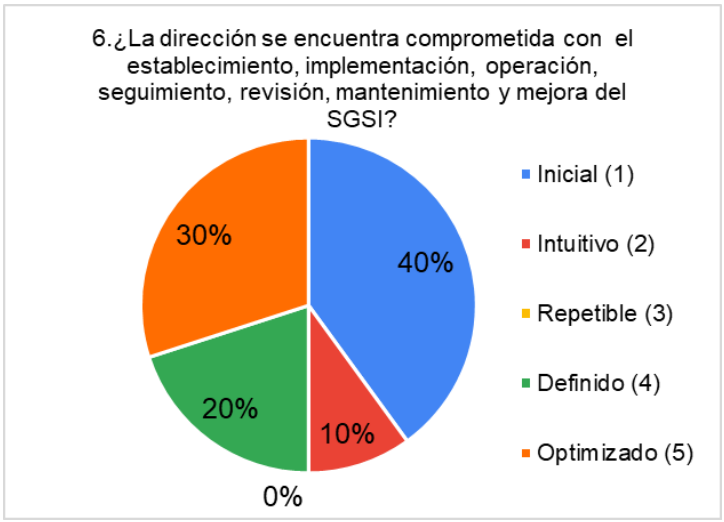
Fuente: Autora

En la Figura 10 se puede apreciar que el 60% de las empresas encuestadas afirman que la documentación del SGSI están legibles y actualizados, por lo que representa un capital

intelectual en el interior de la organización que ayuda a la estandarización de los procesos, a la planificación organizacional, al control de las actividades realizadas y al desarrollo de auditorías. En ese orden de ideas, el 40% de las organizaciones afirmaron que no cumplen este ítem.

Figura 11.

Análisis de la Pregunta No.6. ¿La dirección se encuentra comprometida con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI?



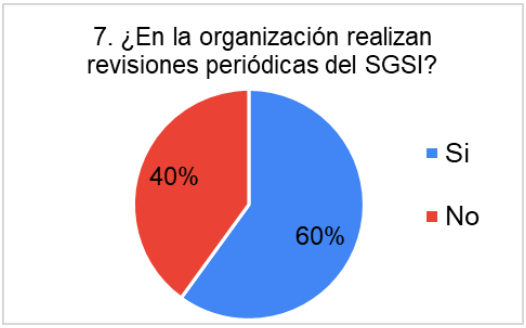
Concepto	Cant	%
Inicial (1)	4	
Intuitivo (2)		
Repetible (3)		
Definido (4)		
Optimi		
To		

Fuente: Autora

Se puede evidenciar en la Figura 11, que el 30% de las empresas encuestadas tienen un gran compromiso con las actividades pertinentes al mejoramiento continuo del SGSI, 20% aseguró que si bien reconocen la importancia del compromiso, existen algunas oportunidades de mejora, mientras que el 50% restante, consideran que el SGSI aporta gran valor a la organización pero que no se encuentra un compromiso real para establecerlo, implementarlo y, menos, para realizar acciones de seguimiento, revisión , mantenimiento y mejora.

Figura 12.

Análisis de la Pregunta No.7. ¿En la Organización realizan revisiones periódicas del SGSI?



Concepto	Cant	%
Si		
No		
Tot		

Fuente: Autora

El 60% de las empresas encuestadas afirmaron que realizan revisiones al SGSI permitiendo de esta forma, identificar si se están cumpliendo los requisitos, mientras que, el 40% no lleva revisiones planificadas del SGSI, considerando que es una gran oportunidad de mejora para el establecimiento de controles en el manejo de la seguridad de la información.

Figura 13.

Análisis de la Pregunta No.8. ¿Con qué frecuencia se realizan esas revisiones periódicas del SGSI?

Concepto	Cant	%
Cada 6 meses	3	30%
Cada año	2	20%
Cada dos años	0	0%
No Realizan	5	50%
Total	**10**	**100%**

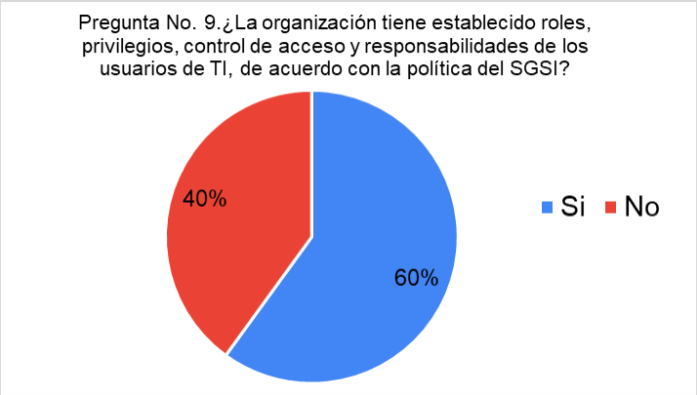
Fuente: Autora

El 30% de las empresas encuestadas afirmaron que realizan auditorías internas periódicas con una frecuencia de cada 6 meses permitiendo presentar informes a la alta gerencia sobre el rendimiento del Sistemas de Gestión de Seguridad de la Información (SGSI), mientras que el

20% afirmó que lo hace cada año. Se observó el mayor porcentaje, que corresponde al 50% no realizan las auditorías internas visualizando una gran oportunidad de mejora.

Figura 14.

Análisis de la Pregunta No. 9.¿La organización tiene establecido roles, privilegios, control de acceso y responsabilidades de los usuarios de TI, de acuerdo con la política del SGSI?



Concepto	Cant	%
Si	6	60%
No	4	40%
Total	**10**	**100%**

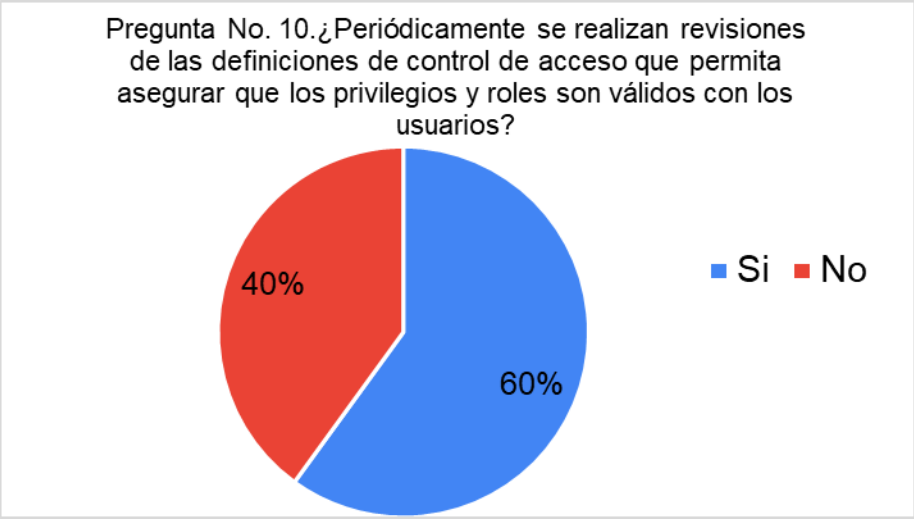
Fuente: Autora

El 40% de los encuestados, informaron que la organización tiene establecidos los roles, privilegios, control de acceso y responsabilidades de los usuarios de TI de acuerdo a las políticas del SGSI. Las organizaciones consideran que adjudicar y anular los privilegios de acceso a los sistemas es útil para mantener la integridad de la información considerándolo un elemento clave en la seguridad organizacional.

El 60% de los encuestados informaron que no tienen establecidos roles, privilegios, control de acceso y responsabilidad debido a que no se cuenta aún con la implementación de un SGSI o que aún se está trabajando en ello.

Figura 15.

Análisis de la Pregunta No. 10. ¿Periódicamente se realizan revisiones de las definiciones de control de acceso que permita asegurar que los privilegios y roles son válidos con los usuarios?



Concepto	Cant	%
Si		
No		
Tot		

Fuente: Autora

El 40% de los encuestados, informaron que la organización realiza revisiones de las definiciones de control de acceso que permite asegurar que los privilegios y roles son válidos con los usuarios. Estas revisiones tienen como objetivo identificar, analizar y comprobar el adecuado funcionamiento de los controles generales que son políticas y procedimientos que llegan a aplicarse a todos los sistemas de información, así como también a plataformas autorizadas.

El 60% de los encuestados informaron que no realizan revisiones de las definiciones de controles de acceso que permita asegurar que los privilegios y roles son válidos con los usuarios, ya sea porque no existe un SGSI o que está en construcción.

Figura 16.

Análisis de la Pregunta No. 11. ¿Se llevan a cabo auditorías internas planificadas al SGSI de la organización?

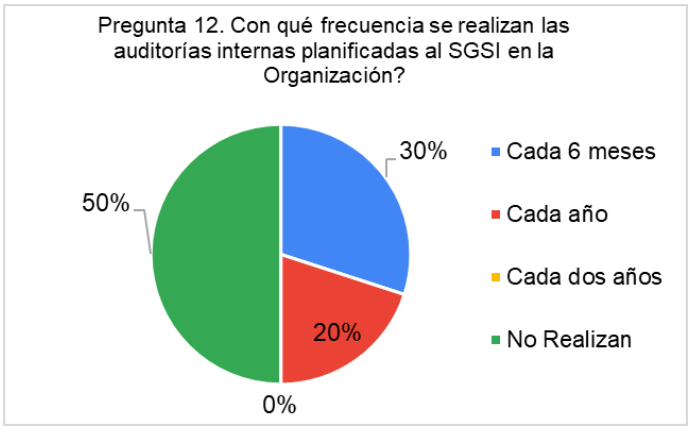
Concepto	Cant	%
Si	6	60%
No	4	40%
Total	**10**	**100%**

Fuente: Autora

El 40% de las empresas encuestadas respondieron que realizan auditorías internas planificadas al SGSI de la organización, mientras que el 60% no lo hacen. Estas auditorías se consideran unas herramientas de gran valor para el control del funcionamiento adecuado del SGSI.

Figura 17.

Análisis de la Pregunta No. 12. ¿Con qué frecuencia se realizan las auditorías internas planificadas al SGSI en la Organización?



Concepto	Cant	%
Cada 6 meses	3	30%
Cada año	2	20%
Cada dos años	0	0%
No Realizan	5	50%
Total	**10**	**100%**

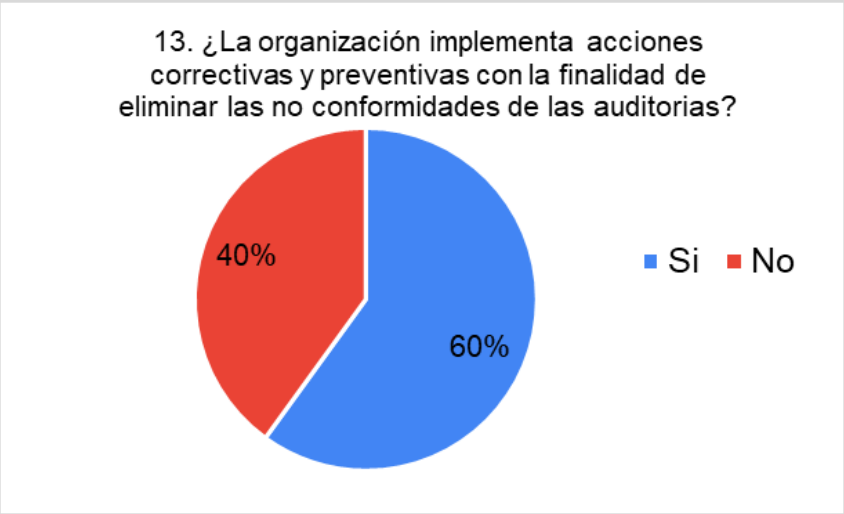
Fuente: Autora

El 30% de las empresas encuestadas afirmaron que realizan auditorías internas periódicas

planificadas al SGSI con una frecuencia de cada 6 meses permitiendo asegurar y consultar objetivamente acciones que agreguen valor y mejoramiento en las operaciones de las empresas, mientras que el 20% afirmó que lo hace cada año. Se observó un mayor porcentaje, que corresponde al 50% que no realizan las auditorías internas estableciendo una gran oportunidad de mejora.

Figura 18.

Análisis de la Pregunta No. 13. ¿La organización implementa acciones correctivas y preventivas con la finalidad de eliminar las no conformidades de las auditorias?



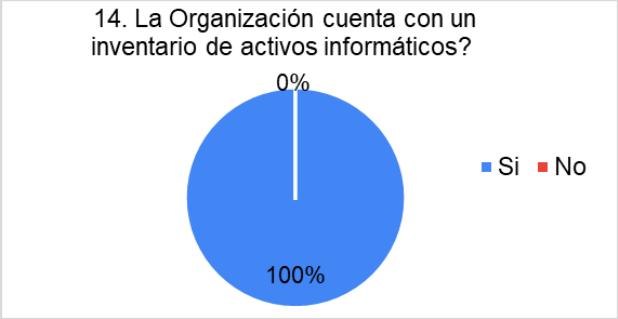
Concepto	Cant	%
Si	6	60%
No	4	40%
Total	**10**	**100%**

Fuente: Autora

El 60% de las empresas encuestadas afirmaron que implementan acciones correctivas y preventivas con la finalidad de eliminar las no conformidades de las auditorias, mientras que el 40% no las realizan debido a que no tienen formalizado un SGSI o están iniciando el proceso de su implementación. Eso demuestra que las empresas que lo implementan tienen un gran apoyo para cumplir sus objetivos, tienen un control de sus gestiones internos y ayuda a evaluar sus procesos de gestión con referencia al Sistema de Gestión de Seguridad de la Información.

Figura 19.

Análisis de la Pregunta No. 14. ¿La Organización cuenta con un inventario de activos informáticos?



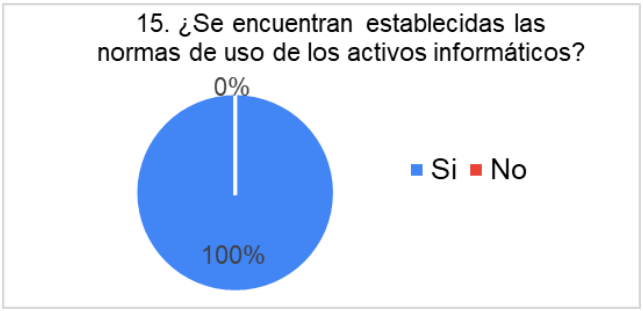
Concepto	Cant	%
Si	10	100%
No	0	0%
Total	**10**	**100%**

Fuente: Autora

El 100% de las organizaciones encuestados informaron que cuentan con un inventario de activos informáticos. Consideran que hacer este inventario, es la base para la gestión de los riesgos de seguridad de la información y así mismo, detectar los niveles de protección que se requieran en el interior de la organización.

Figura 20.

Análisis de la Pregunta No. 15. ¿Se encuentran establecidas las normas de uso de los activos informáticos?



Concepto	Cant	%
Si		
No		
Tot		

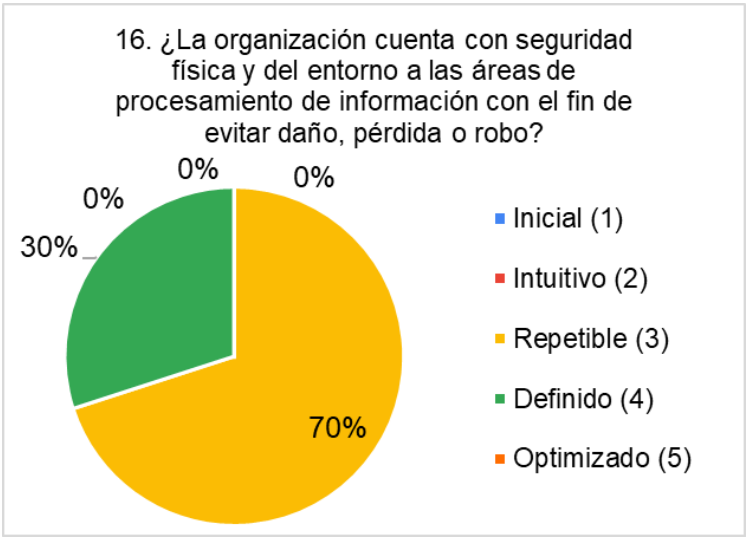
Fuente: Autora

El 100% de las organizaciones tienen establecidas las normas de uso de los activos

informáticos. Ellas consideran que las normas son políticas que se exponen en un documento y sirven como referencia para el uso correcto y brindar la protección adecuada a los activos

Figura 21.

Análisis de la Pregunta No. 16. ¿La organización cuenta con seguridad física y del entorno a las áreas de procesamiento de información con el fin de evitar daño, pérdida o robo?



Concepto	Cant	%
Inicial (1)	0	
Intuitivo (2)		
Repetible (3)		
Definido (4)		
Optimi		
To		

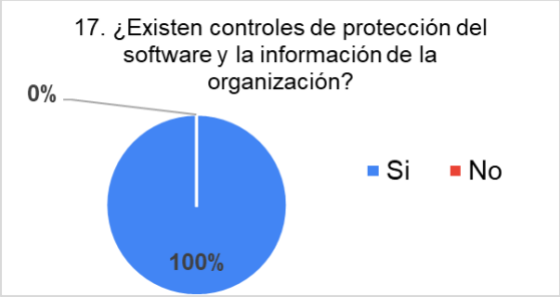
Fuente: Autora

El 70% de las empresas encuestadas, cuentan con una seguridad física repetible y un entorno adecuado en las áreas de procesamiento de la información y el 30% restante, estimó que se han realizado acciones que permite establecer que está definida esa seguridad física y el entorno adecuado para el procesamiento de la información con el fin de evitar pérdidas, robos o daños, pero aún hay acciones para convertirla en un sistema optimizado.

Importante resaltar que se evidenció que todas las empresas encuestadas, ya sean en niveles diferentes, conocen de la importancia que tiene la seguridad física y su entorno en el tema relacionado con la información, como núcleo fundamental en las operaciones de la empresa.

Figura 22.

Análisis de la Pregunta No. 17. ¿Existen controles de protección del software y la información de la organización?



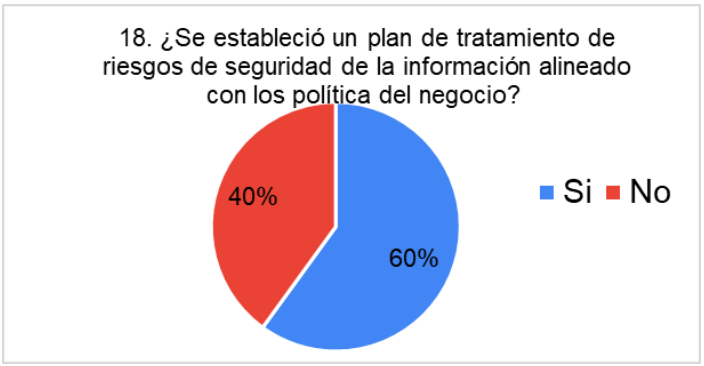
Concepto	Cant	%
Si	10	100%
No	0	0%
Total	**10**	**100%**

Fuente: Autora

Todas las empresas encuestadas informaron que poseen actualmente controles de protección del software y de la información de la organización, estableciendo el porcentaje del 100%. Estos controles los consideran fundamentales y necesarios para mantener a la información segura.

Figura 23.

Análisis de la Pregunta No. 18.¿Se estableció un plan de tratamiento de riesgos de seguridad de la información alineado con las políticas del negocio?



Concepto	Cant	%
Si		
No		
Tot		

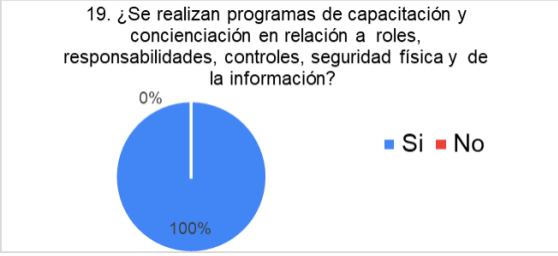
Fuente: Autora

El 60% de las empresas encuestadas informaron que tienen establecido un plan de tratamiento de riesgo de seguridad de la información, y que éste plan, está alineado con las

políticas del negocio, mientras que el 40% restantes de las empresas encuestadas, informaron que no tienen un plan de tratamiento de riesgo de seguridad de la información o que si lo tienen pero que no está alineado con las políticas del negocio por lo que se pudo evidenciar una gran oportunidad de mejora en este punto.

Figura 24.

Análisis de la Pregunta No. 19. ¿Se realizan programas de capacitaciones y concienciación en relación a roles, responsabilidades, controles, seguridad física y de la información?



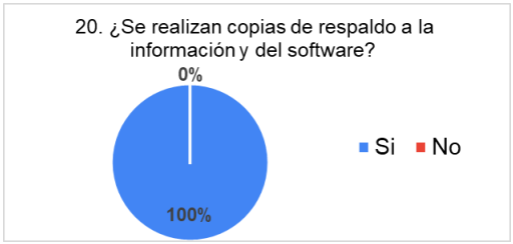
Concepto	Cant	%
Si	10	100%
No	0	0%
Total	**10**	**100%**

Fuente: Autora

El 100% de las empresas encuestadas informaron que realizan programas de capacitaciones y concientización en relación con roles, responsabilidades, controles, seguridad física y de la información. Este tipo de actividades ayuda a minimizar riesgos y a permitir un control sobre las acciones en el contexto de la seguridad de la información.

Figura 25.

Análisis de la Pregunta No. 20. ¿Se realizan copias de respaldo de la información y del software?



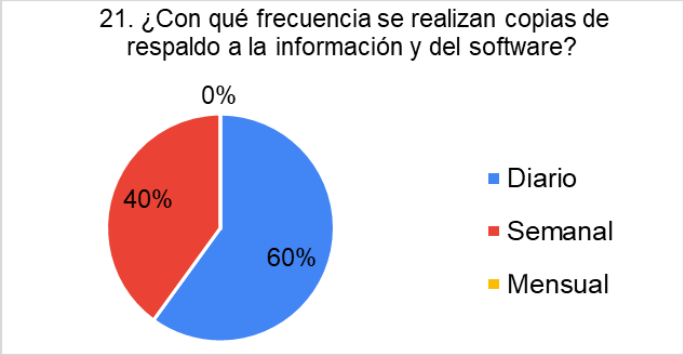
Concepto	Cant	%
Si	10	100%
No	0	0%
Total	**10**	**100%**

Fuente: Autora

El 100% de las empresas encuestadas realizan copias de respaldo de la información. Esto genera confiabilidad y disminución del riesgo en pérdida de información.

Figura 26.

Análisis de la Pregunta No. 21. ¿Con qué frecuencia se hacen las copias de respaldo de la información y del software?



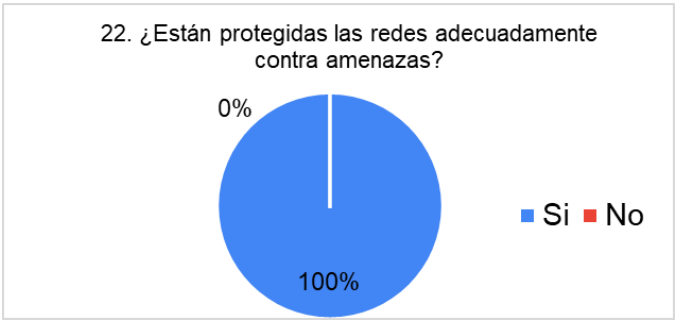
Concepto	Cant	%
Diario	6	60%
Semanal	4	40%
Mensual	0	0%
Total	**10**	**100%**

Fuente: Autora

El 60% de las empresas encuestadas comentaron que diariamente se hace copias de respaldo a la información y al software, mientras que el 40% lo hace semanal. Las copias de seguridad de la información se consideran un kit esencial de seguridad de cualquier empresa, constituyéndose de vital importancia para cuando se necesiten en eventos de infortunio.

Figura 27.

Análisis de la Pregunta No. 22. ¿Están protegidas las redes adecuadamente contra amenazas?



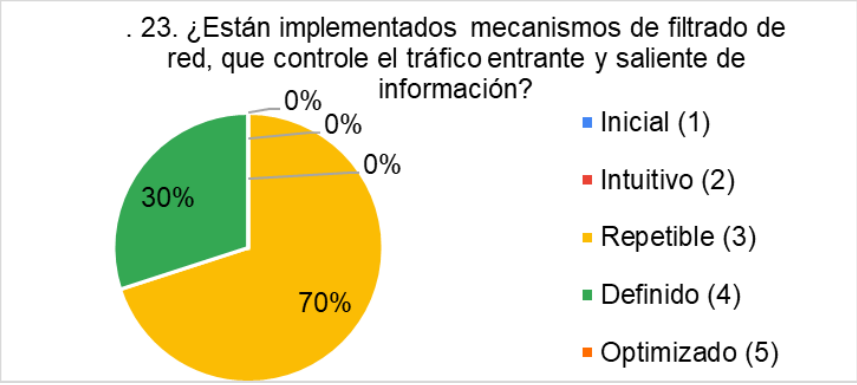
Concepto	Cant	%
Si	10	100%
No	0	0%
Total	**10**	**100%**

Fuente: Autora

El 100% de los encuestados informaron que están protegidas las redes de forma que controlan las amenazas existentes. Se verificó que para las empresas tener seguridad en la red ayuda a prevenir el uso desautorizado y no sufrir invasión a su privacidad teniendo en cuenta los peligros que puedan llegar a tener los usuarios.

Figura 28.

Análisis de la Pregunta No. 23. ¿Están implementados mecanismos de filtrado de red, que controle el tráfico entrante y saliente de información?



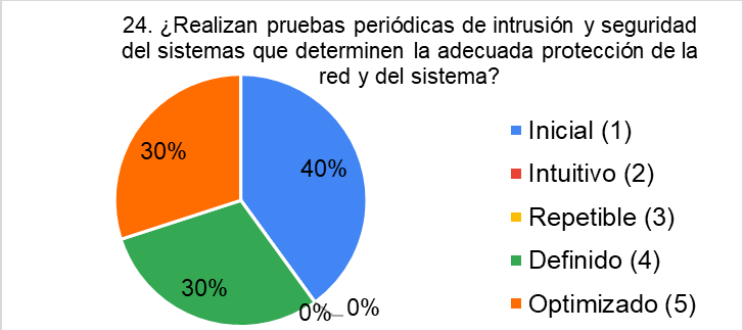
Concepto	Cant	%
Inicial (1)	0	0%
Intuitivo (2)	0	0%
Repetible (3)	7	70%
Definido (4)	3	30%
Optimizado (5)	0	0%
Total	**10**	**100%**

Fuente: Autora

El 70% de las empresas encuestadas establecieron que de forma repetible se están implementando mecanismos de filtrado de red que permite controlar el tráfico entrante y saliente de información, mientras que el 30% informó que tiene definido estos mecanismos y que ello permite mantener un control de salida ilegal de información sensible desde lo que se le llama fuente interna, siendo de mucha ayuda en el interior de las organizaciones.

Figura 29.

Análisis de la Pregunta No. 24. ¿Realizan pruebas periódicas de intrusión y seguridad del sistema que determinen la adecuada protección de la red y del sistema?



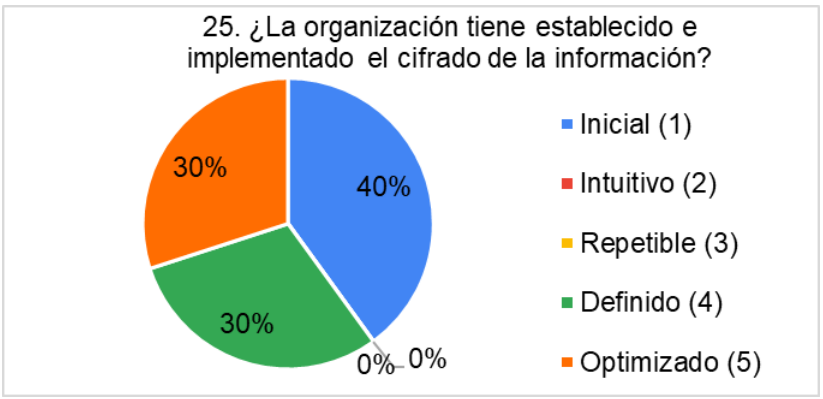
Concepto	Cant	%
Inicial (1)	4	40%
Intuitivo (2)	0	0%
Repetible (3)	0	0%
Definido (4)	3	30%
Optimizado (5)	3	30%
Total	**10**	**100%**

Fuente: Autora

El 40% de las empresas encuestadas respondieron que están iniciando a realizar pruebas de intrusión y seguridad del sistema, el 30% de las empresas ya tienen definidas esas pruebas periódicas de intrusión y seguridad del sistema que determinan la adecuación protección de la red y del sistema y el 30% ya tienen optimizado los tipos de pruebas garantizando un control para protección de la red y del sistema.

Figura 30.

Análisis de la Pregunta No. 25. ¿La organización tiene establecido e implementado el cifrado de la información?



Concepto	Cant	%
Inicial (1)	4	
Intuitivo (2)		
Repetible (3)		
Definido (4)		
Optimi		
To		

Fuente: Autora

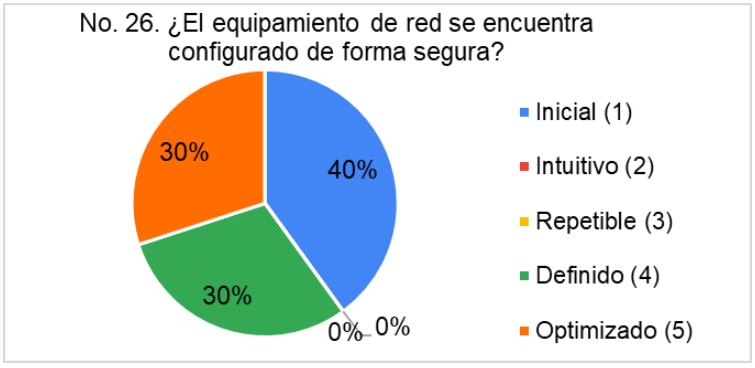
El 40% de las empresas del sector manufacturero encuestadas comentaron que tienen

optimizado el cifrado de la información logrando proteger la información privada contra amenazas y ofreciendo un medio que demuestra la autenticidad verificando el origen de un mensaje.

El 30% de ellas, lo tienen definido y el 30% no lo tienen o lo están iniciando a implementar y reconocen que el cifrado de datos evita tipos de ataques como robo de identidad o fraudes bancarios. Algunas empresas reconocen que este es un mecanismo de protección valioso para el tema de información sensible.

Figura 31.

Análisis de la Pregunta No. 26. ¿El equipamiento de red se encuentra configurado de forma segura?



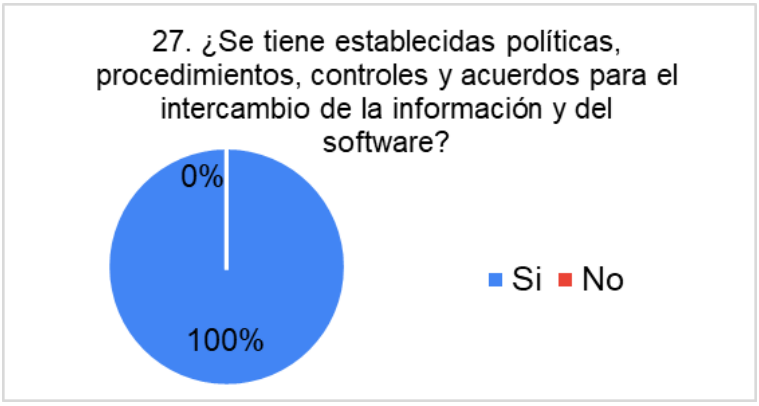
Concepto	Cant	%
Inicial (1)	4	
Intuitivo (2)		
Repetible (3)		
Definido (4)		
Optimi		
To		

Fuente: Autora

El 40% de las empresas del sector manufacturero encuestadas comentaron que tienen configurado de forma segura el equipamiento de red ofreciendo muchas ventajas de seguridad en la red. El 30% de ellas, lo tienen definido y el 30% no lo tienen o lo están iniciando a diseñar su configuración segura de la red.

Figura 32.

Análisis de la Pregunta No. 27. ¿Se tiene establecidas políticas, procedimientos, controles y acuerdos para el intercambio de la información y del software?



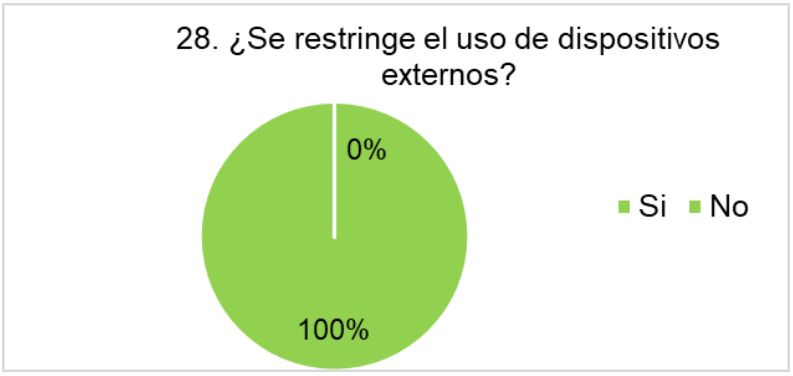
Concepto	Cant
Si	
No	
Tot	

Fuente: Autora

El 100% de las empresas manufactureras encuestadas respondieron que tienen políticas, procedimientos, controles y acuerdos para el intercambio de la información y del software.

Figura 33.

Análisis de la Pregunta No. 28. ¿Se restringe el uso de dispositivos externos?



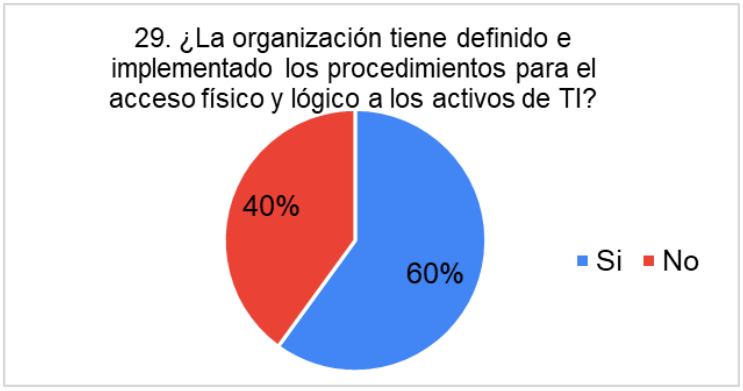
Concepto	Cant
Si	
No	
Tot	

Fuente: Autora

El 100% de las empresas manufactureras encuestadas no restringe el uso de dispositivos externos que permita proteger la información.

Figura 34.

Análisis de la Pregunta No. 29. ¿La organización tiene definido e implementado los procedimientos para el acceso físico y lógico a los activos de TI?



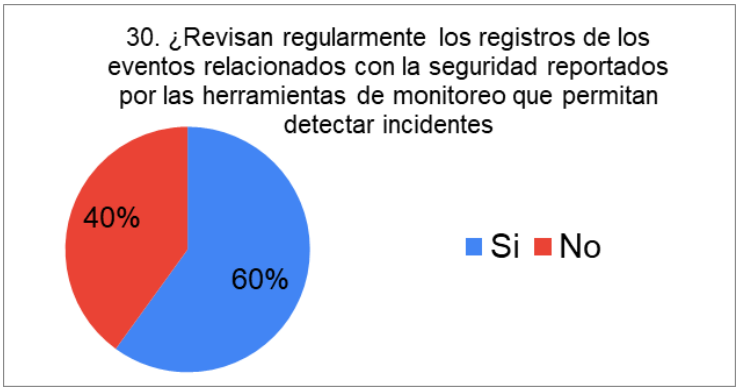
Concepto	Cant
Si	
No	
Tot	

Fuente: Autora

El 60% de las empresas manufactureras encuestadas tienen controles que evitan el acceso a usuarios no autorizados al uso de los activos de Tecnologías de la Información. El 33% de las empresas encuestadas, no tiene implementados controles que permitan el acceso a los activos de tecnologías de Información solo usuarios autorizados.

Figura 35.

Análisis de la Pregunta No. 30. ¿Revisan regularmente los registros de los eventos relacionados con la seguridad reportados por las herramientas de monitoreo que permitan detectar incidentes potenciales?



Concepto	Cant	%
Si	6	60%
No	4	40%
Total	**10**	**100%**

Fuente: Autora

El 60% de las empresas manufactureras encuestadas informaron que revisan de forma regular, los registros de los eventos relacionados con la seguridad reportados por las herramientas de monitoreo que permitan detectar incidentes, mientras que el 40% no lo hacen de forma regular.

Figura 36.

Análisis de la Pregunta No. 31. ¿Se gestionan los documentos sensibles y dispositivos de salida?

Concepto	Cant
Si	
No	
Tot	

Fuente: Autora

El 60% de las empresas manufactureras encuestadas informaron que gestionan los documentos sensibles y dispositivos de salida, mientras que el 40% no lo hacen.

De acuerdo con los resultados nombrados en este capítulo, que fueron obtenidos en las encuestas aplicadas a cada uno de los líderes del área de Tecnologías de Información de cada empresa manufacturera seleccionada, se pudieron identificar algunas fortalezas y debilidades en cada uno de los procesos que adelantan. A continuación, se dan explicaciones de ellas:

Tabla 8.

Fortalezas y Debilidades identificadas

Fortaleza	Dominio/Requisito	Metas de TI
Las empresas manufactureras tienen definidos e implementados los procedimientos y mecanismo de seguridad para restringir el acceso físico y lógico a los activos de TI.	DSS05.05 Gestionar la identidad del usuario y el acceso lógico.	Seguridad de la información, infraestructura de procesamiento y aplicaciones
Las empresas manufactureras tienen identificados todos sus activos informáticos. Mantienen el inventario de esos activos y cuentan con normas básicas para el uso de la información y uso de las instalaciones para procesamiento de la información	A.8. Gestión de activos A.8.1 Responsabilidad por los activos BAI09 Gestionar los Activos	Optimización de activos, recursos y capacidades de TI
Las empresas manufactureras tienen asegurado el acceso actualizado de todos sus usuarios.	DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Seguridad de la información, infraestructura de procesamiento y aplicaciones
Las empresas manufactureras toman medidas frente a las no conformidades presentadas con la finalidad de controlarlo y corregirlo determinado las causas que lo ocasionan	ISO 27001/ Requisitos sección 10	
Las empresas manufactureras usan medidas de seguridad permitiéndole proteger sus redes de comunicación contra amenazas	DSS05.02 Gestionar la seguridad de la red y las conexiones. A13.2 Transferencia de información	Seguridad de la información, infraestructura de procesamiento y aplicaciones
Las empresas manufactureras cuentan con políticas, procedimientos y controles de transferencia información formales para proteger la información	A13.2 Transferencia de información	

Fuente: autora

Fortaleza	Dominio/Requisito	Metas de TI
Las empresas manufactureras realizan copias de respaldo de la información, programas, aplicaciones con el fin de ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo institucional.	A12.3 Copias de respaldo DSS04.07 Gestionar acuerdos de respaldo	Seguridad de la información, infraestructura de procesamiento y aplicaciones
Las empresas manufactureras se han preocupado por el establecimiento del SGSI en un alto porcentaje, sin embargo, se notan oportunidades de mejora en él. Las revisiones periódicas de las políticas, objetivos, alcance, procedimientos, controles, valoración y tratamiento de riegos del SGSI del negocio con el fin de garantizar que sigan siendo adecuados.	ISO 27001/ Requisitos sección 4.4 APO13.01 Establecer y mantener un SGSI.	Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas
Las empresas manufactureras tienen establecido privilegios, control de acceso adecuado, roles y responsabilidades de los usuarios de TI. También tienen un plan de tratamiento de riesgos de seguridad de acuerdo con la política del SGSI	APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información. APO13.03 Supervisar y revisar el SGSI. ISO 27001/ Requisitos sección 4.2.3	Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas
Las empresas manufactureras cuentan la documentación del SGSI estando legible, actualizada, disponible; además los procedimientos brindan apoyo con los requisitos del negocio.	ISO 27001/ Requisitos sección 5.2.1	
Las empresas manufactureras realizan con muy poca frecuencia el desarrollo de programas de capacitación. No existe una real concienciación en relación a roles, controles, seguridad física y de la información.	APO13.02	Seguridad en infraestructura de procesamiento, softwares y seguridad de la información corporativa
Las empresas manufactureras no desarrollan auditorías internas a intervalos planificados y su frecuencia no es adecuada.	APO13.03 Supervisar y revisar el SGSI. 9.2 Auditoría interna	Soporte de Tecnologías de la Información y cumplimiento de

Fuente: Autora

4.2. Estructuración de los elementos que conformaría el modelo de seguridad de la información para las empresas manufactureras

Para la construcción de un modelo de seguridad de la información dirigido a empresas manufactureras, se reconocen como principal elemento, las partes interesadas o stakeholders que pueden ser empresas o personas y que afectan o pueden ser afectados a partir de las actividades que desarrolla la empresa. A partir de allí, se identifican los procesos misionales de este tipo de empresas, que corresponde a las funciones sustantivas de la entidad como productora de bienes como eje central de su cadena de valor.

En el presente proyecto, las actividades fueron enfocadas en los procesos APO12-Gestionar el riesgo, APO13-Gestionar la seguridad y APO14-Gestionar los Datos. Se establece ello, debido a que estos procesos están vinculados directamente con la seguridad de la información cuya finalidad fundamental está orientada hacia el manejo de la información y a la regulación de todos los activos informáticos, razón por la cual, logra establecer la definición, la operación y el monitoreo de un Sistema de Gestión de la Seguridad de la Información. Seguidamente se hace una exposición de cada uno ellos sirviendo de insumo para la presente investigación.

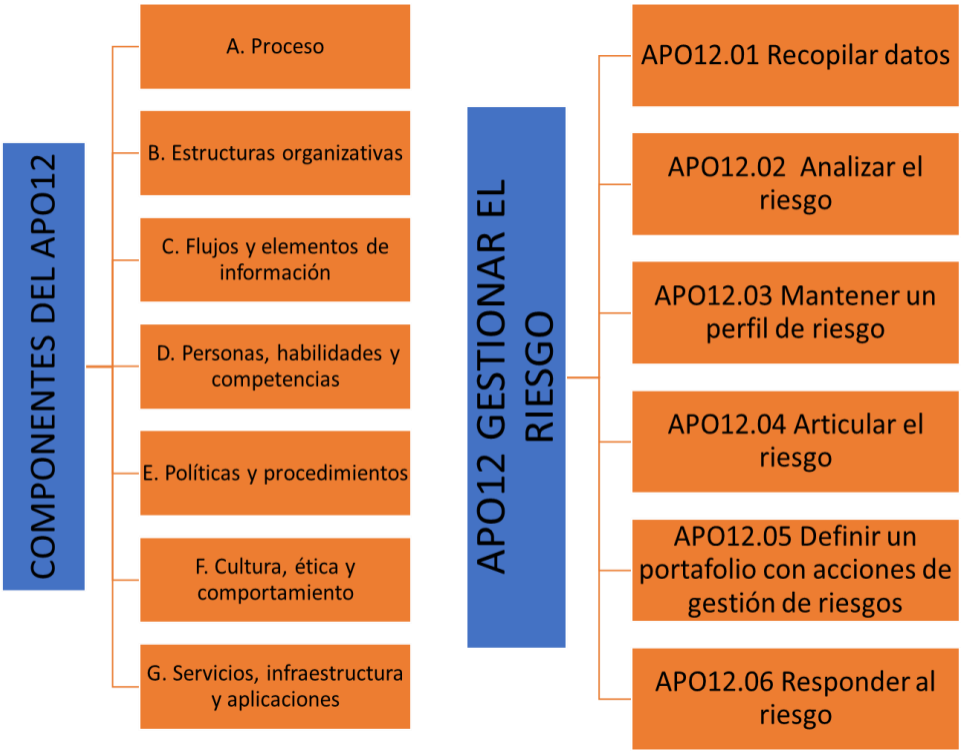
APO12. Gestionar el Riesgo

Este objetivo de gestión hace parte del dominio Alinear, Planificar y Organizar. Hace referencia a identificar, evaluar y reducir continuamente los riesgos relacionados con TI incluídos en los niveles de permisividad establecidos por la gerencia de la Institución.

Su intención está enfocado en juntar la gestión del riesgo empresarial relacionado con TI y el riesgo empresarial global, equilibrando costos y beneficios considerados fundamentales en cualquier organización.

Figura 37.

Clasificación de componentes APO12 Gestionar el riesgo.



Fuente: Cobit 5.0:2019

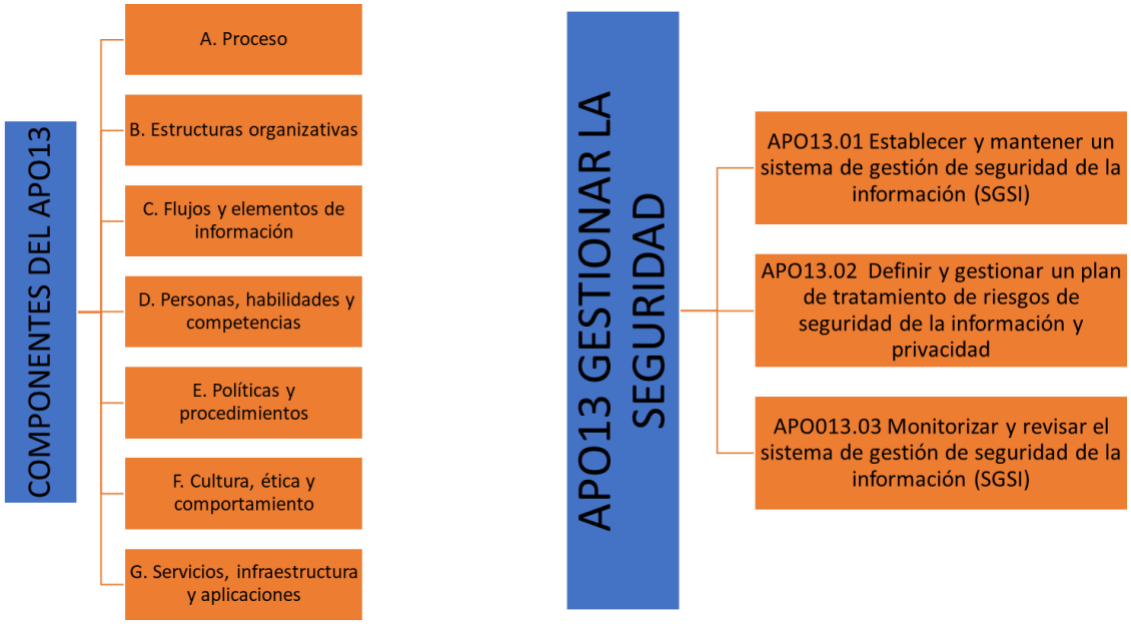
APO13. Gestionar la Seguridad.

El Proceso Gestionar la Seguridad hace parte del dominio: Alinear, Planificar y Organizar dentro del área de Gestión. Su principal característica se enfoca en definir, operar y supervisar un sistema para la gestión de la seguridad de la información. Su principal propósito es

mantener el impacto y la ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de normales de riesgo de la empresa. A continuación, se especifica más detalladamente este proceso:

Figura 38.

Clasificación de componentes APO13 Gestionar la Seguridad.



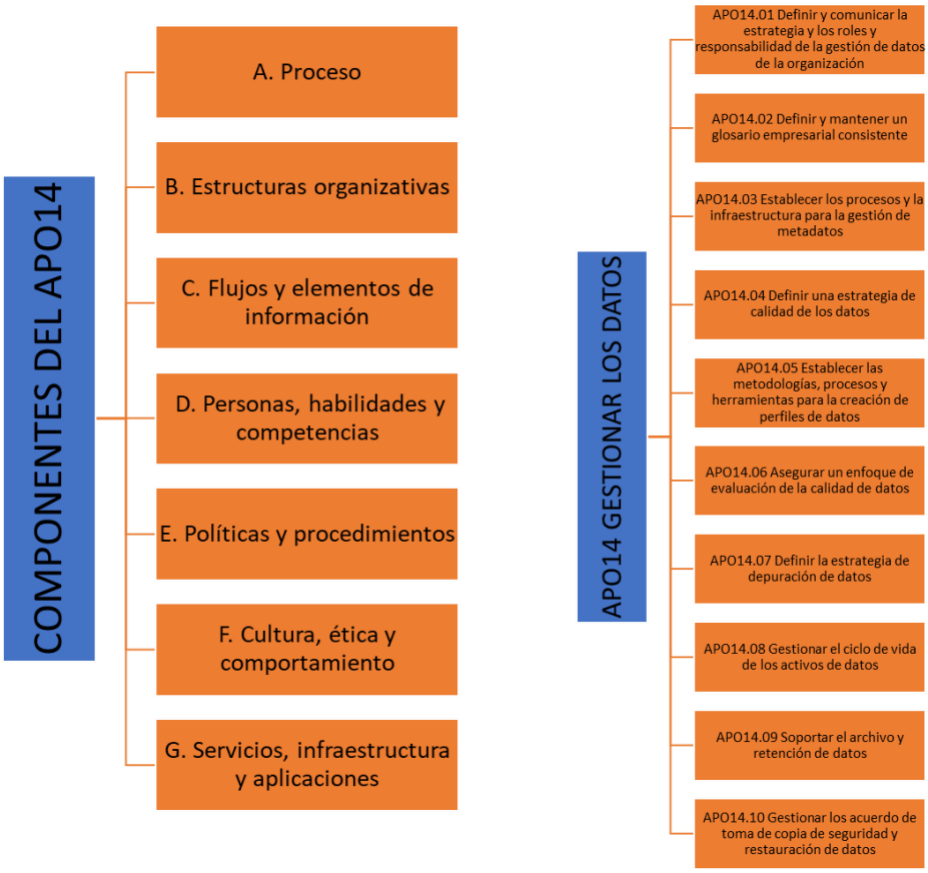
Fuente: Cobit 5.0:2019

APO14-Gestionar los Datos

Este proceso brinda la oportunidad de asegurar de forma eficaz, los activos de datos considerados precisos, para lograr metas y objetivos empresariales.

Figura 39.

Clasificación de componentes APO14 Gestionar los datos.



Fuente: Cobit 5.0:2019

4.2.1. Diseño del modelo de seguridad de la información para empresas manufactureras

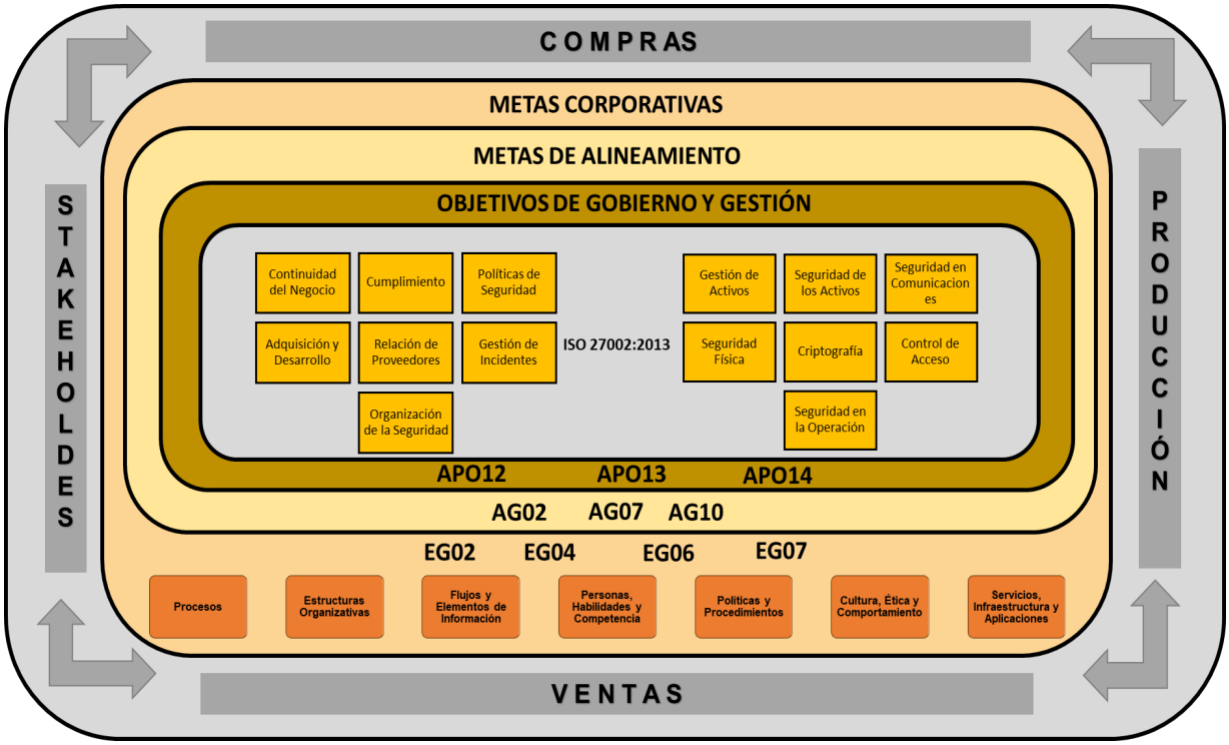
Un modelo de seguridad de la información es aquel esquema que permite especificar detalladamente las políticas de seguridad aplicables promoviendo de forma consistente, mecanismos para la identificación, definición e implementación de controles. Es por ello por lo que sus componentes deberán dirigirse a la identificación de riesgos y todas sus acciones deberán implementarse para poder reducirlos.

En el presente proyecto, el alcance de este modelo aplica para todos los procesos involucrando a todos los funcionarios que hacen parte de la organización independientemente del tipo de contratación, así como a los proveedores de los diferentes bienes y/o servicios; que de cualquier manera, compartan, utilicen o intercambien información independientemente de la ubicación que se encuentren.

A continuación, se presentan el modelo de seguridad de la información para empresas manufactureras

Figura 40.

Modelo de seguridad de la información para empresas manufactureras.



Fuente: Autora

El modelo inicia con las partes interesadas, los Stakeholders, quienes son todos esos actores que se encuentran involucrados con la gestión de proyectos. En este sentido, son ellos los que los financian, así como también, establecen los recursos, los gestionan y hacen los análisis pertinentes necesarios para el desarrollo cabal de las acciones que determinen el fin de los problemas observados.

La gestión de las partes interesadas (Stakeholders) es un aspecto fundamental a la hora de gestionar un proyecto ya sea de inversión o de investigación. Freeman (1984) plantea que los Stakeholders son "…Cualquier individuo o grupo que puede afectar el logro o ser afectado por el logro de los objetivos de una organización…". Por ello, los Stakeholders no deben ser desconocidos en el desarrollo de proyectos. (Valencia, 2017)

Las empresas manufactureras tienen estrategias bien definidas que permite un planteamiento estructurado a largo plazo de un sistema de producción. Estos procesos llamados misionales, también se contemplan en el marco de este modelo. Ellos están relacionados con la generación de valor direccionado para el cliente, en este caso, son Compras, Producción y Ventas quienes proporcionarán el resultado previsto por la empresa debido a que cumplirá su razón de ser.

Los procesos misionales son entendidos como aquellos procesos que "transforman las entradas y consumen los recursos" (Ortiz, 2013), por lo cual se debe entender que estos procesos están implicados complemente con la prestación de un servicio y que las empresas requieren crear valor a través de ellos para poder entregar a sus clientes. De allí, es que este

modelo los contempla como parte fundamental debido a la serie de información se maneja en ellos.

Seguidamente, se observan las Metas Corporativas que se consideran como los objetivos planteados de una forma estratégica y permite describir los resultados que se esperan obtener con base a una guía de esfuerzos que realizan todos los empleados participantes. Es decir, la organización tiene un conjunto de personas, de ideas y un capital que lo utiliza para alcanza el objetivo.

Las Metas Corporativas planteadas en el este modelo son: EG02 Gestión de Riesgo del Negocio, EG04 Calidad de la Información Financiera, EG06 Continuidad y Disponibilidad del Servicio del Negocio y EG07 Calidad de la Información sobre Gestión.

Los 7 componentes interactúan entre sí, formando un sistema de gobierno Integral. Estos elementos son como un núcleo que aplican para cada situación : Procesos, Estructuras organizativas, Flujo y elementos de información, Personas habilidades y competencias, Políticas y procedimientos, Cultura ética y comportamiento y por último, Servicios infraestructura y aplicaciones.

Las metas corporativas involucran a las metas de alineamiento AG02, AG07 y AG10 quienes contribuyen para el logro de los objetivos de la organización. En el interior del modelo se encuentran se localizan los objetivos de gobierno y gestión APO12 Gestionar el riesgo, APO13 Gestionar la seguridad y APO14 Gestionar los datos.

En el interior del modelo se encuentran los 14 dominios de la ISO/IEC 27002:2013 como eje central para la seguridad de la información: continuidad del negocio, cumplimiento, políticas de seguridad, adquisición y desarrollo, relación de proveedores, gestión de incidentes, organización de la seguridad, gestión de activos, seguridad de los activos, seguridad en comunicaciones, seguridad física, criptografía, control de acceso y seguridad de la operación.

4.2.2. Descripción del Modelo de Gobierno TI planteado.

El modelo se inicia con los stakeholders, que involucra a todas las partes interesadas logrando ayudar a mejorar los procesos, a obtener más apoyo de la sociedad, a encontrar nuevas ideas de negocio, a tener una mejor comprensión del entorno y, en última instancia, una mayor efectividad. (PMK Digital, 2020)

Todos los stakeholders deben ser considerados por la empresa, porque los clientes no comprarán productos que no respondan a sus deseos, necesidades o exigencias de precio, calidad, servicio y rapidez; los accionistas no seguirán invirtiendo en la empresa que no satisfaga sus demandas con respecto a los dividendos o ganancias de capital; la sociedad no tolerará empresas que no cumplan sus obligaciones legales y sus expectativas referentes a la calidad de vida; los profesionales no desarrollarán sus actividades y conocimientos, ni harán el esfuerzo requerido para diseñar y gestionar los diferentes procesos de la organización, a menos que ésta dé respuesta a sus deseos y exigencias relativas a la satisfacción en el trabajo; por último, los proveedores no continuarán suministrando sus conocimientos, habilidades y recursos a la empresa que no les facilite la oportunidad de obtener un beneficio razonable. (Lorca Fernández, 2004)

Teniendo en cuenta que el modelo contempla los procesos misionales que tienen las empresas manufactureras debido a ser claves en su ejercicio; se incluyen: compras, producción y ventas. La función de compras es adquirir adecuadamente la materia prima, suministros, equipos y servicios para que el proceso de producción desarrolle satisfactoriamente las operaciones. De igual modo, el proceso de ventas permite que la empresa manufacturera obtenga ingresos. De su desarrollo y gestión es que se genera la rentabilidad de la empresa.

Una empresa manufacturera es aquella que transforma una materia prima en bienes de consumo que posteriormente comercializa ya sea en forma directa o indirecta ya sea a través de distribuidores u agentes concesionarios preestablecidos. En Colombia, este tipo de empresas está caracterizada por pertenecer al sector secundario de la economía y debido a esa transformación, son estos los procesos misionales considerados en el modelo de Gobierno TI como ejes fundamentales que se alinean con los stakeholders.

La estructura usada para detallar las metas corporativas entrega información reelevante con cada uno de los componentes de gobierno que son factores que apoyan al buen funcionamiento del sistema de gobierno de la empresa. Estos componentes logran interactuar y son de diversos tipos.

El componente procesos es el más común porque describe una serie de métodos y acciones con orden que permiten obtener objetivos determinados y producir salidas contribuyendo a la consecución de todos los objetivos que están relacionados con las TI. El componente Estructuras Organizativas son elementos claves para la toma de decisiones en una

empresa. Quien convierte el comportamiento deseado en una aplicación práctica para la gestión diaria es el componente denominado Principios, Políticas y Marcos de Referencia.

El componente información tiene que ver con el núcleo principal o eje cental en cualquier organización, es la unidad que que es producida y utilizada. COBIT se fundamenta en la información necesaria para el funcionamiento competente y valioso del sistema de gobierno de la empresa. El componente que es subestimado como un factor de éxito en todas las actividades de gobierno y gestión es Cultura, Ética y Comportamiento, que hace relación a los individuos que actúan en una organización.

El componente Personas, Habilidades y Competencias, hacen parte de las necesidades para la toma decisiones adecuadas, ellevar a cabo medidas correctivas y completar cabalmente todas las actividades. Por último, los Servicios, Infraestructura y Aplicaciones, involucra esos mismos elementos para brindar a la empresa un sistema de gobierno para el procesamiento de I & T.

Las metas empresariales involucradas en el Modelo de Gobierno de TI corresponden a: EG02 -Gestión del riesgo; EG04-Calidad de la información financiera; EG06 – Continuidad y disponibilidad del servicio del negocio y EG07 Calidad de la Información sobre Gestión

EG02, corresponde a la gestión del riesgo, cuyas métricas contempladas en la Figura 41, involucran:

a. Porcentaje de objetivos y servicios críticos del negocio, cubiertos por la evaluación de riesgos

b. Proporción de percances con reelevancia que no se identificaron en la evaluación de riesgos frente al total de incidentes

c. Frecuencia de actualización del perfil del riesgo.

Igualmente se pueden observar las actividades a realizar con el nivel de capacidad para poder identificar, evaluar y reducir continuamente los riesgos que tienen relación con I&T. El mayor objetivo para una organización que trabaja con su información, es salvaguardar la seguridad de la información gestionando el riesgo.

Figura 41.

EG02: Meta empresarial: Gestión de riesgo de negocio en AP012 gestionar el riesgo

Dominio: Alinear, Planificar y Organizar Objetivo de gestión: AP012—Gestionar el riesgo		Área prioritaria: Modelo Core de COBIT
Descripción		
Identificar, evaluar y reducir continuamente los riesgos relacionados con I&T dentro de los niveles de tolerancia establecidos por la gerencia ejecutiva de la empresa.		
Propósito		
Integrar la gestión del riesgo empresarial relacionado con la I&T con la gestión del riesgo empresarial global (ERM), y equilibrar los costes y beneficios de la gestión del riesgo empresarial relacionado con las I&T.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales	➡	**Metas de alineamiento**
• EG02 Gestión de riesgo de negocio • EG06 Continuidad y disponibilidad del servicio de negocio		• AG02 Gestión de riesgo relacionado con I&T • AG07 Seguridad de la información, infraestructura de procesamiento y aplicaciones, y privacidad
Métricas modelo para metas empresariales		**Métricas modelo para metas de alineamiento**
EG02 a. Porcentaje de objetivos y servicios críticos del negocio, cubiertos por la evaluación de riesgos b. Proporción de incidentes significativos que no se identificaron en la evaluación de riesgos frente al total de incidentes c. Frecuencia de actualización del perfil de riesgo		AG02 a. Frecuencia de actualización del perfil de riesgo b. Porcentaje de las evaluaciones de riesgo en la empresa que incluyen el riesgo relacionado con la I&T c. Número de incidentes significativos relacionados con I&T que no se identificaron en la evaluación de riesgos
EG06 a. Número de interrupciones del servicio al cliente o procesos empresariales que han causado incidentes significativos b. Coste de incidentes para el negocio c. Número de horas de procesamiento de negocio perdidas debido a interrupciones del servicio no planificadas d. Porcentaje de quejas en función de los objetivos de disponibilidad del servicio acordados		AG07 a. Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o descrédito público b. Número de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o descrédito público c. Número de incidentes de integridad que causan pérdidas financieras, interrupción del negocio o descrédito público

A. Componente: Proceso		
Práctica de gestión	**Métricas modelo**	
APO12.01 Recopilar datos. Identificar y recopilar datos relevantes para habilitar una efectiva identificación, análisis y reporte de los riesgos relacionados con I&T.	a. Número de eventos de pérdida con características clave capturados en repositorios b. Porcentaje de auditorías, eventos y tendencias capturados en repositorios c. Porcentaje de sistemas críticos con problemas conocidos	
Actividades		**Nivel de capacidad**
1. Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con el riesgo de I&T.		2
2. Registrar datos relevantes y significativos relacionados con los riesgos de I&T en el entorno operativo interno y externo de la empresa.		
3. Adoptar o definir una taxonomía de riesgo para las definiciones consistentes de escenarios de riesgo y categorías de impacto y probabilidad.		3
4. Registrar datos de eventos de riesgo que han causado o podrían causar impacto en el negocio conforme a las categorías de impacto definidas en la taxonomía de riesgo. Capturar datos relevantes de cuestiones, incidentes, problemas e investigaciones.		
5. Estudiar y analizar los datos históricos de riesgo de I&T y de pérdidas experimentadas a partir de datos y tendencias externos disponibles, homólogos de la industria a través de logs de eventos de la industria, bases de datos, y acuerdos de la industria, para la publicación común de eventos.		4
6. Para clases de eventos similares, organizar los datos recopilados y resaltar los factores causantes. Determinar los factores causantes comunes en múltiples eventos.		
7. Determinar las condiciones específicas que existieron o estuvieron ausentes cuando tuvieron lugar los eventos de riesgo y la forma en que las condiciones afectaron a la frecuencia del evento y la magnitud de la pérdida.		
8. Realizar un análisis periódico de eventos y factores de riesgo para identificar riesgos nuevos o emergentes y para mejorar el entendimiento de los factores de riesgo internos y externos asociados.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**	
CMMI Data Management Maturity Model, 2014	Supporting Processes - Risk Management	
COSO Enterprise Risk Management, junio de 2017	8. Performance—Principle 10	
ISO/IEC 27005:2011(E)	8.2 Risk identification; 12. Information security risk monitoring and review	
National Institute of Standards and Technology Special Publication 800 37, Revisión 2 (Borrador), mayo de 2018	3.1 Preparation (Task 7)	

Fuente: Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión

EG04 Calidad de la Información Financiera correspondiente a una de las metas empresariales cuyas métricas del modelo se contemplan:

a) Encuestas de satisfacción de las partes afectadas con respecto al nivel de transparencia, comprensión y precisión de la información financiera de la empresa.
b) Costo real del incumplimiento con respecto a todas las regulaciones financieras.

La Calidad de la información financiera estipulada en la Figura 42, como meta empresarial alineada con el objetivo de gestión AP014 que hace parte de gestionar los datos permite que las decisiones que toman los inversores y/o gerentes de una empresa manufacturera se basa en información confiable y que cumpla con requisitos donde esté bien estructurada, clara y de forma entendible.

Figura 42.

EG04 Calidad de la información financiera en AP014 – Gestionar los datos

Dominio: Alinear, planificar y organizar Objetivo de gestión: APO14 – Gestionar los datos		Área prioritaria: Modelo Core de COBIT
Descripción		
Lograr y mantener la gestión eficaz de los activos de datos de la empresa durante todo el ciclo de vida de los datos, desde la creación hasta su entrega, mantenimiento y archivo.		
Propósito		
Garantizar el uso eficaz de activos de datos críticos para lograr las metas y objetivos empresariales.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales		**Metas de alineamiento**
• EG04 Calidad de la información financiera • EG07 Calidad de la información sobre gestión		AG10 Calidad de la información sobre gestión de I&T
Métricas modelo para metas empresariales		**Métricas modelo para metas de alineamiento**
EG04 a. Encuesta de satisfacción de las partes interesadas clave con respecto al nivel de transparencia, comprensión y precisión de la información financiera de la empresa b. Coste de incumplimiento con respecto a regulaciones financieras		AG10 a. Nivel de satisfacción del usuario con la calidad, puntualidad y disponibilidad de la información de gestión relacionada con I&T, tras considerar los recursos disponibles b. Proporción y extensión de las decisiones de negocio erróneas en las que la información errónea o no disponible relacionada con I&T fue un factor clave c. Porcentaje de información que satisface los criterios de calidad
EG07 a. Grado de satisfacción del consejo de administración y la dirección ejecutiva con la información para la toma de decisiones b. Número de incidentes causados por decisiones erróneas de negocio basadas en información imprecisa c. Tiempo que se tarda en proporcionar la información que respalde la toma de decisiones de negocio eficaces d. Puntualidad de la información sobre gestión		

Fuente: Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión

Dentro las actividades que este componente establece, se aprecian en la Figura 43, con su nivel de capacidad adecuada.

Figura 43.

EG04 Calidad de la información financiera en AP014 – Gestionar los datos

A. Componente: Proceso		
Práctica de gestión	**Métricas modelo**	
APO14.01 Definir y comunicar la estrategia y los roles y responsabilidades de la gestión de datos de la organización. Definir cómo gestionar y mejorar los activos de datos de la organización, en línea con la estrategia y objetivos de la empresa. Comunicar la estrategia de gestión de datos a todas las partes interesadas. Asignar roles y responsabilidades para garantizar que los datos corporativos se gestionen como activos críticos e implementar y mantener la estrategia de gestión de datos de forma eficaz y sostenible.	a. Número de violaciones de gestión de datos comparado con la estrategia definida b. Porcentaje de roles y responsabilidades identificadas para respaldar el gobierno de la gestión de datos y la interacción entre gobierno y la función de gestión de datos.	
Actividades		**Nivel de capacidad**
1. Establecer una función de gestión de los datos con responsabilidad de gestionar las actividades que respalden los objetivos de gestión de los datos.		2
2. Especificar roles y responsabilidades para respaldar la gestión de los datos y la interacción entre el gobierno y la función de gestión de datos.		
3. Asegurar que el negocio y la tecnología desarrollan de forma colaborativa la estrategia de gestión de datos de la organización. Asegurar que los objetivos, prioridades y alcance de la gestión de datos reflejen los objetivos empresariales, sean consistentes con las políticas y regulación de gestión de datos y cuenten con la aprobación de todas las partes interesadas.		3
4. Comunicar los objetivos, prioridades y alcance de la gestión de datos y ajustarlos conforme sea necesario, con base en la retroalimentación recibida.		
5. Usar métricas para evaluar y monitorizar la consecución de los objetivos de la gestión de datos.		4
6. Monitorizar el plan secuencial para la implementación de la estrategia de gestión de datos. Actualizarla como corresponda, con base en las revisiones de su progreso.		
7. Usar técnicas estadísticas y otras técnicas cuantitativas para evaluar la eficacia de los objetivos estratégicos de la gestión de datos a la hora de lograr los objetivos de negocio. Realizar las modificaciones necesarias, con base en las métricas.		
8. Asegurar que la organización investiga procesos innovadores de negocio y requisitos regulatorios emergentes para garantizar que el programa de gestión de datos sea compatible con futuras necesidades del negocio.		5
9. Realizar contribuciones a las mejores prácticas de la industria para el desarrollo e implementación de la estrategia de gestión de datos.		

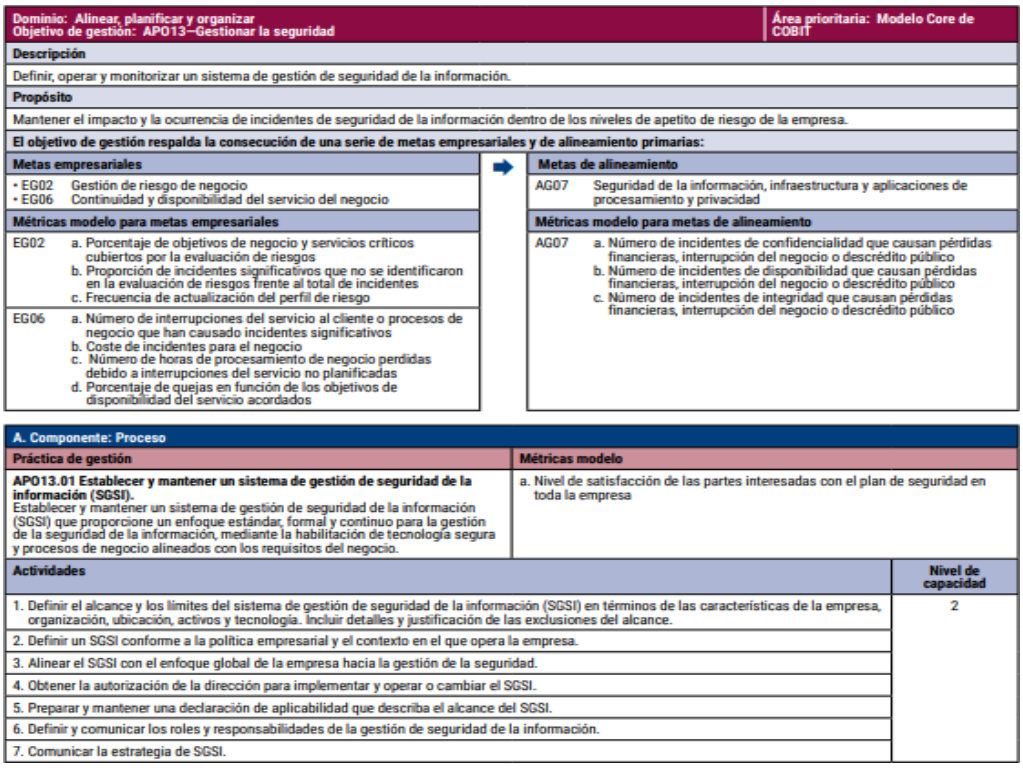
Fuente: Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión

EG06 Continuidad y Disponibilidad del Servicio del Negocio en AP013 contiene las siguientes métrica empresariales:

- Número de interrupciones del servicio al cliente o en su defecto, de procesos de negocio que han causado percances significativos
- Costo de incidentes para el negocio
- Cantidad de tiempo de procesamiento de negocio perdido debido a interrupciones del servicio no planificadas
- Porcentaje de quejas en función de los objetivos de disponibilidad del servicio acordados

Figura 44.

Métricas Metas Empresariales EG06 – Continuidad y disponibilidad del servicio del negocio



Dominio: Alinear, planificar y organizar Objetivo de gestión: APO13—Gestionar la seguridad	Área prioritaria: Modelo Core de COBIT
Descripción	
Definir, operar y monitorizar un sistema de gestión de seguridad de la información.	
Propósito	
Mantener el impacto y la ocurrencia de incidentes de seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.	
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:	
Metas empresariales	**Metas de alineamiento**
• EG02 Gestión de riesgo de negocio • EG06 Continuidad y disponibilidad del servicio del negocio	AG07 Seguridad de la información, infraestructura y aplicaciones de procesamiento y privacidad
Métricas modelo para metas empresariales	**Métricas modelo para metas de alineamiento**
EG02 a. Porcentaje de objetivos de negocio y servicios críticos cubiertos por la evaluación de riesgos b. Proporción de incidentes significativos que no se identificaron en la evaluación de riesgos frente al total de incidentes c. Frecuencia de actualización del perfil de riesgo	AG07 a. Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o descrédito público b. Número de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o descrédito público c. Número de incidentes de integridad que causan pérdidas financieras, interrupción del negocio o descrédito público
EG06 a. Número de interrupciones del servicio al cliente o procesos de negocio que han causado incidentes significativos b. Coste de incidentes para el negocio c. Número de horas de procesamiento de negocio perdidas debido a interrupciones del servicio no planificadas d. Porcentaje de quejas en función de los objetivos de disponibilidad del servicio acordados	

A. Componente: Proceso	
Práctica de gestión	**Métricas modelo**
APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI). Establecer y mantener un sistema de gestión de seguridad de la información (SGSI) que proporcione un enfoque estándar, formal y continuo para la gestión de la seguridad de la información, mediante la habilitación de tecnología segura y procesos de negocio alineados con los requisitos del negocio.	a. Nivel de satisfacción de las partes interesadas con el plan de seguridad en toda la empresa
Actividades	**Nivel de capacidad**
1. Definir el alcance y los límites del sistema de gestión de seguridad de la información (SGSI) en términos de las características de la empresa, organización, ubicación, activos y tecnología. Incluir detalles y justificación de las exclusiones del alcance.	2
2. Definir un SGSI conforme a la política empresarial y el contexto en el que opera la empresa.	
3. Alinear el SGSI con el enfoque global de la empresa hacia la gestión de la seguridad.	
4. Obtener la autorización de la dirección para implementar y operar o cambiar el SGSI.	
5. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.	
6. Definir y comunicar los roles y responsabilidades de la gestión de seguridad de la información.	
7. Comunicar la estrategia de SGSI.	

Fuente: Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión

En la Figura 45 se observa el componente EG07 Calidad de la Información sobre Gestión. Este componente está alineado con la AP014 que corresponde a gestionar los datos. En él existen las siguientes métricas modelo para gestionar las metas empresariales:

- Grado de complacencia del consejo de administración y la dirección ejeutiva con toda la información necesaria para la toma de decisiones
- Cantidad de incidentes causados por resoluciones equivocadas de negocio basadas en información no precisa
- Tiempo que se tarda en dar la información que respalde la toma de decisiones de negocio eficaces
- Puntualidad de la información sobre gestión

Figura 45.

Métricas Metas Empresariales EG06 – Continuidad y disponibilidad del servicio del negocio

Dominio: Alinear, planificar y organizar **Objetivo de gestión: APO14 – Gestionar los datos**		**Área prioritaria: Modelo Core de COBIT**
Descripción		
Lograr y mantener la gestión eficaz de los activos de datos de la empresa durante todo el ciclo de vida de los datos, desde la creación hasta su entrega, mantenimiento y archivo.		
Propósito		
Garantizar el uso eficaz de activos de datos críticos para lograr las metas y objetivos empresariales.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales	➡	**Metas de alineamiento**
• EG04 Calidad de la información financiera • EG07 Calidad de la información sobre gestión		AG10 Calidad de la información sobre gestión de I&T
Métricas modelo para metas empresariales		**Métricas modelo para metas de alineamiento**
EG04 a. Encuesta de satisfacción de las partes interesadas clave con respecto al nivel de transparencia, comprensión y precisión de la información financiera de la empresa b. Coste de incumplimiento con respecto a regulaciones financieras		AG10 a. Nivel de satisfacción del usuario con la calidad, puntualidad y disponibilidad de la información de gestión relacionada con I&T, tras considerar los recursos disponibles b. Proporción y extensión de las decisiones de negocio erróneas en las que la información errónea o no disponible relacionada con I&T fue un factor clave c. Porcentaje de información que satisface los criterios de calidad
EG07 a. Grado de satisfacción del consejo de administración y la dirección ejecutiva con la información para la toma de decisiones b. Número de incidentes causados por decisiones erróneas de negocio basadas en información imprecisa c. Tiempo que se tarda en proporcionar la información que respalde la toma de decisiones de negocio eficaces d. Puntualidad de la información sobre gestión		

Fuente: Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión

Con respecto a las Metas de Alineamiento, "*In COBIT 5, alignment is considered to be the result of all governance and management activities*" (en COBIT 5, se considera el alineamiento como el resultado de todas las actividades de gobernanza y gestión). (ISACA, 2012) Por lo que esta expresión muestra claramente que el alineamiento es considerado como todo aquel resultado de todas las actividades de gobernanza y gestión; razón por la cual, se incluyó en el presente modelo. Las Metas de Alineamiento estructuradas son: AG02 Gestión de riesgo relacionado con I&T, AG07 Seguridad de la información, infraestructura de procesamiento, aplicaciones y privacidad, AG10 Calidad de la Información sobre gestión de I&T.

En este orden de ideas, en la Tabla 9, se plantea el relacionamiento de las Metas Empresarias – Metas de alineamiento estipulados en el modelo. Cabe mencionar, que en esta tabla se establece que la letra "P" que se refiere a ser un relacionamiento tipo primario, considerado de mucha relevancia y tangibilidad por lo que tienen una relación directa.

Tabla 9.

Tabla de Relacionamiento de las Metas Empresariales-Metas de Alineamiento.

Metas Corporativas / Metas de Alineamiento	EG02 Gestión del riesgo del negocio	EG04 Calidad de la información financiera	EG06 Continuidad y disponibilidad del servicio del negocio	EG07 Calidad de la información sobre gestión
AG02 Gestión de riesgo relacionado con I&T	P			
AG07 Seguridad de la información, infraestructura de procesamiento y aplicaciones y privacidad	P		P	
AG10 Calidad de la información sobre gestión de I&T		P		P

Fuente: Autora con base al Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión

Los objetivos de gobierno y gestión, según el COBIT 5.0:2019, están agrupados en cinco dominios que se pueden visualizar en la Figura 41. Estos dominios tienen la finalidad de expresar el propósito de los objetivos que contienen.

Figura 41.

Dominios de COBIT 5.0:2019 objetivos de gobierno y objetivos de gestión

Fuente: Autora con base al Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión

En este orden de ideas, el modelo propuesto plantea los objetivos de gobierno y gestión: APO12 Gestionar el riesgo, APO13 Gestionar la seguridad, APO14 Gestionar los datos.

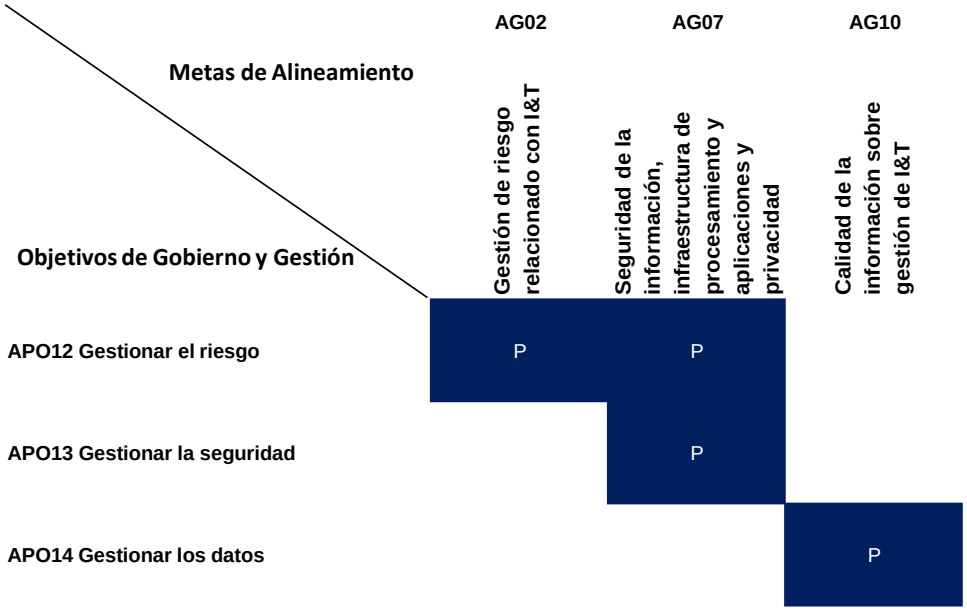
Un objetivo de gobierno y gestión siempre está relacionado a un proceso y a unos componentes que permiten ayudar a la consecución del objetivo. En este modelo, se ven claramente en la Tabla 8, las relaciones de los objetivos con su relación respecto a las metas de alineamiento con un relacionamiento “P”, primario.

APO12 Gestionar el riesgo: Integrar la gestión del riesgo empresarial relacionado con la I&T con la gestión del riesgo empresarial global equilibrando los costes y beneficios de la gestión del riesgo empresarial relacionado con T&I.

APO13 Gestionar la seguridad: conservar el impacto y la existencia de incidentes de seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.

Tabla 10.

Relación primaria Metas de alineamiento con los objetivos de gobierno/gestión



Fuente: Autora con base al Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión

APO14 Gestionar los datos Asegurar el uso eficaz de activos de datos críticos para lograr las metas y objetivos empresariales.

En el interior del modelo propuesto, se observa la importancia de involucrar los 14 controles de la norma ISO 27002:2013 debido a que en la medida en que se establezcan

directrices y principios de manera general que tienen como finalidad iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una empresa haciendo que sus metas y objetivos sean de mayor valor. En la Tabla 9 se puede aprecias los controles involucrados en el modelo propuesto.

Tabla 11.

Controles ISO 27002:2013involucrados en el modelo

1. Continuidad del negocio	2. Cumplimiento	3. Políticas de seguridad	4. Adquisión y desarrollo	5. Relación de proveedores	6. Gestión de incidentes	7. Organización de la seguridad
8. Gestión de activos	9. Seguridad de activos	10. Seguridad en comunicaciones	11. Seguridad física	12. Criptografía	13. Control de acceso	14. Seguridad en la operación

Fuente: Norma ISO 27002:2013

Esta norma proporciona recomendaciones valiosas sobre las mejores prácticas en la gestión de la seguridad de la información, por lo cual, se considera importante definir cada uno de ellos:

1. Continuidad del negocio: garantizar el seguimiento de actividades de las organizaciones
2. Cumplimiento: relaciones de hechos y normas política aplicables en el campo garantizando su cumplimiento.
3. Políticas de seguridad: disposición de una normatividad adecuada de seguridad aprobada por la dirección.
4. Adquisición y desarrollo: es el elemento transversal clave involucrado en el ciclo de vida de un sistema de gestión

5. Relación de proveedores: componente que establece medidas de seguridad entre las relaciones con terceras partes.
6. Gestión de incidentes: es la preparación para cuando ocurran incidentes permitiendo dar respuesta de forma rápida y eficiente logrando una prevención futura.
7. Organización de la seguridad : acciones pertinentes para salvaguardar y recuperar de alguna forma, información relevante cuando se haya perdido.
8. Gestión de activos: se centra en la atención en la información como activo y en cómo se deben establecer medidas adecuadas para guardarlos de las incidencias, quiebras en la seguridad y en la alteración no deseada.
9. Seguridad de activos: parámetros que tiene como fin salvaguardar la integridad de los activos físico de información
10. Seguridad en comunicaciones: garantiza y protege de forma adecuada los medios de transmisión de datos.
11. Seguridad física: gestiona adecuadamente hábitos que aportan eficiencia en la gestión de salvaguardar a nivel tecnológicos los recursos
12. Criptografía: técnicas para proteger y garantizar autenticidad, confidencialidad e integridad de la información
13. Control de acceso: gestiona los privilegios de acceso en un sistema de información
14. Seguridad en la operación: es un componente técnico que relaciona todos los aspectos disponibles como la protección del software, copias de seguridad, gestión de vulnerabilidad, entre otros.

4.3. Viabilidad del modelo de seguridad de la información para el sector industrial manufacturero

Una vez, teniendo el modelo de seguridad de la información propuesto para el sector industrial manufacturero, se seleccionó una metodología de pronóstico que brindara confiabilidad y que permitiera visualizar los diferentes puntos de vista de personas expertas en la temática. El autor Mengual (Mengual, 2011) indica que se puede llegar a entender por experto: ¨*tanto al individuo como al grupo de personas que son capaces de proporcionar valoraciones fiables sobre un problema en cuestión, y al mismo tiempo, hacen recomendaciones en función de un máximo de competencia*¨.

De este modo, se estableció el método Delphi como el más adecuado para este fin, debido a que fue desarrollado con el propósito de utilizar la experticia para predecir o pronosticar como se comportaría un fenómeno en el futuro. (MSc.Margarita García Valdés, 2013) Para la autora, quien consideró que esta técnica tenía muchas ventajas y características atractivas realizar procesos iterativos, para hacer retroalimentación, para tener anonimato y por último el más importante: la construcción de un concenso.

Para la aplicación de esta técnica, se inició con una primera fase que consistió en seleccionar un panel de expertos que tendrán la responsabilidad de responder la consulta, considerada ésta el principal objetivo. En esta fase se definieron las variables de competencias de cada uno de ellos diseñando un instrumento que permitiera ser aplicado de manera directa e individual (ver Apéndice B). (Aguilar, 2019)

Se puede apreciar el cuadro de los expertos seleccionados tanto en la Universidad Francisco de Paula Santander en Ocaña, como también expertos en la Universidad Popular del Cesar y otros profesionales egresados que cumplen un rol importante dentro del área de TI del sector industrial manufacturero :

Tabla 12.

Perfil de los diferente expertos que hicieron parte de la consulta

Experto	Entidad Productiva / Institución Educativa	Calificación Profesional	Tiempo Experiencia (años)
1	Universidad Popular del Cesar	Doctor	8
2	Universidad Popular del Cesar	Magister	10
3	Universidad Francisco de Paula Santander	Doctor	20
4	Colcircuitos (Jefe TI)	Especialista	10
5	Electrónica de la Costa (Jefe TI)	Especialista	10
6	DPA (Gerente TI)	Especialista	15
7	Coca Cola Femsa (Gerente TI)	Magister	11
8	Servicios y Asesorías del Litoral (Jefe Sistemas)	Especialista	12
9	Universidad Antonio Nariño	Magister	21

Fuente: Autora, Basado en (Rodríguez, García & García)

Una vez aplicado el instrumento a los Expertos seleccionados, como resultado, se obtuvo información valiosa por las variadas opiniones; con criterios válidos todos, lo cual enriqueció mucho más la investigación. Importante resaltar que se encontraron panelistas muy preparados en conocimiento teórico, así como también, muchos profesionales con muchos años de experiencia técnica en el campo de Tecnologías de la Información en empresas privadas de producción manufacturera como también en el área de servicios.

A continuación, se da a conocer los resultados de esta valoración iniciando por el grupo de expertos seleccionados:

Tabla 13.

Frecuencia acumulada encuesta a expertos

	Preguntas	MR	BR	R	PR	NT	TOT
1	El ¨Modelo de Seguridad de la Información bajo los principios de Gobierno TI para el sector industrial manufacturero¨se sustenta en estándares reconocidos?	9	9	9	9	9	45
2	Los elementos incorporados en el ¨Modelo de seguridad de la información bajo los principios de Gobierno TI para el sector industrial manufacturero¨los ve pertinentes?	6	7	9	9	9	40
3	Existe una correspondencia entre el ¨Modelo de seguridad de la información bajor los principios de Gobierno TI para el sector industrial manufacturer¨y la definición?	8	9	9	9	9	44
4	El ¨Modelo de seguridad de la información bajo los principios de Gobierno TI para el sector industrial manufacturero¨podría ser adaptado en una empresa del sector productivo manufacturero?	7	8	9	9	9	42
5	Hay coherencia entre los componentes del modelo propuesto?	6	9	9	9	9	42
6	Hay una correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características?	8	9	9	9	9	44

Fuente: Autor. Basado en (Rodríguez, García & García)

A partir de la frecuencia acumulada, se continua con la división de cada resultado de la tabla entre la cantidad de expertos del área que participaron en la consulta. Por lo tanto, cada valor se divide entre 9 obteniéndose un cociente que debe estar aproximado hasta unas diez milésimas. Es por ello, que a continuación, se muestra en la Tabla 14, la Frecuencia Relativa Acumulada como resultado de esta división. Igualmente se logra establecer solamente los cuatro puntos de corte debido a que se trata solamente de cinco categorías.

Tabla 14.

Frecuencia relativa acumulada encuesta a expertos

	Preguntas	MR	BR	R	PR
1	El ¨Modelo de Seguridad de la Información bajo los principios de Gobierno TI para el sector industrial manufacturero¨se sustenta en estándares reconocidos?	1,000	1,000	1,000	1,000
2	Los elementos incorporados en el ¨Modelo de seguridad de la información bajo los principios de Gobierno TI para el sector industrial manufacturero¨los ve pertinentes?	0,667	0,778	2,000	1,000
3	Existe una correspondencia entre el ¨Modelo de seguridad de la información bajor los principios de Gobierno TI para el sector industrial manufacturer¨y la definición?	0,889	1,000	1,000	1,000
4	El ¨Modelo de seguridad de la información bajo los principios de Gobierno TI para el sector industrial manufacturero¨podría ser adaptado en una empresa del sector productivo manufacturero?	0,778	0,889	1,000	1,000
5	Hay coherencia entre los componentes del modelo propuesto?	0,667	1,000	1,000	1,000
6	Hay una correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características?	0,889	1,000	1,000	1,000

Fuente: Autor. Basado en (Rodríguez, García & García)

Conociendo la frecuencia relativa acumulada, se pudo encontrar las imágenes correspondientes a cada uno de los valores por la inversa de la curva normal, por lo tanto, se encontraron los siguientes valores expresados en la Tabla No.15. Puntos de corte de la función.

Tabla 15.

Puntos de corte de la funcion analizada

	Preguntas	MR	BR	R	PR	TOT	PROM
1	El ¨Modelo de Seguridad de la Información bajo los principios de Gobierno TI para el sector industrial manufacturero¨se sustenta en estándares reconocidos?	4,50	4,50	4,50	4,50	18,00	4,50
2	Los elementos incorporados en el ¨Modelo de seguridad de la información bajo los principios de Gobierno TI para el sector industrial manufacturero¨los ve pertinentes?	0,17	0,29	4,50	4,50	9,46	2,37
3	Existe una correspondencia entre el ¨Modelo de seguridad de la información bajor los principios de Gobierno TI para el sector industrial manufacturer¨y la definición?	0,28	4,50	4,50	4,50	13,78	3,45
4	El ¨Modelo de seguridad de la información bajo los principios de Gobierno TI para el sector industrial manufacturero¨podría ser adaptado en una empresa del sector productivo manufacturero?	0,12	4,50	4,50	4,50	13,62	3,41
5	Hay coherencia entre los componentes del modelo propuesto?	0,21	4,50	4,50	4,50	13,71	3,43
6	Hay una correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características?	0,28	4,50	4,50	4,50	13,78	3,45
	SUMA TOTAL COLUMNA	5,56	22,79	27,00	27,00	82,35	
	PROMEDIO	0,9258	3,7983	4,5000	4,5000	13,7242	3,4310

Fuente: Autor. Basado en (Rodríguez, García & García)

Los puntos de corte son importantes establecerlos para identificar las respuestas inconsistentes en la valoración del modelo pues está basado en la elección y se supone que el experto encuestado es racional, logra también estar bien informado en la temática y quizás, pueda elegir de forma experimental con una guía, sin embargo, en investigaciones se han detectado la carencia de motivaciones en la búsqueda de la mejor elección. Es por ello, que al establecer estos puntos de corte se logra una decisión racional y se eliminan respuestas inconsistentes.

Conclusión de respuestas de expertos. Se hizo un análisis y se logró una comparación detalla de cada una de las respuestas de los expertos estableciendo una idea concluyente sobre

cada criterio de categoría analizada, por lo tanto, en la Tabla 15, se detalla la validación de respuestas de expertos. También fue importante considerar las respuestas a las preguntas abiertas establecidas en el instrumentos de consulta donde los expertos estuvieron de acuerdo en establecer varios aspectos como: la correspondencia que existe entre el modelo y la metodología utilizada, las categorías del modelo diseñado, lo específico del modelo, la claridad del contenido y obviamente, la coherencias estructural del modelo.

Como conclusión de esta valoración, se pudo establecer que el panel de expertos seleccionado, evaluaron y determinaron de manera muy favorable del modelo que se propuso dando pertinencia de cada aseveración. Esto se observó por las respuestas de MR (muy relevante) sumó una totalidad de un 66,6%, mientras que el resultado de BR (bastante relevante) sumó una totalidad de 33,3%, conservando así, un resultado cero, en los casos R(relevante), PR (poco relevante) y NR (nada relevante).

Tabla 16.

Validación de respuestas de expertos

	Preguntas	MR	BR
1	El ¨Modelo de Seguridad de la Información bajo los principios de Gobierno TI para el sector industrial manufacturero¨se sustenta en estándares reconocidos?	SI	
2	Los elementos incorporados en el ¨Modelo de seguridad de la información bajo los principios de Gobierno TI para el sector industrial manufacturero¨los ve pertinentes?		SI
3	Existe una correspondencia entre el ¨Modelo de seguridad de la información bajor los principios de Gobierno TI para el sector industrial manufacturer¨y la definición?	SI	
4	El ¨Modelo de seguridad de la información bajo los principios de Gobierno TI para el sector industrial manufacturero¨podría ser adaptado en una empresa del sector productivo manufacturero?		SI
5	Hay coherencia entre los componentes del modelo propuesto?	SI	
6	Hay una correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características?	SI	

Fuente: Autora. Basado en (Rodríguez, García & García)

En la última fase del análisis de valoración de expertos, se revisaron las respuestas cualitativas donde los expertos proponen modificaciones al modelo para mejorarlo, pero se pudo observar que no hubo propuestas significativas, por lo tanto, se establece que el modelo tuvo la aceptación adecuada.

Tabla 17.

Juicio cualitativo de expertos del modelo a valorar

No. Experto	Para incluir	Por eleminar	Por cambiar
Experto 1	Ninguna	Ninguna	Ninguna
Experto 2	Ninguna	Ninguna	Ninguna
Experto 3	Ninguna	Ninguna	Ninguna
Experto 4	Ninguna	Ninguna	Ninguna
Experto 5	Ninguna	Ninguna	Ninguna
Experto 6	Ninguna	Ninguna	Ninguna
Experto 7	Ninguna	Ninguna	Ninguna
Experto 8	No responde	No responde	No responde
Experto 9	Ninguna	Ninguna	Ninguna

Fuente: Autora. Basado en (Rodríguez, García & García)

Capítulo 5. Conclusiones

Los estándares más referenciados de prácticas de seguridad de la información se lograron identificar, tomando referentes el COBIT 5.0 y el grupo de normas ISO 27000:2017, ISO 27001:2015, ISO 27002:2017, ISO 27005:2011; analizando los componentes esenciales que son aplicables al sector de la industria manufacturera. Igualmente se estudiaron los diferentes procesos establecidos en el interior del tipo de organizaciones industriales.

Con base al marco de referencia COBIT 5.0:2019 y a la familia de normas ISO 27000, se logró estructurar los componentes necesarios en Gobierno TI para el diseño del modelo de seguridad de la información para empresas en el sector industrial manufacturero. Esta estructura se inició con los Stakeholders, los procesos misionales de las empresas, metas empresariales, metas de alineamiento y los objetivos de gobierno y gestión.

Tomando como referencia el Modelo Delphi, se logró hacer la validación del modelo propuesto contando con la participación de un panel de 9 expertos con perfiles en Tecnologías de la Información y Comunicación y con amplios conocimientos metodológicos y experimentales. Esto logró establecer que el modelo propuesto cumple con las características básicas y es recomendable para la aplicación en empresas del sector industrial manufacturero.

Capítulo 6. Recomendaciones

Se recomienda implementar el modelo de seguridad de la información en empresas productoras del sector de manufactura. Deberá estar involucrado y comprometido el personal pertinente.

Referencias

Aguilar, Norly. (2019). Modelo de Seguridad de la Información para Instituciones de Educación Superior. Ocaña, Norte de Santander.

Ackerman, S. E. (2013). *Metodología de la investigación.* Buenos Aires, Argentina: Ediciones del Aula Taller.

Alvarado Ortega, M. (2016). Barrranquilla, Ciudad con Río y Mar.

Andrade, S. (2018). *Estrategia y Conducción de los Contenidos y Procesos de Enseñanza y Aprendizaje en el Sistema Modular.*

Baca Urbina, G. (2016). *Introducción a la seguridad informática.* México D.F: Grupo Editorial Patria.

Baca Urbina, G. (2016). *Proyectos de sistemas de información.* México: Recuperado de https://elibro.net/es/ereader/biblioupc/40423?page=38.

Baena Paz, G. M. (2017). *Metodología de la investigación (3a. ed.).* . México D.F.: Grupo Editorial Patria. Recuperado de https://elibro.net/es/ereader/biblioupc/40513?page=8.

Banco de la República. (2019). BER Boletín Económico Regional IV Trimestre 2019 ISSN 2665-1807. Bogotá, Cundinamarca, Colombia.

Camelo, L. (02 de 2010). *http://seguridadinformacioncolombia.blogspot.com/2010/02/seguridad-de-la-informacion-y-seguridad.html*.

Carolina Masso. (2018). Qué tan conscientes son las empresas colombianas de los riesgos de seguridad informática? *Enter.co*.

CongresodelaRepública. (2019). *http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html.*

CorteConstitucional. (2016). *https://www.corteconstitucional.gov.co/inicio/Constitucion%20politica%20de%20Colombia.pdf.* Obtenido de

www.cvn.com.co. (2020). *Sector Manufacturero Colombiano más optimista en el 2019*. Obtenido de www.cnv.com.co: https://www.cvn.com.co/sector-manufacturero/

DANE. (27 de Diciembre de 2019). Boletín Técnico Indicadores Básicos de Tenencia y uso de Técnologías de la Información y Comunicación en Empresas (TIC empresas) 2018. Bogotá, Cundinamarca, Colombia. Obtenido de https://www.dane.gov.co/files/investigaciones/boletines/tic/bol_empresas_2018.pdf:

DANE. (2019). *http://microdatos.dane.gov.co/index.php/catalog/650*. Obtenido de www.dane.gov.co: http://microdatos.dane.gov.co/index.php/catalog/650

Escrivá Gascó, G. (2013). *Seguridad informática. Recuperado de https://elibro.net/es/ereader/biblioupc/43260?page=8.* Madrid, España: Macmillan Iberia S.A. .

Farello&Sagbini. (2019). *DISEÑO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SGSI BASADO EN EL ESTÁNDAR ISO 27001, EN ULTRALINE ELECTRÓNICA S.A.S., EN LA CIUDAD DE BARRANQUILLA.* Ocaña.

http://www.prakmatic.com/. (2017). *http://www.prakmatic.com*. Obtenido de http://www.prakmatic.com: http://www.prakmatic.com/gestion-ti/por-que-implementar-el-gobierno-de-ti-en-las-empresas/

https://advisera.com/. (2016). *https://advisera.com/*. Obtenido de https://advisera.com/.

https://es.wikipedia.org/. (2019). *https://es.wikipedia.org/wiki/Barranquilla*. Obtenido de https://es.wikipedia.org/wiki/Barranquilla: https://es.wikipedia.org/wiki/Barranquilla

https://geniusitt.com/. (2018). *https://geniusitt.com/*.

https://iveconsultores.com/. (2020). *https://iveconsultores.com/*.

https://nextech.pe/. (2018). *https://nextech.pe/*.

https://ostec.blog/. (s.f.). *https://ostec.blog/*. Obtenido de https://ostec.blog/.

https://www.definicionabc.com. (2020). *https://www.definicionabc.com/*.

https://www.elheraldo.co/. (05 de 2020). Obtenido de https://www.elheraldo.co/economia/comercio-e-industria-con-miras-la-digitalizacion-en-el-atlantico-729807

https://www.esan.edu.pe/. (junio de 2016).

https://www.servicetonic.com/. (2019). *https://www.servicetonic.com/*.

ICONTEC. (2013). *NTC-ISO/IEC 27001*.

(ICONTEC), I. C. (2006). *NORMA TÉCNICA NTC-ISO/IEC.* Instituto Colombiano de Normas Técnicas y Certificación.

Informacolombia.com. (2020). *https://www.informacolombia.com/directorio-empresas/actividad/2790_FABRICACION-DE-OTROS-TIPOS-DE-EQUIPO-ELECTRICO-N-C-P/localidad_barranquilla*.

ISACA. (2012). *COBIT 5, Un Marco de Negocio para le Gobierno y la Gestión de las TI de la Empresa.*

ISACA. (2019). *Framework-Governance-and-Management-Objectives.*

ISO. (2012). *ISO/IEC 27001 TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS.*

Iso. (01 de Febrero de 2019). *International Organization for Standardization*. Obtenido de iso.org: https://www.iso.org/standard/54534.html

IT Governance, I. (2009). *IT GOVERNANCE USING COBIT AND VAL IT*.

ITGIRolling Meadows. (2008). IT Governance, global status report 2008. .

Johansen. (2000). *Introducción a la Teoría General de Sistemas.* México: Limusa S.A. de C.V.

Lapiedra Alcamí, R. D.-U. (2016). *Introducción a la gestión de sistemas de información en la empresa.* . Madrid: Castelló de la Plana, Spain: D - Universitat Jaume I. Servei de Comunicació i Publicacions. Recuperado de https://eli.

Lopez, F. (2002). El Análisis de Contenido como Método de Investigación. *Revista de Educación 4, Universidad de Huelva*, 167-179.

López-RoldánPedro&FachelliSandra. (2017). El Diseño de la Muestra. *Metodología de la Investigación Social Cuantitativa*, 64.

Lorca Fernández, P. (2004). *La creación de valor en la empresa y los "stakeholders".* Barcelona: Ediciones Deusto-Planeta de Agostini Profesional y Formación S.L.

MINTIC. (2018). *Guñia para la Administración del Riesgo y Diseño de Controles en Entidades Públicas.*

MINTIC. (2020). *Gobierno TI*. Obtenido de https://www.mintic.gov.co/: https://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8078.html

Monfort, R. (2016). *COBIT 5 y El Cuadro de Mando Integral como Herramientas de Gobierno de TI.* Valencia.

Monje, C. A. (2011). *Metodología de la Investigación Cuantitativa y Cualitativa, Guía didáctica*. Neiva: Universidad Surcolombiana.

Muñóz, I. G. (2011). Gobierno de TI-Estado del arte. *Sistemas&Telemática*, 23-53.

Ortiz, N. R. (2013). *Mejoramiento de Procesos en Empresas de Prestación de Servicios.* UIS.

Pablos Heredero, C. D.-R. (2019). *Organización y transformación de los sistemas de información en la empresa (4a. ed.).* Madrid: ESIC Editorial - Recuperado de https://elibro.net/es/ereader/biblioupc/119671?p.

Pineda, D. G. (2016). *REVISIÓN BIBLIOGRÁFICA DE LA NORMA ISO 27001 Y SUS.* Tunja.

PMK Digital, L. (10 de 08 de 2020). *www.pmkvirtual.com*.

Procolombia. (2020). *https://colombia.travel/es/barranquilla*. Obtenido de https://colombia.travel/es/barranquilla: https://colombia.travel/es/barranquilla

QUINTERO, N. A. (2018). *MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES DE EDUCACIÓN SUPERIOR.* OCAÑA, NORTE DE SANTANDER.

Reis, L. C. (2015). *Fundamentos de COBIT.*

Revista Semana. (2020). Los hackers se están volviendo más fuertes. *Semana*.

Rojas Córsico, I. S. (2009). *Trabajo de auditoría normas COBIT.* Santa Fe, Argentina: El Cid Editor.

RSM. (04 de 08 de 2017). *https://www.rsm.global*. Obtenido de https://www.rsm.global/: https://www.rsm.global/mexico/es/perspectivas/special-reports/implementando-un-gobierno-de-ti-en-6-fases-parte-1

Surveymonkey. (2016). *https://es.surveymonkey.com/mp/quantitative-vs-qualitative-research/?program=7013A000000mweBQAQ&utm_bu=CR&utm_campaign=71700000064157461&utm_adgroup=58700005704021388&utm_content=39700052007818784&utm_medium=cpc&utm_source=adwords&utm_term=p52007818784&ut.*

TapiaB., M. (2000). Metodología de Investigación. Santiago de Chile, Santiago de Chile, Chile. Obtenido de https://aulavirtual.fio.unam.edu.ar: https://aulavirtual.fio.unam.edu.ar/pluginfile.php/6545/mod_resource/content/0/Metodologia_de_la_Investigacion_-_Lect._Compl_1.pdf

Universia. (04 de 09 de 2017). *https://noticias.universia.cr/educacion/noticia/2017/09/04/1155475/tipos-investigacion-descriptiva-exploratoria-explicativa.html*.

Valencia, P. A. (2017). *Aplicación de la Gestión de Stakeholders en Proyectos de Investigaión en Colombia, caso de Estudio Universidad de Cundinamarca.* Cartagena.

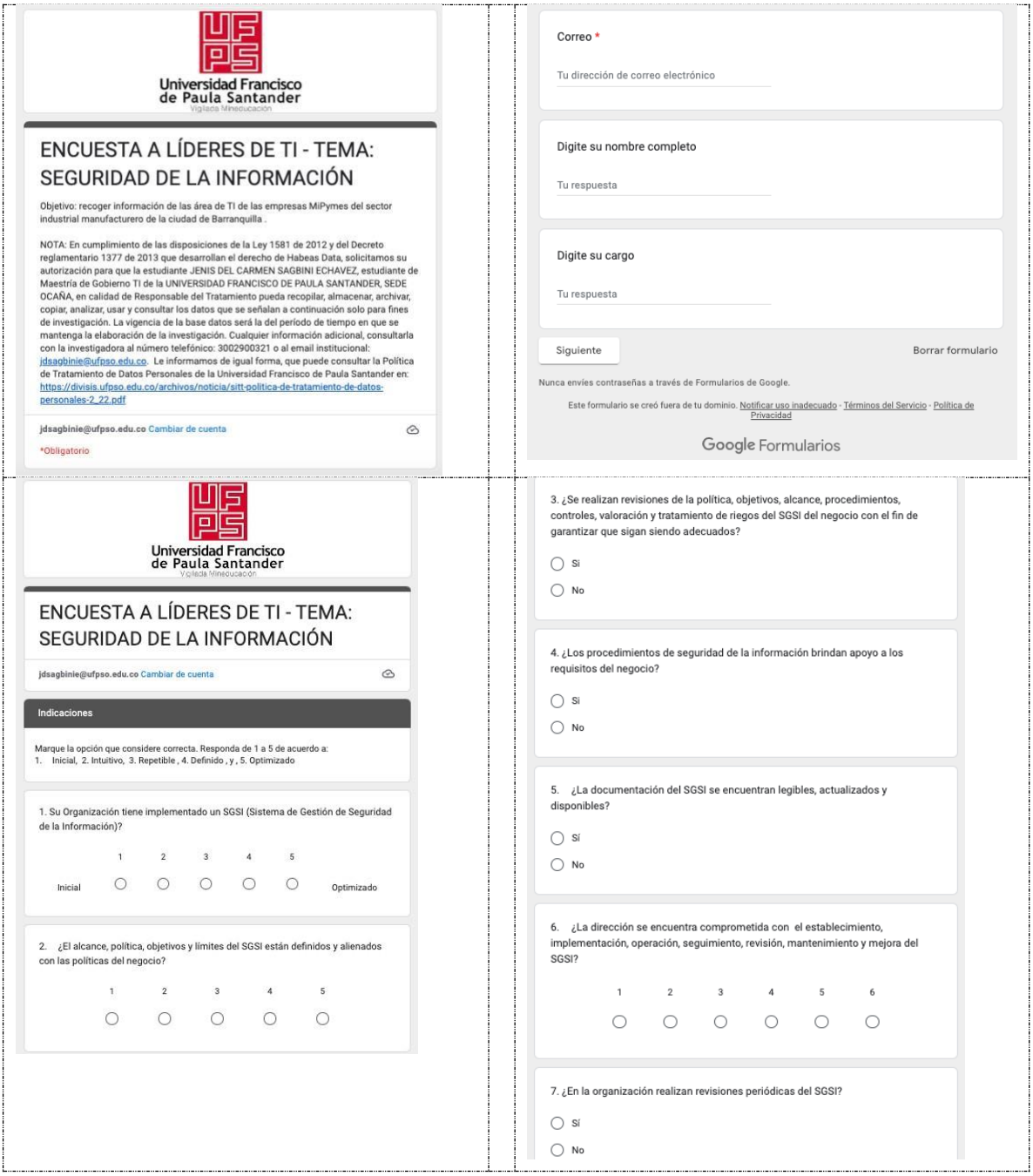
www.informacolombia.com. (2020). *https://www.informacolombia.com/directorio-empresas/actividad/2790_FABRICACION-DE-OTROS-TIPOS-DE-EQUIPO-ELECTRICO-N-C-P/localidad_barranquilla*.

www.wikipedia.org. (26 de 05 de 2020). *Historia_de_Barranquilla*. Obtenido de https://es.wikipedia.org/: https://es.wikipedia.org/wiki/Historia_de_Barranquilla

Apéndices

Apéndice A

https://forms.gle/CSrqSbGw9wJYBeYa8



Universidad Francisco de Paula Santander

Vigilada Mineducación

ENCUESTA A LÍDERES DE TI - TEMA: SEGURIDAD DE LA INFORMACIÓN

Objetivo: recoger información de las área de TI de las empresas MiPymes del sector industrial manufacturero de la ciudad de Barranquilla .

NOTA: En cumplimiento de las disposiciones de la Ley 1581 de 2012 y del Decreto reglamentario 1377 de 2013 que desarrollan el derecho de Habeas Data, solicitamos su autorización para que la estudiante JENIS DEL CARMEN SAGBINI ECHAVEZ, estudiante de Maestría de Gobierno TI de la UNIVERSIDAD FRANCISCO DE PAULA SANTANDER, SEDE OCAÑA, en calidad de Responsable del Tratamiento pueda recopilar, almacenar, archivar, copiar, analizar, usar y consultar los datos que se señalan a continuación solo para fines de investigación. La vigencia de la base datos será la del período de tiempo en que se mantenga la elaboración de la investigación. Cualquier información adicional, consultarla con la investigadora al número telefónico: 3002900321 o al email institucional: jdsagbinie@ufpso.edu.co. Le informamos de igual forma, que puede consultar la Política de Tratamiento de Datos Personales de la Universidad Francisco de Paula Santander en: https://divisis.ufpso.edu.co/archivos/noticia/sitt-politica-de-tratamiento-de-datos-personales-2_22.pdf

jdsagbinie@ufpso.edu.co Cambiar de cuenta

*Obligatorio

Correo *

Tu dirección de correo electrónico

Digite su nombre completo

Tu respuesta

Digite su cargo

Tu respuesta

Siguiente

Borrar formulario

Nunca envíes contraseñas a través de Formularios de Google.

Este formulario se creó fuera de tu dominio. Notificar uso inadecuado - Términos del Servicio - Política de Privacidad

Google Formularios

Universidad Francisco de Paula Santander

Vigilada Mineducación

ENCUESTA A LÍDERES DE TI - TEMA: SEGURIDAD DE LA INFORMACIÓN

jdsagbinie@ufpso.edu.co Cambiar de cuenta

Indicaciones

Marque la opción que considere correcta. Responda de 1 a 5 de acuerdo a:
1. Inicial, 2. Intuitivo, 3. Repetible , 4. Definido , y , 5. Optimizado

1. Su Organización tiene implementado un SGSI (Sistema de Gestión de Seguridad de la Información)?

1 2 3 4 5

Inicial ○ ○ ○ ○ ○ Optimizado

2. ¿El alcance, política, objetivos y límites del SGSI están definidos y alienados con las políticas del negocio?

1 2 3 4 5

○ ○ ○ ○ ○

3. ¿Se realizan revisiones de la política, objetivos, alcance, procedimientos, controles, valoración y tratamiento de riegos del SGSI del negocio con el fin de garantizar que sigan siendo adecuados?

○ Si

○ No

4. ¿Los procedimientos de seguridad de la información brindan apoyo a los requisitos del negocio?

○ Si

○ No

5. ¿La documentación del SGSI se encuentran legibles, actualizados y disponibles?

○ Si

○ No

6. ¿La dirección se encuentra comprometida con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI?

1 2 3 4 5 6

○ ○ ○ ○ ○ ○

7. ¿En la organización realizan revisiones periódicas del SGSI?

○ Si

○ No

8. Con qué frecuencia se realizan esas revisiones periódicas del SGSI?

- ◯ Cada 6 meses
- ◯ Cada año
- ◯ Cada dos años

9.¿La organización tiene establecido roles, privilegios, control de acceso y responsabilidades de los usuarios de TI, de acuerdo con la política del SGSI?

- ◯ Sí
- ◯ No

10. ¿Periódicamente se realizan revisiones de las definiciones de control de acceso que permita asegurar que los privilegios y roles son validos con los usuarios?

- ◯ Si
- ◯ No

11. ¿Se llevan a cabo auditorías internas planificadas al SGSI de la organización?

- ◯ Sí
- ◯ No

12. Con qué frecuencia se realizan las auditorías internas planificadas al SGSI en la Organización?

- ◯ Cada 6 meses
- ◯ Cada año
- ◯ Cada dos años

13. ¿La organización implementa acciones correctivas y preventivas con la finalidad de eliminar las no conformidad de las auditorias?

- ◯ Si
- ◯ No

14. La Organización cuenta con un inventario de activos informáticos?

- ◯ Sí
- ◯ No

15. ¿Se encuentran establecidas las normas de uso de los activos informáticos?

- ◯ Sí
- ◯ No

16. ¿La organización cuenta con seguridad física y del entorno a las áreas de procesamiento de información con el fin de evitar daño, pérdida o robo?

1	2	3	4	5
◯	◯	◯	◯	◯

17. ¿Existen controles de protección del software y la información de la organización?

- ◯ Sí
- ◯ No

18. ¿Se estableció un plan de tratamiento de riesgos de seguridad de la información alineado con los política del negocio?

- ◯ Si
- ◯ No

19. ¿Se realizan programas de capacitación y concienciación en relación a roles, responsabilidades, controles, seguridad física y de la información?

- ◯ Sí
- ◯ No

20. ¿Se realizan copias de respaldo de la información y del software?

- ◯ Sí
- ◯ No

21. ¿Con qué frecuencia se hacen las copias de respaldo de la información y del software?

- ◯ Diario
- ◯ Semanal
- ◯ Mensual

22. ¿Están protegidas las redes adecuadamente contra amenazas?

- ◯ Sí
- ◯ No

23. ¿Están implementados mecanismos de filtrado de red, que controle el tráfico entrante y saliente de información?

1	2	3	4	5
◯	◯	◯	◯	◯

24. ¿Realizan pruebas periódicas de intrusión y seguridad del sistemas que determinen la adecuada protección de la red y del sistema?

1	2	3	4	5
◯	◯	◯	◯	◯

25. ¿La organización tiene establecido e implementado el cifrado de la información?

1	2	3	4	5
◯	◯	◯	◯	◯

26. ¿El equipamiento de red se encuentra configurado de forma segura?

1	2	3	4	5
◯	◯	◯	◯	◯

27. ¿Se tiene establecidas políticas, procedimientos, controles y acuerdos para el intercambio de la información y del software?

- ◯ Sí
- ◯ No

28. ¿Se restringe el uso de dispositivos externos?

- ◯ Sí
- ◯ No

29. ¿La organización tiene definido e implementado los procedimientos para el acceso físico y lógico a los activos de TI?

- ◯ Sí
- ◯ No

30. ¿Revisan regularmente los registros de los eventos relacionados con la seguridad reportados por las herramientas de monitoreo que permitan detectar incidentes potenciales?

- ◯ Sí
- ◯ No

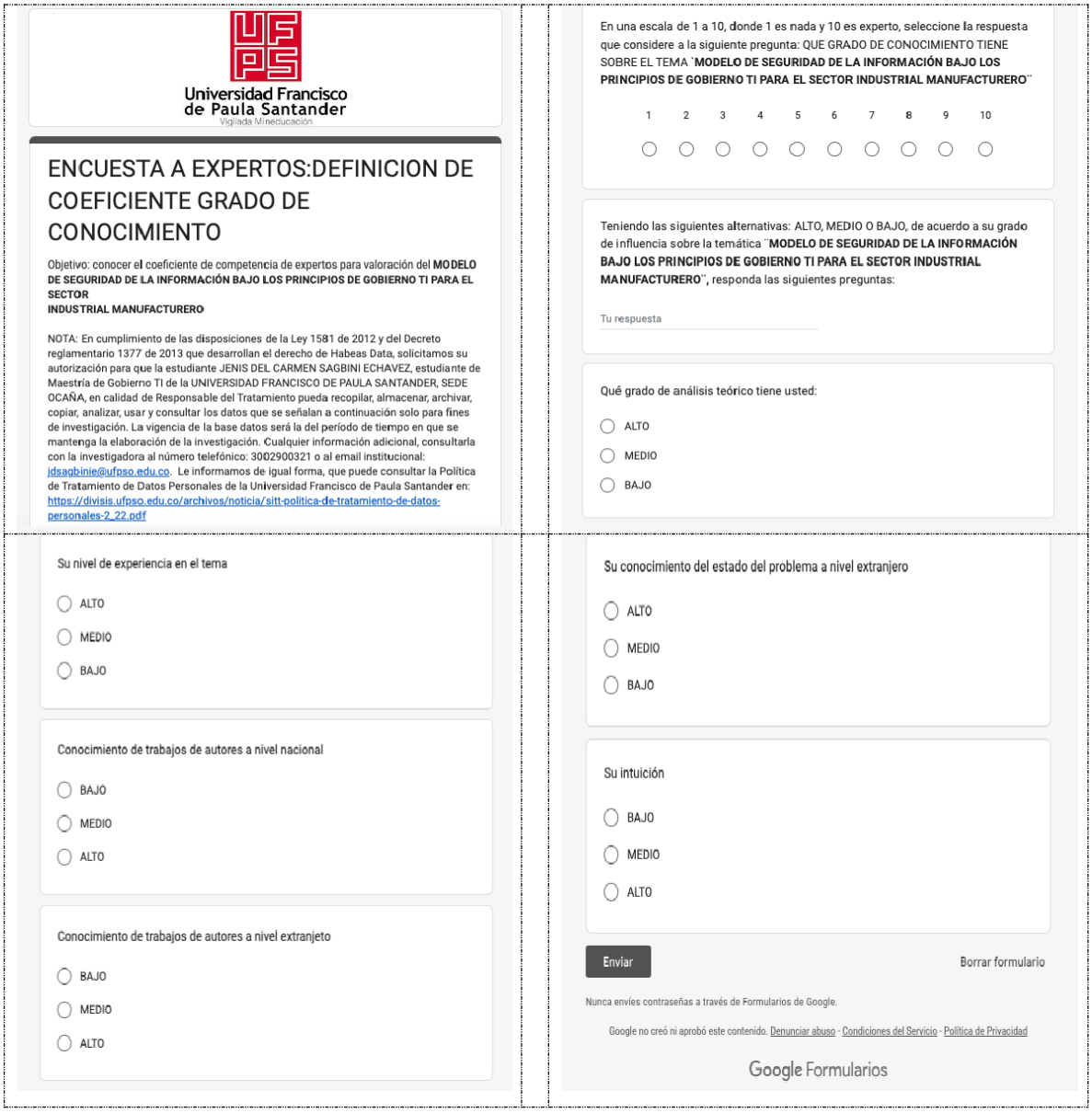
31. ¿Se gestionan los documentos sensibles y dispositivos de salida?

- ◯ Sí
- ◯ No

Atrás | Enviar | Borrar formulario

Apéndice B

https://forms.gle/7HwAPdGjN9bxWMmh7



Universidad Francisco de Paula Santander
Vigilada Mineducación

ENCUESTA A EXPERTOS:DEFINICION DE COEFICIENTE GRADO DE CONOCIMIENTO

Objetivo: conocer el coeficiente de competencia de expertos para valoración del **MODELO DE SEGURIDAD DE LA INFORMACIÓN BAJO LOS PRINCIPIOS DE GOBIERNO TI PARA EL SECTOR INDUSTRIAL MANUFACTURERO**

NOTA: En cumplimiento de las disposiciones de la Ley 1581 de 2012 y del Decreto reglamentario 1377 de 2013 que desarrollan el derecho de Habeas Data, solicitamos su autorización para que la estudiante JENIS DEL CARMEN SAGBINI ECHAVEZ, estudiante de Maestría de Gobierno TI de la UNIVERSIDAD FRANCISCO DE PAULA SANTANDER, SEDE OCAÑA, en calidad de Responsable del Tratamiento pueda recopilar, almacenar, archivar, copiar, analizar, usar y consultar los datos que se señalan a continuación solo para fines de investigación. La vigencia de la base datos será la del período de tiempo en que se mantenga la elaboración de la investigación. Cualquier información adicional, consultarla con la investigadora al número telefónico: 3002900321 o al email institucional: jdsagbinie@ufpso.edu.co. Le informamos de igual forma, que puede consultar la Política de Tratamiento de Datos Personales de la Universidad Francisco de Paula Santander en: https://divisis.ufpso.edu.co/archivos/noticia/sitt-politica-de-tratamiento-de-datos-personales-2_22.pdf

En una escala de 1 a 10, donde 1 es nada y 10 es experto, seleccione la respuesta que considere a la siguiente pregunta: QUE GRADO DE CONOCIMIENTO TIENE SOBRE EL TEMA `**MODELO DE SEGURIDAD DE LA INFORMACIÓN BAJO LOS PRINCIPIOS DE GOBIERNO TI PARA EL SECTOR INDUSTRIAL MANUFACTURERO**¨

1 2 3 4 5 6 7 8 9 10

Teniendo las siguientes alternativas: ALTO, MEDIO O BAJO, de acuerdo a su grado de influencia sobre la temática ¨**MODELO DE SEGURIDAD DE LA INFORMACIÓN BAJO LOS PRINCIPIOS DE GOBIERNO TI PARA EL SECTOR INDUSTRIAL MANUFACTURERO**¨, responda las siguientes preguntas:

Tu respuesta

Qué grado de análisis teórico tiene usted:

- ALTO
- MEDIO
- BAJO

Su nivel de experiencia en el tema

- ALTO
- MEDIO
- BAJO

Conocimiento de trabajos de autores a nivel nacional

- BAJO
- MEDIO
- ALTO

Conocimiento de trabajos de autores a nivel extranjeto

- BAJO
- MEDIO
- ALTO

Su conocimiento del estado del problema a nivel extranjero

- ALTO
- MEDIO
- BAJO

Su intuición

- BAJO
- MEDIO
- ALTO

Enviar Borrar formulario

Nunca envíes contraseñas a través de Formularios de Google.

Google no creó ni aprobó este contenido. Denunciar abuso · Condiciones del Servicio · Política de Privacidad

Google Formularios

Apéndice C

Validación del modelo propuesto

https://forms.gle/tXn4FtB54NBh7LzR9

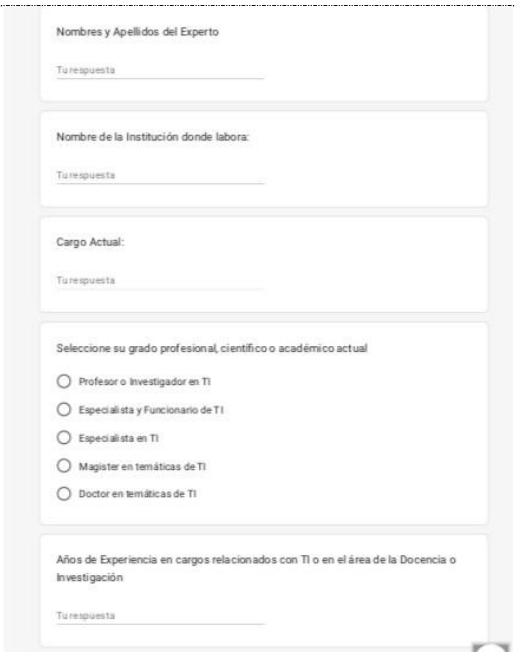
Universidad Francisco de Paula Santander

Vigilada Mineducación

VALIDACION DEL **MODELO DE SEGURIDAD DE LA INFORMACIÓN BAJO LOS PRINCIPIOS DE GOBIERNO TI PARA EL SECTOR INDUSTRIAL MANUFACTURERO**

Objetivo: Validar el modelo propuesto con expertos del tema.

NOTA: En cumplimiento de las disposiciones de la Ley 1581 de 2012 y del Decreto reglamentario 1377 de 2013 que desarrollan el derecho de Habeas Data, solicitamos su autorización para que la estudiante JENIS DEL CARMEN SAGBINI ECHAVEZ, estudiante de Maestría de Gobierno TI de la UNIVERSIDAD FRANCISCO DE PAULA SANTANDER, SEDE OCAÑA, en calidad de Responsable del Tratamiento pueda recopilar, almacenar, archivar, copiar, analizar, usar y consultar los datos que se señalan a continuación solo para fines de investigación. La vigencia de la base datos será la del período de tiempo en que se mantenga la elaboración de la investigación. Cualquier información adicional, consultarla con la investigadora al número telefónico: 3002900321 o al email institucional: jdsagbinie@ufpso.edu.co. Le informamos de igual forma, que puede consultar la Política de Tratamiento de Datos Personales de la Universidad Francisco de Paula Santander en: https://divisis.ufpso.edu.co/archivos/noticia/sitt-politica-de-tratamiento-de-datos-personales-2_22.pdf



Nombres y Apellidos del Experto

Tu respuesta

Nombre de la Institución donde labora:

Tu respuesta

Cargo Actual:

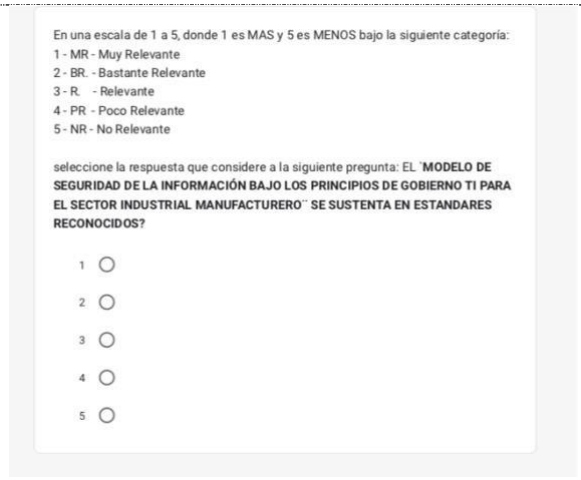
Tu respuesta

Seleccione su grado profesional, científico o académico actual

- Profesor o Investigador en TI
- Especialista y Funcionario de TI
- Especialista en TI
- Magister en temáticas de TI
- Doctor en temáticas de TI

Años de Experiencia en cargos relacionados con TI o en el área de la Docencia o Investigación

Tu respuesta

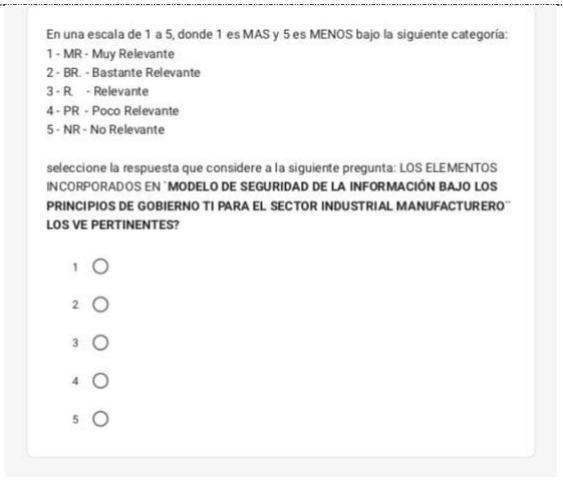


En una escala de 1 a 5, donde 1 es MAS y 5 es MENOS bajo la siguiente categoría:

1 - MR - Muy Relevante
2 - BR. - Bastante Relevante
3 - R. - Relevante
4 - PR - Poco Relevante
5 - NR - No Relevante

seleccione la respuesta que considere a la siguiente pregunta: EL "**MODELO DE SEGURIDAD DE LA INFORMACIÓN BAJO LOS PRINCIPIOS DE GOBIERNO TI PARA EL SECTOR INDUSTRIAL MANUFACTURERO" SE SUSTENTA EN ESTANDARES RECONOCIDOS?**

1 ○
2 ○
3 ○
4 ○
5 ○



En una escala de 1 a 5, donde 1 es MAS y 5 es MENOS bajo la siguiente categoría:

1 - MR - Muy Relevante
2 - BR. - Bastante Relevante
3 - R. - Relevante
4 - PR - Poco Relevante
5 - NR - No Relevante

seleccione la respuesta que considere a la siguiente pregunta: LOS ELEMENTOS INCORPORADOS EN "**MODELO DE SEGURIDAD DE LA INFORMACIÓN BAJO LOS PRINCIPIOS DE GOBIERNO TI PARA EL SECTOR INDUSTRIAL MANUFACTURERO" LOS VE PERTINENTES?**

1 ○
2 ○
3 ○
4 ○
5 ○

En una escala de 1 a 5, donde 1 es MAS y 5 es MENOS bajo la siguiente categoría:
1 - MR - Muy Relevante
2 - BR. - Bastante Relevante
3 - R. - Relevante
4 - PR - Poco Relevante
5 - NR - No Relevante

seleccione la respuesta que considere a la siguiente pregunta: EXISTE UNA CORRESPONDENCIA ENTRE EL `**MODELO DE SEGURIDAD DE LA INFORMACIÓN BAJO LOS PRINCIPIOS DE GOBIERNO TI PARA EL SECTOR INDUSTRIAL MANUFACTURERO`` Y LA DEFINICION?**

1 ○
2 ○
3 ○
4 ○
5 ○

En una escala de 1 a 5, donde 1 es MAS y 5 es MENOS bajo la siguiente categoría:
1 - MR - Muy Relevante
2 - BR. - Bastante Relevante
3 - R. - Relevante
4 - PR - Poco Relevante
5 - NR - No Relevante

seleccione la respuesta que considere a la siguiente pregunta: EL `**MODELO DE SEGURIDAD DE LA INFORMACIÓN BAJO LOS PRINCIPIOS DE GOBIERNO TI PARA EL SECTOR INDUSTRIAL MANUFACTURERO`` PODRIA SER ADAPTADO EN UNA EMPRESA DEL SECTOR PRODUCTIVO MANUFACTURERO?**

1 ○
2 ○
3 ○
4 ○
5 ○

En una escala de 1 a 5, donde 1 es MAS y 5 es MENOS bajo la siguiente categoría:
1 - MR - Muy Relevante
2 - BR. - Bastante Relevante
3 - R. - Relevante
4 - PR - Poco Relevante
5 - NR - No Relevante

seleccione la respuesta que considere a la siguiente pregunta: **HAY COHERENCIA ENTRE LOS COMPONENTES DEL MODELO PROPUESTO?**

1 ○
2 ○
3 ○
4 ○
5 ○

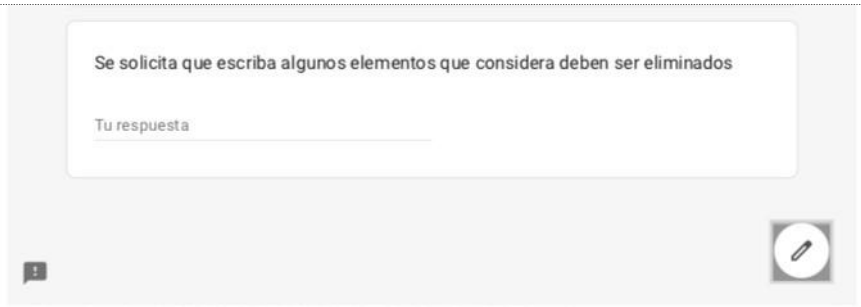
En una escala de 1 a 5, donde 1 es MAS y 5 es MENOS bajo la siguiente categoría:
1 - MR - Muy Relevante
2 - BR. - Bastante Relevante
3 - R. - Relevante
4 - PR - Poco Relevante
5 - NR - No Relevante

seleccione la respuesta que considere a la siguiente pregunta: **HAY UNA CORRESPONDENCIA ENTRE LOS ELEMENTOS ESTRUCTURALES DEL MODELO, SUS OBJETIVOS Y SUS CARACTERISTICAS?**

1 ○
2 ○
3 ○
4 ○
5 ○

Se solicita que escriba fases o elementos que considera deberían incluirse en la presente propuesta.

Tu respuesta


Se solicita que escriba algunos elementos que considera deben ser eliminados
Tu respuesta


Se solicita que escriba fases o elementos que considera deberían ser cambiados en la presente propuesta.
Tu respuesta
Enviar
Borrar formulario
Nunca envíes contraseñas a través de Formularios de Google.
Google no creó ni aprobó este contenido. Denunciar abuso - Condiciones del Servicio - Política de Privacidad
Google Formularios