INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

DISEÑO DEL PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI) PARA ENTIDADES DE ORDEN NACIONAL

Presenta
Daissy Janneth Mesa López Cód. 1712010135
Leonardo Favio Pérez López Cód. 1712010071

ASESOR TEMÁTICO:
WILMAR JAIMES FERNÁNDEZ
MAGISTER EN INGENIERÍA ELECTRÓNICA Y DE COMPUTADORES

Mayo, 2018

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

RESUMEN

Nuestro proyecto tiene como fin el desarrollo de un plan estratégico de seguridad de la información (PESI) para entidades de orden nacional. Mediante mecanismos de seguimiento y análisis al estado actual de las organizaciones al perfilarse hacia una seguridad de la información, se propone un plan estratégico para lograr en corto plazo la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) de acuerdo con el Decreto 1078 de 2015. Para efectos de este proyecto se seleccionaron tres (3) entidades de orden nacional a las cuales se les realizó un análisis y cuyos resultados fueron la base para el desarrollo del PESI.

ABSTRACT

Our project aims to develop a strategic plan for information security (PESI) for national entities. Through monitoring mechanisms and analysis of the current state of the entities in the framework of information security, a strategic plan for the short term is offered, the implementation of the Information Security Management System (ISMS) according to Decree 1078 of 2015. For the purposes of this project, three (3) national entities were selected, which were analyzed and whose results were the basis for the development of the PESI.

PALABRAS CLAVE

Modelo de Seguridad y Privacidad de la Información (MSPI).
Gestión de TI.
Entidades Públicas.
Sistema de Gestión de Seguridad de la Información (SGSI).
Seguridad de la Información.

KEY WORDS

Information Security and Privacy Model (ISPM).
IT management.
Public entities
Information Security Management System (ISMS).
Information Security.

INTRODUCCIÓN

El Gobierno en línea en Colombia ha implementado de una manera coordinada el uso de la tecnología en todas las entidades públicas. En los últimos años, se han evidenciado cambios y avances en el uso y apropiación de la tecnología como herramienta que ayuden a mejorar la gestión pública, la provisión de servicios y la transparencia, con el fin de cumplir las funciones del Estado (Salas, 2011).

Con lo anterior, el Gobierno Nacional reglamenta el MSPI (Modelo de Seguridad y Privacidad de la Información) a través del Decreto 1078 de 2015 para que todas las entidades de Orden Nacional lo implementen en el plazo establecido.

Este proyecto se divide en tres partes, en la primera se realizará el *Análisis de diagnóstico desde el modelo de planeación estratégica situacional* para llegar a la *descripción de la situación de interés,* identificando *la red de actores relevantes tanto internos como externos* y *las causas que originan la situación problema.* Asimismo, se identificarán los *indicadores* que soportan la situación problema. Adicionalmente se realizará el Análisis de prospectiva y viabilidad de las acciones formuladas como respuesta a la situación de interés, para lo cual se diseñará una matriz para la valoración estratégica y táctica.

En la segunda parte, se recopilará los resultados del análisis diagnóstico, la descripción de la situación de interés y la red de actores relevantes con el fin de plantear el problema de la propuesta. Se continuará con la construcción de la justificación a partir de los indicadores identificados, se proyectarán los objetivos, se establecerán los límites del proyecto y las actividades que componen el plan de trabajo.

La tercera y última parte está enfocada a la puesta en marcha del plan de trabajo propuesto, enmarcado en la selección de tres (3) entidades de orden nacional, el análisis GAP a dichas entidades, el diseño de la herramienta PESI, la evaluación de los resultados de su aplicación y las conclusiones donde se confirma la eficacia del plan.

1. ANÁLISIS DIAGNÓSTICO DESDE EL MODELO DE PLANEACIÓN ESTRATÉGICA SITUACIONAL

El Gobierno de Colombia, mediante el documento CONPES 3701 del 14 de julio de 2011, instauró la Estrategia Nacional de Ciberseguridad y Ciberdefensa, para adoptar medidas que contemplen la seguridad de la información de todos los individuos frente a las amenazas que se presentan día a día de tipo informáticas, creando obligaciones que debe cumplir el Ministerio de las TIC con las diferentes entidades respecto al desarrollo de estrategias, planes, políticas, formaciones y sensibilización en todo lo referente a la seguridad de la información.

Con la creación y adaptación del decreto 2618 del 2012, se reformuló el diseño del Ministerio de las TIC, se creó la Subdirección de Seguridad y Privacidad de TI y se le atribuyeron facultades al Ministerio de las TIC, el cual tendría la obligación de crear estrategias de implementación y evaluación del modelo de seguridad y privacidad de la información, en todas las entidades del Estado.

Posteriormente el 12 de diciembre de 2014 se expide el decreto 2573, en el cual se constituyen las directrices generales de la estrategia de Gobierno el Línea, y cuyo objetivo es “Definir los lineamientos, instrumentos y plazos de la estrategia de Gobierno en línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que preste mejores servicios con la colaboración de toda la sociedad” (MinTIC, 2014). Así mismo el 26 de mayo del año 2015, se expidió el Decreto 1078, “Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las comunicaciones” (“Decreto Único Reglamentario del Sector TIC - Decreto 1078 del 26 de mayo de 2015,” n.d.).

En efecto para el año 2016, las entidades adscritas al Orden Nacional debían implementar las actividades establecidas en el Manual de Seguridad y Privacidad de la información, en adelante MSPI, en los siguientes plazos y porcentajes:

Componente/Año	2015	2016	2017	2018	2019	2020
Seguridad y privacidad de la información	40%	60%	80%	100%	Mantener el 100%	Mantener el 100%

Tabla 1. Plazos y porcentajes Decreto 2573 de 2014

A continuación, se detalla los componentes del MSPI y su porcentaje:

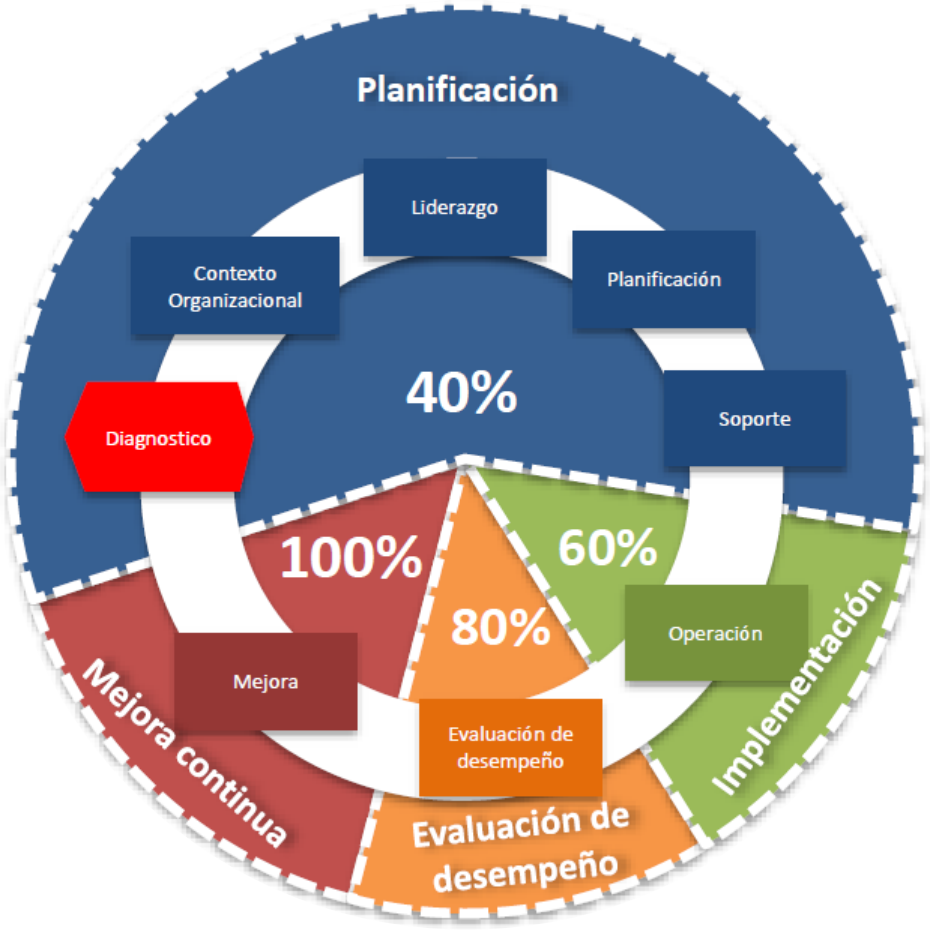


Ilustración 1. Fases del MSPI Fuente: MSPI

COMPONENTE DE PLANIFICACIÓN

En este componente se define una metodología que permite establecer los objetivos generales y específicos, así como también el alcance, los procesos y los procedimientos necesarios que

permitan una mejor gestión de los riesgos y aplicar los correctivos necesarios para asegurar la información, con el fin de lograr los resultados que proporcionen lograr cumplir con las metas propuestas del MSPI.

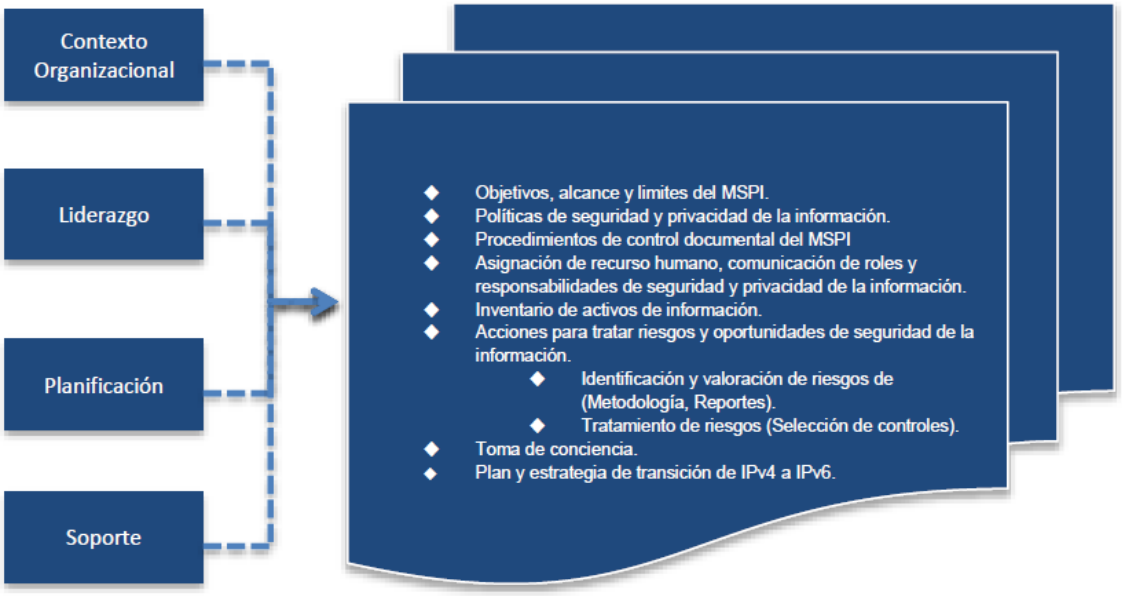


Ilustración 2. Componente de Planificación Fuente: MSPI

COMPONENTE DE IMPLEMENTACIÓN

Para este componente la Entidad llevará a cabo la planificación del MSPI, validando los aspectos más relevantes en la evolución para la implementación del MSPI. Así al culminar la definición del Modelo de Operación de Seguridad y Privacidad de la Información (MSPI), y con la competencia de saber identificar las necesidades de la Entidad, se procede con el desarrollo del plan de Implementación del MSPI.

El objetivo de este componente es analizar, diseñar y ejecutar de manera específica la estrategia del sistema de gestión. Para esta estrategia se deben definir roles y actividades indispensables para lograr cumplir con las metas ya establecidas y lograr la implementación y ejecución del MSPI en la Entidad, de una forma organizada y planificada se pueden abarcar todo el proceso de gestión en la organización teniendo en cuenta su ambiente identificado en el primer componente de planificación.

Ilustración 3. Componente de Implementación Fuente: MSPI

1.1. DESCRIPCIÓN DE LA SITUACIÓN DE INTERÉS

Para el cierre del año 2016 sólo el **46%** de las entidades adscritas al Orden Nacional cumplieron con el **60%** del componente de implementación del Modelo de Seguridad y Privacidad de la Información establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones a través del Decreto 1078 de 2015.

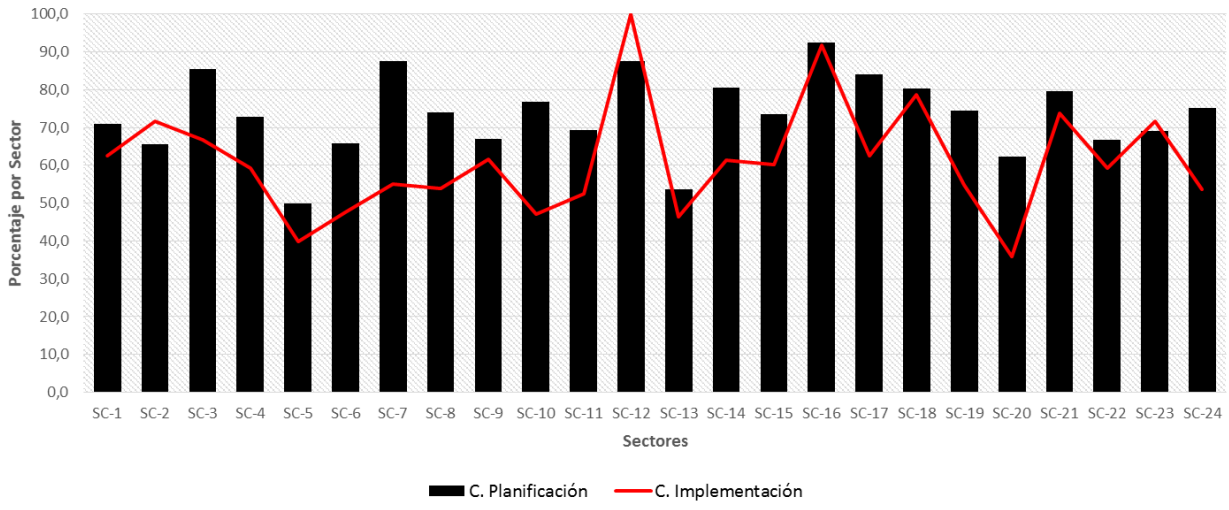


Ilustración 4. Cumplimiento por Sector para el año 2016 (FURAG, 2017)

Como se observa en el gráfico anterior, la mayoría de las entidades cumplieron el **40%** requerido para el componente de planificación, sin embargo, sólo un **13%** de ellas implementaron el 60% de dicha planificación. A continuación, se presenta el detalle por sector:

Código	Sector	Porcentaje de Planificación	Porcentaje de Implementación
SC-1	Agricultura y Desarrollo Rural	71,1	62,6

Código	Sector	Porcentaje de Planificación	Porcentaje de Implementación
SC-2	Ambiente y Desarrollo Sostenible	65,6	71,7
SC-3	Ciencia, Tecnología e innovación	85,4	66,7
SC-4	Comercio, Industria y Turismo	72,8	59,3
SC-5	Cultura	49,8	39,8
SC-6	Defensa	65,8	47,5
SC-7	Del Deporte, la Recreación, la Actividad Física y el Aprovechamiento del Tiempo Libre	87,5	55,0
SC-8	Educación	74,1	53,9
SC-9	Estadísticas	67,0	61,7
SC-10	Función Pública	76,7	47,1
SC-11	Hacienda y Crédito Público	69,2	52,5
SC-12	Inteligencia Estratégica y Contrainteligencia	87,5	100,0
SC-13	Interior	53,7	46,4
SC-14	Justicia y del Derecho	80,6	61,3
SC-15	Minas y Energía	73,5	60,1
SC-16	Planeación	92,5	91,7
SC-17	Presidencia de la República	84,0	62,5
SC-18	Relaciones Exteriores	80,2	78,8
SC-19	Salud y Protección Social	74,4	54,9
SC-20	Tecnologías de la Información y las Comunicaciones	62,4	36,0
SC-21	Trabajo	79,5	73,8
SC-22	Transporte	66,8	59,2
SC-23	Vivienda Ciudad y Territorio	69,0	71,7
SC-24	Inclusión Social y Reconciliación	75,2	53,8

Tabla 2. Porcentaje de cumplimiento por Sector (FURAG, 2017)

1.2. CADENAS CAUSALES DE LA SITUACIÓN PROBLEMA

A continuación, se describen las principales causas de la situación problema, de acuerdo con los diferentes actores identificados que inciden o son afectados por la situación problema:

Actor	Descripción de la causa
MinTic	✓ Capacitación insuficiente para la implementación del MSPI

Actor	Descripción de la causa
Entidades de Orden Nacional	✓ Falta de planificación para la implementación del MSPI ✓ Procesos de contratación demorados
Gerente General	✓ Falta de compromiso y liderazgo
Consejo Directivo	✓ Apoyo insuficiente en las actividades de implementación
Planeación	✓ Reprocesos que obstaculizan la implementación del MSPI
Gerente de TI	✓ Sobrecarga laboral
Líderes de proceso	✓ Desconocimiento del proyecto del MSPI
Líderes u Oficiales de SI	✓ Autoridad delegada insuficiente
Funcionario	✓ Alta resistencia al cambio
Contratista	✓ Alta rotación anual de contratistas
Firmas consultoras externas	✓ Contrataciones con tiempos insuficientes para la implementación del MPSI
Asesores y Consultores externos	✓ Autoridad insuficiente para la toma de decisiones

Tabla 3. Autoridades y causas de la situación problema

1.3. FLUJOGRAMA EXPLICATIVO

En adelante se presenta el flujograma explicativo con las cadenas causales:

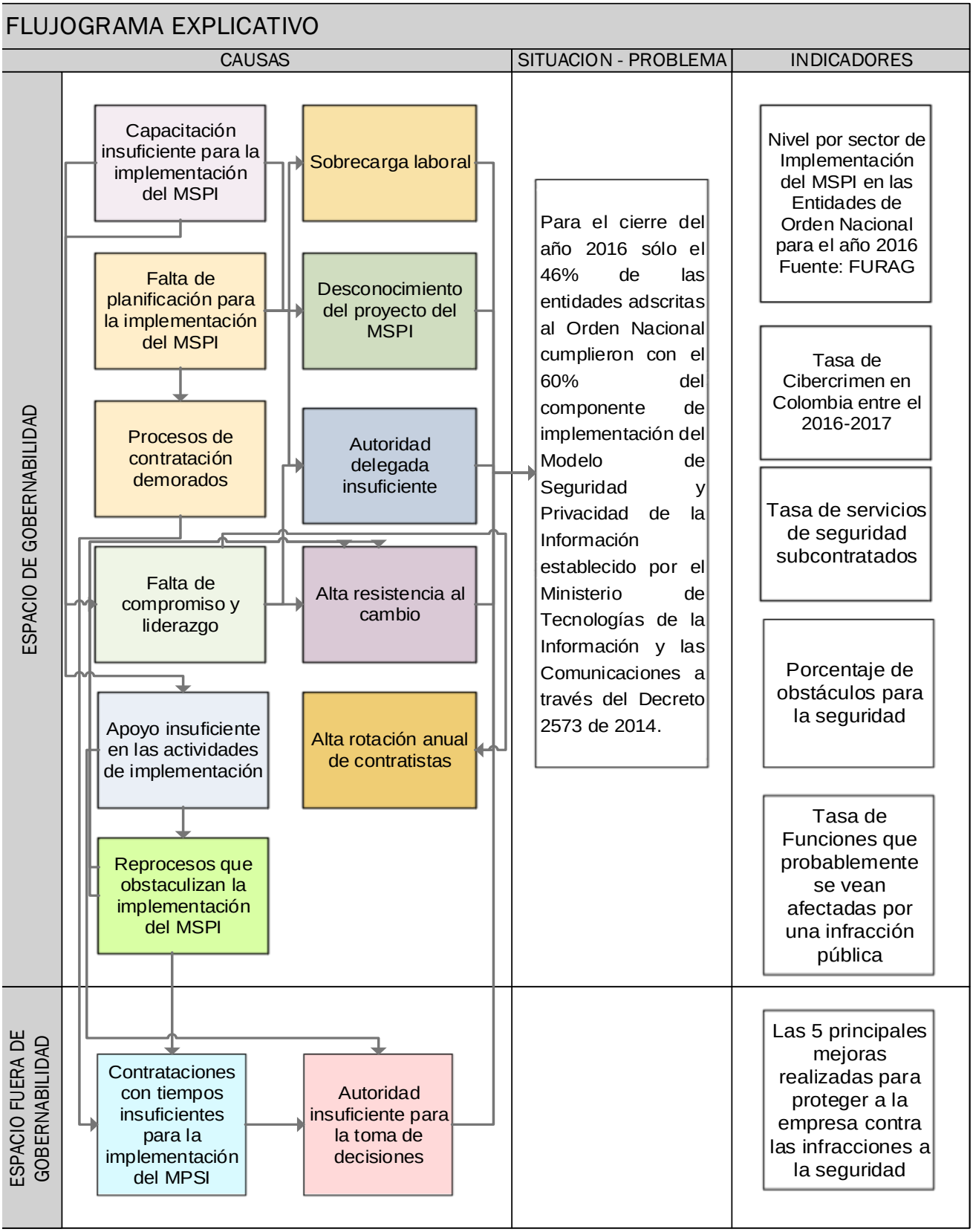


Ilustración 5. Flujograma Explicativo

1.4. TABLA DE INDICADORES

A continuación, se presentan los indicadores que soportar el análisis de la situación problema:

No.	Nombre del Indicador	Valor	Descripción	Fuente
1	Nivel por sector de Implementación del MSPI en las Entidades de Orden Nacional para el año 2016	~46%	Para el cierre del año 2016 sólo el 46% de las entidades adscritas al Orden Nacional cumplieron con el 60% del componente de implementación del Modelo de Seguridad y Privacidad de la Información establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones a través del Decreto 1078 de 2015	FURAG (2017)
2	Tasa de Cibercrimen en Colombia entre el 2015-2016	~15%	El Cibercrimen representa el 15 por ciento de los ilícitos cometidos a empresas en Colombia y generó un daño económico cercano a 600 millones de dólares en el último año.	Intel Security (2016)
3	Tasa de servicios de seguridad subcontratados	~55%	Las grandes empresas son mucho más propensas a subcontratar las auditorias, el asesoramiento y la consultoría.	CISCO (2017)
4	Porcentaje de obstáculos para la seguridad	~35%	En el 2016, el 35 % de los profesionales de seguridad dijo que el presupuesto era el obstáculo más grande para adoptar procesos y tecnología de seguridad avanzada.	CISCO (2017)

No.	Nombre del Indicador	Valor	Descripción	Fuente
5	Tasa de Funciones que probablemente se vean afectadas por una infracción pública	~36%	El 36 % de los profesionales de seguridad dijo que las operaciones fueron la función con más probabilidades de verse afectadas.	CISCO (2017)
6	Las 5 principales mejoras realizadas para proteger a la empresa contra las infracciones a la seguridad	~38%	De las organizaciones afectadas por infracciones, el 38 % afirmó que respondió dividiendo al equipo de seguridad del departamento de TI.	CISCO (2017)

Tabla 4. Indicadores que soportan el análisis de la situación problema

1.4.1. Nivel por sector de Implementación del MSPI en las Entidades de Orden Nacional para el año 2016

A través del instrumento de medición establecido por el FURAG (Modelo Integrado de Planeación y Gestión) las entidades de orden nacional fueron evaluadas con el fin de identificar su nivel de cumplimiento frente al componente de implementación (**60%**) establecido para el año 2016 en lo referente al MSPI.

A continuación, se presenta una gráfica de alto nivel en donde se observa el cumplimiento por sector:

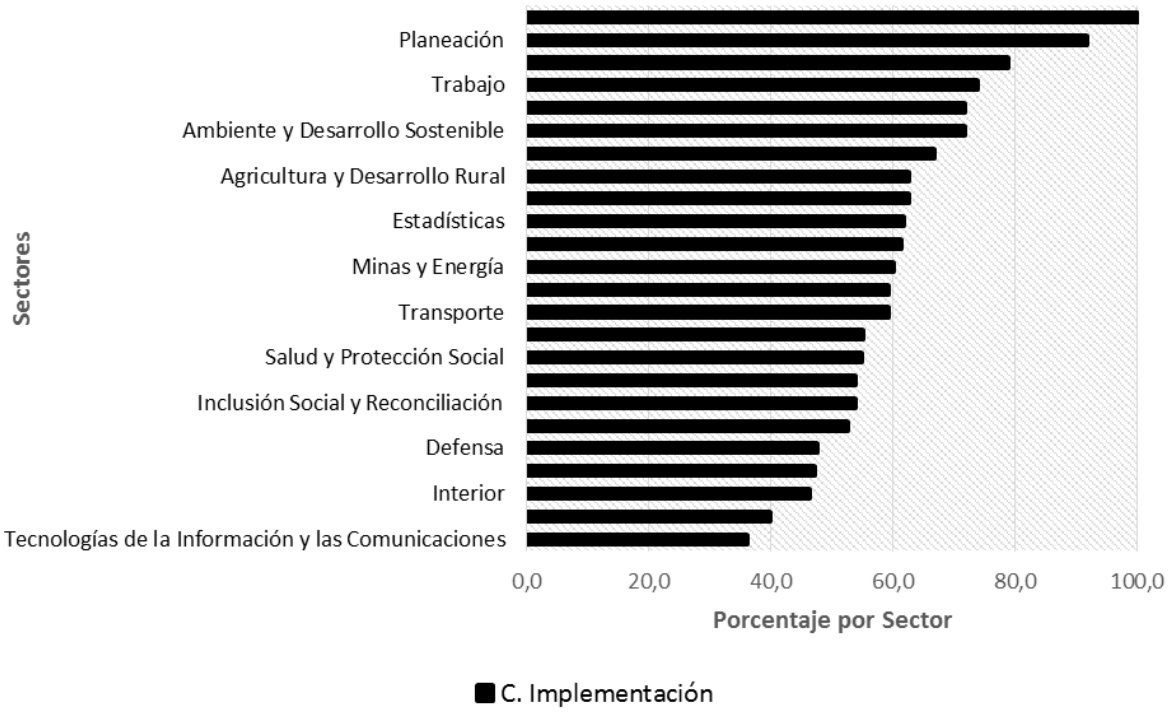


Ilustración 6. Nivel por sector de Implementación del MSPI en las Entidades de Orden Nacional para el año 2016 (FURAG, 2017)

1.4.2. Tasa de Cibercrimen en Colombia entre el 2015-2016

El Cibercrimen representa el 15 por ciento de los ilícitos cometidos a empresas en Colombia y generó un daño económico cercano a 600 millones de dólares en el último año, reveló Intel Security. (El Tiempo, 2016). Lo anterior representa una amenaza que crece continuamente para las entidades de orden nacional que no han llegado al porcentaje requerido en la implementación del MSPI, el cual da los lineamientos para evitar este tipo de incidentes que puedan afectar la reputación y/o las finanzas de las entidades públicas.

En la siguiente ilustración se observa los delitos informáticos más representativos en nuestro país:

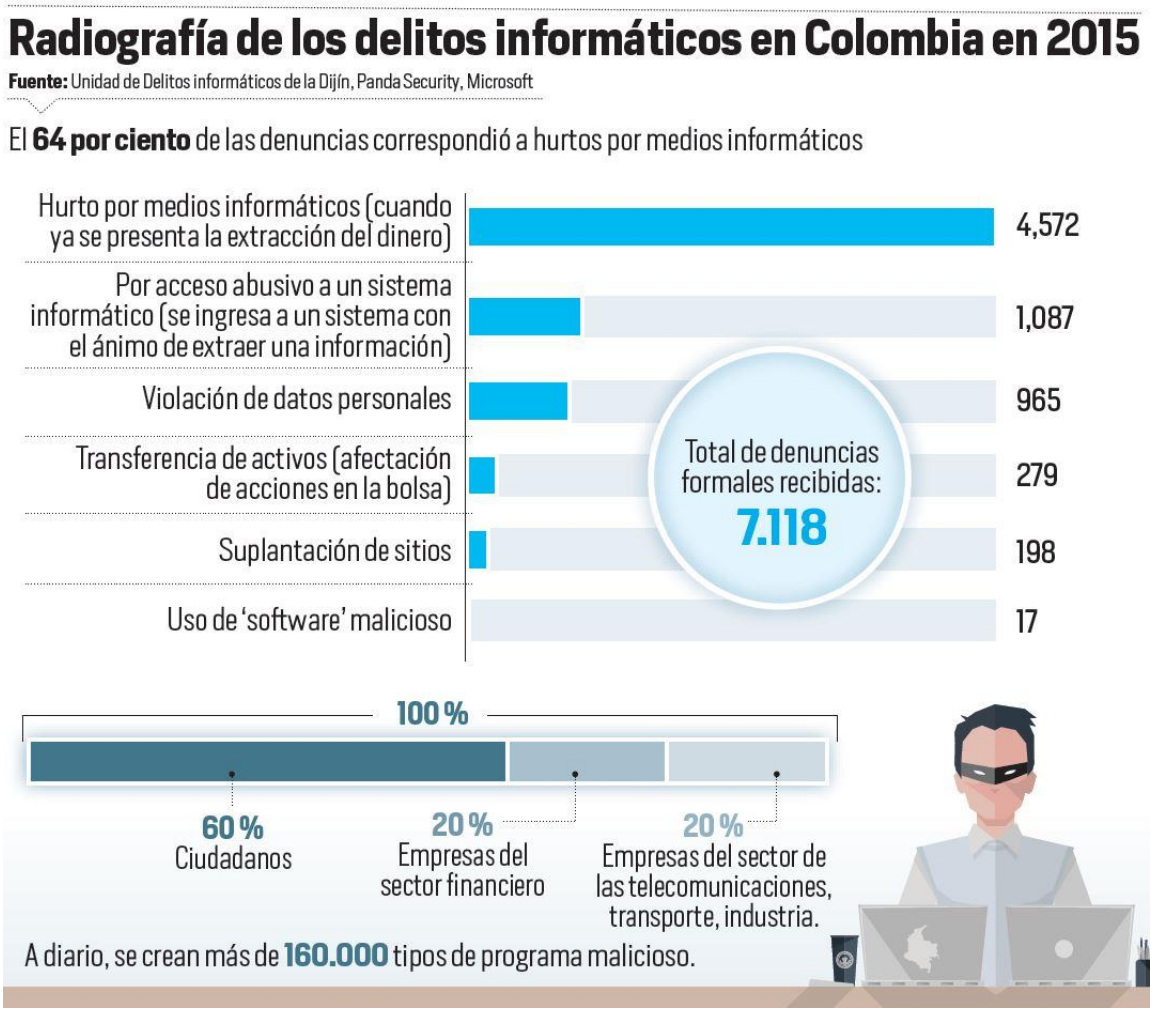


Ilustración 7. Radiografía de los delitos informáticos en Colombia en 2015 (El Tiempo, 2016)

Durante el 2016 hubo un incremento del 114.4% en ataques de malware en el país, en relación al 2015 (153 incidentes reportados en el 2015, 328 incidentes reportados en el 2016).(POLICIA NACIONAL DE COLOMBIA, 2017)

1.4.3. Tasa de servicios de seguridad subcontratados

Las grandes empresas son mucho más propensas a subcontratar las auditorias, el asesoramiento y la consultoría. A continuación, se exponen los resultados de una encuesta realizada con el fin de identificar qué servicios de seguridad se subcontratan:

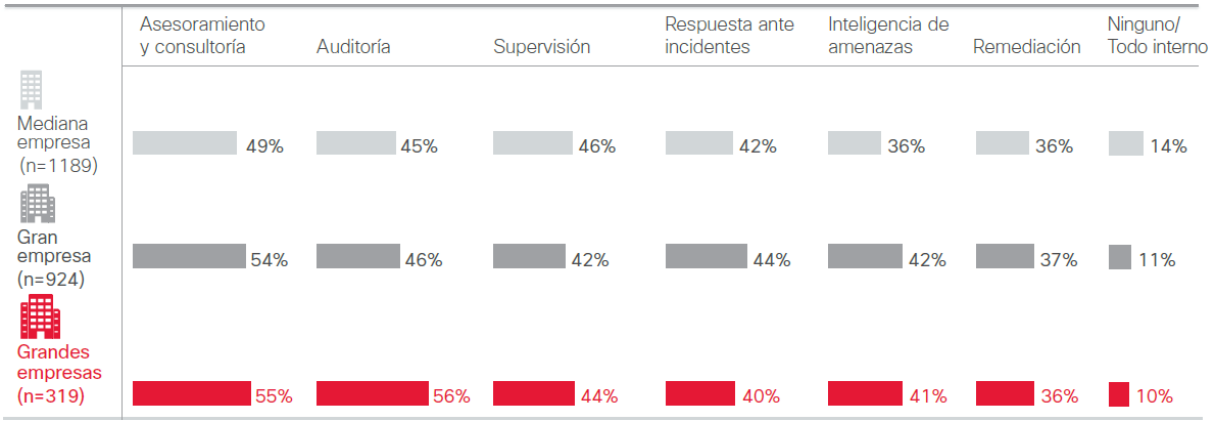


Ilustración 8. Tasa de servicios de seguridad subcontratados (CISCO, Informe Anual de Seguridad 2016, 2017)

El hecho de que cada vez más las entidades adopten la subcontratación como una forma de gestionar la seguridad es una buena noticia. Indica que las entidades buscan herramientas flexibles para proteger las redes que no supongan una carga para su menor número de empleados o para presupuestos más conservadores. Sin embargo, las entidades pueden creer de manera equivocada que los procesos de subcontratación de seguridad reducirán considerablemente la posibilidad de que se produzca una brecha en la red. O pueden trasladar la responsabilidad de la seguridad a un tercero. Este punto de vista sería una ilusión, ya que solo un sistema de defensa contra amenazas verdaderamente integrado, que analice y mitigue los ataques al mismo tiempo que los evite, puede ofrecer una protección de seguridad de nivel empresarial. (CISCO, Informe Anual de Seguridad 2016, 2017)

1.4.4. Porcentaje de obstáculos para la seguridad

En el 2016, el 35 % de los profesionales de seguridad dijo que el presupuesto era el obstáculo más grande para adoptar procesos y tecnología de seguridad avanzada. (CISCO, Informe Anual sobre Ciberseguridad 2017, 2017)

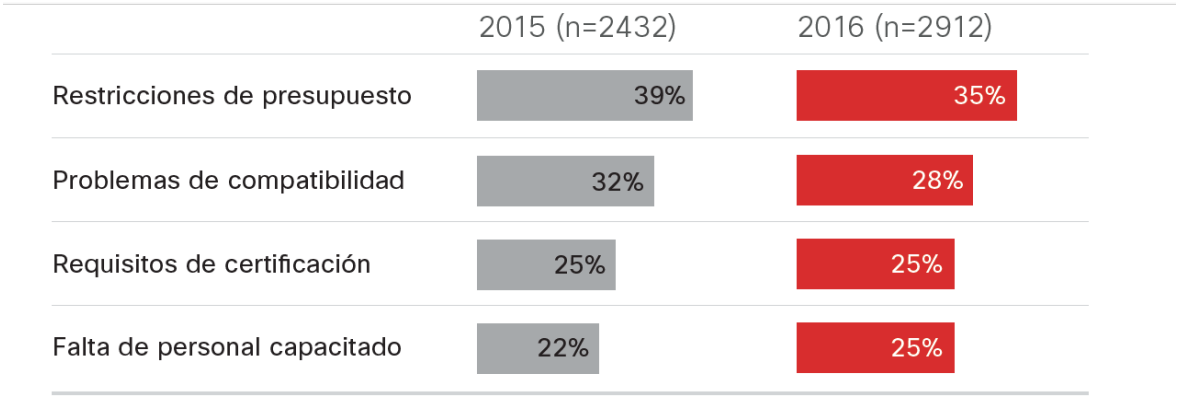


Ilustración 9 . Porcentaje de obstáculos para la seguridad (CISCO, Informe Anual sobre Ciberseguridad 2017, 2017)

1.4.5. Tasa de Funciones que probablemente se vean afectadas por una infracción pública

El 36 % de los profesionales de seguridad dijo que las operaciones fueron la función con más probabilidades de verse afectadas. Esto significa que los sistemas centrales de productividad, que afectan a distintos sectores (desde transporte hasta servicios de salud y fabricación), pueden volverse lentos o incluso detenerse. A las operaciones les siguen las finanzas como función con más probabilidades de verse afectada (mencionada por el 30 % de los encuestados), seguida por la reputación de la marca y la retención de clientes (26 % en ambos casos). (CISCO, Informe Anual sobre Ciberseguridad 2017, 2017)

Ilustración 10. Tasa de Funciones que probablemente se vean afectadas por una infracción pública (CISCO, Informe Anual sobre Ciberseguridad 2017, 2017)

1.4.6. Las 5 principales mejoras realizadas para proteger a la empresa contra las infracciones a la seguridad

De las organizaciones afectadas por infracciones, el 38 % afirmó que respondió dividiendo al equipo de seguridad del departamento de TI; el 38 % dijo que aumentó la capacitación sobre el conocimiento de la seguridad entre los empleados; y el 37 % afirmó que aumentó su enfoque para el análisis y la mitigación de riesgos. (CISCO, Informe Anual sobre Ciberseguridad 2017, 2017)

Ilustración 11. Las 5 principales mejoras realizadas para proteger a la empresa contra las infracciones a la seguridad (CISCO, Informe Anual sobre Ciberseguridad 2017, 2017)

1.5. FORMULACIÓN DE LA SITUACIÓN DESEADA

ANÁLISIS DE PROSPECTIVA Y VIABILIDAD

Para el ejercicio prospectivo, se trabajarán dos escenarios: el optimista y la situación deseada.

1.5.1. ESCENARIO OPTIMISTA

Horizonte de tiempo: 3 años

Las entidades del Orden Nacional para el año 2020, logran implementar y mantener el 100% el modelo de seguridad y privacidad de la información gracias a los siguientes hechos:

- El MinTic fortaleció sus programas de capacitación en cada entidad.
- Las entidades de orden nacional realizaron una adecuada planificación para la implementación del MSPI.
- Las entidades de orden nacional ejecutaron procesos de contratación más agiles.
- La Gerencia General de cada entidad incrementó su compromiso y liderazgo, el modelo MSPI pasó a ser uno de los principales proyectos del Plan Estratégico Institucional.
- El consejo directivo de cada entidad aumentó su apoyo a la implementación del modelo MSPI.
- Desde la planificación, las entidades involucraron las áreas de planeación y trabajaron de la mano del Líder u Oficial del SI, con procesos más agiles que facilitaron la implementación del MSPI.
- El Gerente de TI dejó de ser el responsable del modelo MSPI, la entidad creó un cargo propio para el modelo que reporta depende y reporta directamente a la Gerencia General.
- Las entidades fortalecieron los planes de comunicación, sensibilización y concientización a todas las partes interesadas.
- El Líder u Oficial del SI pasó a ser un cargo formal en la entidad y depende directamente de la Gerencia General.
- Los funcionarios entendieron la importancia del modelo MSPI y acogieron los cambios que este involucraba.
- El gobierno emitió una resolución para que el modelo anual de contratación pasará a mantener los contratistas por lo menos durante 2 años.
- Las firmas consultoras entregaron implementaciones más reales, acordes y eficaces a cada entidad.
- Los asesores y consultores externos trabajaron de la mano del Líder u Oficial de SI, y lograron aprobaciones más rápidas por parte de la Gerencia General.

1.5.2. ANÁLISIS DE LA SITUACIÓN DESEADA

Horizonte de tiempo: 3 años

Las entidades del Orden Nacional para el año 2020, logran implementar y mantener el 100% el modelo de seguridad y privacidad. En efecto, la situación a la que se quiere llegar con la

implementación de este proyecto es donde las entidades de orden nacional logren cumplir el porcentaje pactado por el Gobierno Nacional a través del Decreto 1078 de 2015 para el año 2020. Lo anterior se alcanzará, identificando inicialmente las variables o acciones internas (que están al alcance de la gobernabilidad de los actores) y externas (que están fuera del alcance de gobernabilidad de los actores), y valorándolas teniendo en cuenta su viabilidad, impacto y gobernabilidad.

VARIABLES O ACCIONES

A continuación, se listan las variables o acciones identificadas para cambiar la situación actual en una situación deseada u optimista:

No.	Variable o Acción	Tipo
1	✓ Intervenir las entidades con un cumplimiento por debajo del 60% fortaleciendo los planes de capacitación y entrenamiento en el MSPI.	✓ Interno
2	✓ Crear el PESI (Plan estratégico de seguridad de la información)	✓ Interno
3	✓ Mejorar el alcance y las especificaciones de los procesos licitatorios, aterrizarlos a la realidad	✓ Interno
4	✓ Crear un cargo al interior de la entidad que responda al rol de Líder u Oficial de SI independiente de las demás áreas y dependiente de la Gerencia General.	✓ Interno
4	✓ Incluir en las responsabilidades de los directivos la gestión de seguridad de la información al interior de sus áreas.	✓ Interno
5	✓ Involucrar a planeación desde la planificación del proyecto, asignando un representante que acompañe y apoye al Líder u Oficial del SI en la implementación del MSPI.	✓ Interno
6	✓ Asignar un representante de TI para que apoye al Líder u Oficial del SI en la implementación del modelo MSPI.	✓ Interno
7	✓ Fortalecer los planes de capacitación y divulgación del modelo MSPI	✓ Interno
8	✓ Adicionar al Comité directivo las actividades de revisión y aprobación del modelo MSPI.	✓ Interno

No.	Variable o Acción	Tipo
9	✓ Aplicar un modelo de gestión de cambio para funcionarios y contratistas	✓ Interno
10	✓ Modificar el tiempo limitado de los contratos por prestación de servicios de un año a dos años.	✓ Externo
11	✓ Licitar contratos de implementación del MSPI no menores a un año.	✓ Interno

Tabla 5. Variables internas y externas

1.6. MATRIZ DE VALORACIÓN ESTRATÉGICA

A continuación, se realiza la evaluación de las acciones propuestas frente a las causas de la situación problema, realizando la valoración bajo los siguientes criterios: ***impacto*** (consecuencia sobre la causa), ***gobernabilidad*** (qué tanto puede actuar el actor o los actores sobre ellos) y ***pertinencia*** (que tan viable y oportuna es la resolución), para ello se tendrá en cuenta los siguientes niveles:

Nivel	Valor
Bajo	4
Medio	7
Alto	10

Tabla 6. Criterios de valoración

A continuación, se presentan los niveles de viabilidad como resultado de la valoración de cada uno de los criterios:

Resultado (I+G+P)	Nivel
Entre 1 y 14	Limitadamente viable
Entre 15 y 23	Medianamente viable
Entre 24 y 30	Potencialmente viable

En adelante se presenta los resultados de la valoración para cada una de las variables o acciones:

No.	Causa	Actor	Acción	Valoración			
				Gobernabilidad	Impacto	Pertinencia	Viabilidad
1	Capacitación insuficiente para la implementación del MSPI	MinTic[1]	Intervenir las entidades con un cumplimiento por debajo del 60% fortaleciendo los planes de capacitación y entrenamiento en el MSPI[2].	ALTO	MEDIO	MEDIO	**Potencialmente Viable**
2	Falta de planificación para la implementación del MSPI	Entidades de Orden Nacional	Crear el PESI (Plan estratégico de seguridad de la información)	ALTO	MEDIO	MEDIO	**Potencialmente Viable**
3	Procesos de contratación demorados	Entidades de Orden Nacional	Mejorar el alcance y las especificaciones de los procesos licitatorios, aterrizarlos a la realidad	MEDIO	MEDIO	MEDIO	**Medianamente Viable**
4	Falta de compromiso y liderazgo	Gerente General	Crear un cargo al interior de la entidad que responda al rol de Líder u Oficial de SI independiente de las demás áreas y dependiente de la Gerencia General.	ALTO	ALTO	ALTO	**Potencialmente Viable**
5	Apoyo insuficiente en las actividades de implementación	Consejo Directivo	Incluir en las responsabilidades de los directivos la gestión de seguridad de la información al interior de sus áreas.	ALTO	ALTO	MEDIO	**Potencialmente Viable**
6	Reprocesos que obstaculizan la implementación del MSPI	Planeación	Involucrar a planeación desde la planificación del proyecto, asignando un representante que acompañe y apoye al Líder u Oficial del SI en la implementación del MSPI.	ALTO	MEDIO	MEDIO	**Potencialmente Viable**

[1] Ministerio de las Tecnologías y las Comunicaciones
[2] Modelo de Seguridad y Privacidad de la Información

No.	Causa	Actor	Acción	Valoración			
				Gobernabilidad	Impacto	Pertinencia	Viabilidad
7	Sobrecarga laboral	Gerente de TI	Asignar un representante de TI para que apoye al Líder u Oficial del SI en la implementación del modelo MSPI.	ALTO	ALTO	ALTO	**Potencialmente Viable**
8	Desconocimiento del proyecto del MSPI	Líderes de proceso	Fortalecer los planes de capacitación y divulgación del modelo MSPI	MEDIO	MEDIO	MEDIO	**Medianamente Viable**
9	Autoridad delegada insuficiente	Líderes u Oficiales de SI	Adicionar al Comité directivo las actividades de revisión y aprobación del modelo MSPI.	MEDIO	MEDIO	MEDIO	**Medianamente Viable**
10	Alta resistencia al cambio	Funcionario	Aplicar un modelo de gestión de cambio para funcionarios y contratistas	MEDIO	MEDIO	MEDIO	**Medianamente Viable**
11	Alta rotación anual de contratistas	Contratista	Modificar el tiempo limitado de los contratos por prestación de servicios de un año a dos años.	BAJO	MEDIO	BAJO	**Medianamente Viable**
12	Contrataciones con tiempos insuficientes para la implementación del MPSI	Firmas consultoras externas	Licitar contratos de implementación del MSPI no menores a un año.	BAJO	BAJO	BAJO	**Limitadamente Viable**

Tabla 7. Matriz de Valoración Estratégica

1.6.1. MOMENTO TÁCTICO

Una vez realizada la matriz de valoración estratégica, teniendo en cuenta el resultado de viabilidad, se seleccionan las acciones que se van a ejecutar para llegar al escenario optimista ordenándolas de **Potencialmente Viable** a **Limitadamente Viable**:

No.	Causa	Actor	Acción	Valoración			
				Gobernabilidad	Impacto	Pertinencia	Viabilidad
1	Capacitación insuficiente para la implementación del MSPI	MinTic	Intervenir las entidades con un cumplimiento por debajo del 60% fortaleciendo los planes de capacitación y entrenamiento en el MSPI.	ALTO	MEDIO	MEDIO	**Potencialmente Viable**
2	Falta de planificación para la implementación del MSPI	Entidades de Orden Nacional	Crear el PESI (Plan estratégico de seguridad de la información)	ALTO	MEDIO	MEDIO	**Potencialmente Viable**
4	Falta de compromiso y liderazgo	Gerente General	Crear un cargo al interior de la entidad que responda al rol de Líder u Oficial de SI independiente de las demás áreas y dependiente de la Gerencia General.	ALTO	ALTO	ALTO	**Potencialmente Viable**
5	Apoyo insuficiente en las actividades de implementación	Consejo Directivo	Incluir en las responsabilidades de los directivos la gestión de seguridad de la información al interior de sus áreas.	ALTO	ALTO	MEDIO	**Potencialmente Viable**

No.	Causa	Actor	Acción	Valoración			
				Gobernabilidad	Impacto	Pertinencia	Viabilidad
6	Reprocesos que obstaculizan la implementación del MSPI	Planeación	Involucrar a planeación desde la planificación del proyecto, asignando un representante que acompañe y apoye al Líder u Oficial del SI en la implementación del MSPI.	ALTO	MEDIO	MEDIO	**Potencialmente Viable**
7	Sobrecarga laboral	Gerente de TI	Asignar un representante de TI para que apoye al Líder u Oficial del SI en la implementación del modelo MSPI.	ALTO	ALTO	ALTO	**Potencialmente Viable**

Tabla 8. Acciones por ejecutar

2. PROPUESTA

2.1. PLANTEAMIENTO DEL PROBLEMA

Con los crecientes avances tecnológicos, vemos el incremento de ataques por parte de individuos que buscando beneficios económicos o simplemente demostrando las vulnerabilidades de los sistemas de información, hacen que los responsables de la seguridad siempre estén desarrollando tecnologías y técnicas cada vez más sofisticadas para contrarrestar estos ataques. Por su parte, los atacantes están creando infraestructuras sólidas y cada vez más complejas. Los ciberdelincuentes están cada día perfeccionando y mejorando sus técnicas para obtener beneficios económicos de sus de sus víctimas u organizaciones y para evitar ser detectados mientras continúan vulnerando la seguridad de los datos y de la propiedad intelectual.

Frente a lo anterior, el Gobierno Nacional a través del documento CONPES 3701 del 14 de julio de 2011, instauró la Estrategia Nacional de Ciberseguridad y Ciberdefensa, para adoptar medidas que contemplen la seguridad de la información de todos los individuos frente a las amenazas que se presentan día a día de tipo informáticas, creando obligaciones que debe cumplir el Ministerio de las TIC con las diferentes entidades respecto al desarrollo de estrategias, planes, políticas, formaciones y sensibilización en todo lo referente a la seguridad de la información

Como resultado del Decreto 1078 de 2015, aparece el Modelo de Seguridad y Privacidad de la información (MSPI) el cual es de obligatorio cumplimiento para las Entidades de Orden Nacional. El MSPI consiste en diseñar e implementar modelos de seguridad de la información tomando como base el estándar ISO 27001 y buenas prácticas del sector.

Para medir el nivel de cumplimiento del MSPI en las Entidades de Orden Nacional, la Función Pública estableció un instrumento denominado FURAG, el cual es el Formulario único de reporte de avances y gestión. En efecto, para el cierre del año 2016, las entidades reportaron sus avances frente a los plazos y porcentajes establecidos en el decreto. En el componente de Seguridad y Privacidad de la Información, objeto de este análisis, se presentó la situación de interés puesto que sólo el 46% de las entidades adscritas al Orden Nacional cumplieron con el 60% del componente de implementación del Modelo de Seguridad y Privacidad de la Información fijado para el 2016.

La razón de lo anterior se debe a diferentes actores internos o externos cuya influencia afectó la implementación del MSPI en las entidades. Entre los actores más representativos se encuentran: El Ministerio de Tecnologías de la Información y las Comunicaciones – MinTic, las propias entidades de orden nacional y sus dependencias internas (gerente general, consejo directivo, planeación, gerente de ti, líderes de proceso, lideres u oficiales del SI, funcionarios y contratistas), firmas consultoras, asesores y consultores externos.

No obstante, la mayoría de las causas provienen de los actores internos las cuales van desde capacitaciones insuficientes, falta de planificación, ausencia de compromiso y liderazgo, reprocesos, sobrecarga laboral, resistencia al cambio, rotación de contratistas hasta la delegación de autoridad insuficiente.

En efecto, las entidades no lograron el porcentaje requerido, como consecuencia de ello, las entidades se pueden enfrentar a sanciones, multas y penalizaciones que ponen en riesgo no solo la imagen y las finanzas públicas, sino que también pueden sufrir interrupciones en su servicio puesto que no todos los controles de seguridad de la información fueron implementados, lo que representa aumento en las vulnerabilidades que pueden ser utilizadas por los atacantes informáticos.

2.2. JUSTIFICACIÓN

A medida que las empresas adoptan la digitalización y el internet, los líderes de seguridad de la información tendrán más vulnerabilidades por las cuales deben preocuparse. Entre el 2015 y el 2016 el 64% de las denuncias correspondió a hurtos por medios informáticos, de los cuales, el 20% fueron reportados por empresas del sector de las telecomunicaciones, transporte e industria, lo que se traduce en daños económicos alrededor de los 600 millones de dólares en el 2016.

Por consiguiente, entre las funciones que más se ven afectadas luego de un ataque informático se encuentran: Operaciones (36%), Finanzas (30%), Reputación de la marca (26%) y Retención de Clientes (26%). Lo anterior presenta un panorama de las consecuencias a las que las entidades se pueden enfrentar al no implementar oportunamente los controles de seguridad de la información del MSPI.

Los resultados de las encuestas realizadas por CISCO 2016 arrojaron que los principales obstáculos por los que las empresas descuidan la seguridad de la información son: Restricciones de presupuesto (35%), problemas de compatibilidad (28%) y requisitos de certificación (25%), lo que confirma algunas de las causas y actores relevantes que influyen a la hora de implementar el MSPI. Aunque en las entidades públicas la asignación de presupuesto para temas de seguridad de la información ha mejorado, su administración y disposición no es del todo correcta, causas como la mala planificación hace que los recursos no se gestionen de manera adecuada.

En cuanto a las empresas que han superado éstas causas y han logrado implementar el modelo de seguridad de la información, se encontró que a su interior realizaron mejoras que impactaron potencialmente la gestión de proteger a la empresa contra las infracciones de seguridad, entre las principales mejoras se encuentran: Separación del equipo de seguridad del departamento de TI (38%), aumento de las capacitaciones para la concientización sobre la seguridad entre los empleados (38%), profundización del enfoque sobre el análisis de riesgos y la mitigación de riesgos (37%), aumento de las inversiones en tecnología o soluciones para la defensa ante amenazas de seguridad (37%) y aumento de las inversiones en capacitación del personal de seguridad (37%).

En apoyo a lo anterior, las grandes empresas son mucho más propensas a subcontratar auditorias (56%), asesoramiento y consultoría (55%), de ahí la importancia de desarrollar este proyecto enfocado a realizar un diagnóstico y proponer posibles acciones para mitigar las causas que impiden la implementación del modelo MSPI en las entidades públicas.

En síntesis, los resultados del FURAG arrojaron que los sectores con reportes de avance por debajo del 60% para el año 2016 fueron: Tecnologías de la información y las comunicaciones, interior, defensa, inclusión social y reconciliación, salud y protección social y transporte.

Visto que sólo el 46% de las Entidades de Orden Nacional reportaron un avance de implementación del 60% requerido, es preocupante el otro 50% de las entidades que aún se encuentran por debajo del porcentaje y fuera del plazo establecido, lo que las expone no solo a sanciones, multas y penalizaciones por incumplimiento al Decreto 1078 de 2015 sino que también aumenta sus posibilidades de ser un blanco más para los atacantes. Esto ha impulsado la realización de este proyecto cuya investigación y diagnóstico se centrará en identificar las

acciones necesarias para que las entidades públicas logren en un corto plazo la implementación del MSPI.

2.3. MARCO TEÓRICO

Hasta el momento se ha analizado y justificado por qué la necesidad de la implementación del MSPI en las entidades de orden nacional, no obstante, es importante conocer la percepción de éstas a fin de determinar cuáles son sus necesidades y expectativas para poner en marcha dicha reglamentación.

Un estudio sobre el estado y alcances del gobierno de TI y la gestión de TI en las entidades públicas de la ciudad de Manizales, departamento de Caldas, Colombia realizado por los estudiantes de la Universidad EAFIT en Medellín, coloca en evidencia varias de las razones por las cuales las entidades públicas no se acogen rápidamente a las estrategias de gobierno en línea, entre ellas el MSPI.(Marulanda Echeverry, López Trujillo, & Valencia Duque, 2017).

¿Por qué Gobierno de TI y gestión de TI?, es importante aclarar que la reglamentación, es decir, el Decreto 1078 de 2015 está enmarcado en las tecnologías y la información, por tanto, toda la gestión recae sobre el Gobierno y gestión de TI en cada entidad pública.

Con lo anterior, el área de TI dejo de ser sólo un proceso de apoyo y se convirtió en uno de los principales aliados estratégicos para la alta gerencia y la junta directiva en el logro de las estrategias y objetivos de la entidad.

El actual plan de desarrollo de tecnologías de información de Colombia denominado “Vive Digital” para el período 2014-2018, liderado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC, 2016), contempla cuatro líneas estratégicas: empleo, educación, gobierno digital y ciudad región. En particular, el decreto 1078 de 2015 establece, en su título 9, las políticas y lineamientos de tecnologías de la información para el Estado colombiano, a partir del cual se estructuran cuatro componentes de la estrategia de gobierno en línea: TIC para servicios, TIC para el gobierno abierto, TIC para la gestión y seguridad y privacidad de la información; además, establece, en forma adicional, el marco de referencia para la gestión de tecnologías de información.(Marulanda Echeverry et al., 2017).

El estudio realizado por los estudiantes de la Universidad EAFIT en Medellín, utilizo una investigación cualitativa y cuantitativa, en la que se aplicó una encuesta a 19 entidades públicas de la ciudad de Manizales en Colombia, entre las cuales se contempló el componente de sistema de gestión de seguridad de la información.

En lo relacionado con el gobierno de TI y, en específico, con la normatividad y el marco legal, los procesos y la estructura de TI, la toma de decisiones, las interrelaciones con otras áreas y organizaciones, la diligencia con los proveedores, la alineación con los procesos, los acuerdos de servicios y de desarrollos, el estudio arroja como resultado, que seis de las entidades públicas encuestadas, es decir, el 32%, no tienen calificación sobre el tema de gobierno de TI (Marulanda Echeverry et al., 2017), lo que quiere decir probablemente que desconocen la reglamentación y por tanto no hay un cumplimiento de la misma.

Por otro lado, en lo relacionado con la infraestructura y los recursos de TI disponibles y suficientes para lograr los objetivos estratégicos de la entidad, el 58% de las entidades públicas de la ciudad de Manizales no cuentan con infraestructura ni con los recursos de TI disponibles y suficientes para lograr los objetivos estratégicos de ellas. En comparación con muchas organizaciones del mismo tipo del país, se viene dando una tendencia de disminución de presupuesto en términos reales para su desarrollo, dadas las políticas de los últimos gobiernos frente al manejo presupuestal de dichas entidades.(Marulanda Echeverry et al., 2017)

La inquietud que surge es que, aunque se presentan planes, programas y proyectos, hacerlos realidad requiere recursos; sin embargo, el Gobierno exige el cumplimiento de metas sin los recursos necesarios para cumplirlas.

Lo anterior refleja la falta de capacitación y asignación de recursos por parte del gobierno en las entidades públicas para que estas logren lo exigido en la reglamentación.

Como lo soporta el estudio, las universidades pueden ser parte del acompañamiento que requieren las entidades públicas, facilitándoles el conocimiento y las herramientas administrativas para el desarrollo de los proyectos relacionados con Gobierno en Línea.

No obstante, el gobierno debe realizar una asignación de recursos más coherente y apropiado a fin de apoyar a las entidades públicas en el logro de las iniciativas presentadas.

Los resultados del estudio están de acuerdo con los resultados encontrados por Kim et al. (2013), que hallaron lo siguiente: se requiere un gobierno efectivo TI que facilite la toma de decisiones correspondiente, con inclusión del establecimiento de prioridades para los recursos de TI; hay una relación directa entre la estructura y el proceso, el control y la coordinación, así como con la alineación con la política corporativa, y enfatizan que, para ser efectivos, la gobernabilidad necesita ser estructurada de manera que permita la entrega de valores únicos, la asignación óptima de recursos, la gestión de riesgos y la medición de los resultados.(Marulanda Echeverry et al., 2017).

Como consecuencia de lo expuesto en los estudios realizados, concluimos que para mejorar el porcentaje de acción de las entididades del estado es necesario que MinTic reevalue la estrategia de comunicación, capacitacion y asignacion de recursos en todas las entidades de orden nacional. No obtanate es de nuestro interes apoyar y acompañar desde nuestra firma consultora a las entidades, en especial desde el Gobierno de TI, en el camino de implementar por lo menos el MSPI.

2.4. OBJETIVO GENERAL DEL PROYECTO

Presentar el Plan Estratégico de Seguridad de la Información (en adelante PESI), el cual es una herramienta (en Excel) que dirige la implementación de los controles de seguridad de acuerdo con el Modelo de Seguridad y Privacidad de la Información MSPI, dirigido a las entidades de orden nacional, presentando las prioridades, fases, tiempos y recursos para la implementación del modelo enmarcado en el ciclo de mejoramiento continuo PHVA (planear, hacer, verificar y actuar).

2.5. OBJETIVOS ESPECÍFICOS

- Diseñar una herramienta, fácil y dinámica, que les permita a las entidades de orden nacional proyectar la implementación del MSPI.
- Incrementar el nivel de cumplimiento en la gestión de la seguridad y privacidad de la información en las entidades de orden nacional que apliquen la herramienta.

- Proponer a las entidades de orden nacional, los criterios para implementar el MSPI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.

2.6. ALCANCE

El presente proyecto va desde la selección de tres (3) entidades públicas, el análisis diagnóstico de la brecha existente entre la situación actual y el nivel esperado en relación a seguridad de la información, la comparación de los resultados, la identificación de los principales hallazgos, la elaboración del Plan Estratégico de Seguridad de la Información (PESI) con las principales acciones en una línea de tiempo especifica con las que una entidad pública puede alcanzar la implementación del MSPI; continua con el perfeccionamiento del proyecto y concluye con la sustentación respectiva.

No hace parte del alcance de este proyecto:

- El contacto físico con las entidades seleccionadas
- La presentación y/o entrega de los Análisis GAP y/o del PESI a todas o alguna de las entidades seleccionadas
- La implementación del PESI
- La asignación de recursos económicos para la implementación del PESI
- La asignación de asesores y/o consultores a las entidades seleccionadas
- La actualización del PESI
- La entrega de las guías, instructivos, procedimientos, formatos y demás documentos que se mencionen en PESI
- El presupuesto específico que la entidad debe asignar para la implementación del PESI
- El seguimiento y las mediciones a la implementación del PESI en las entidades.

2.7. PLAN DE TRABAJO

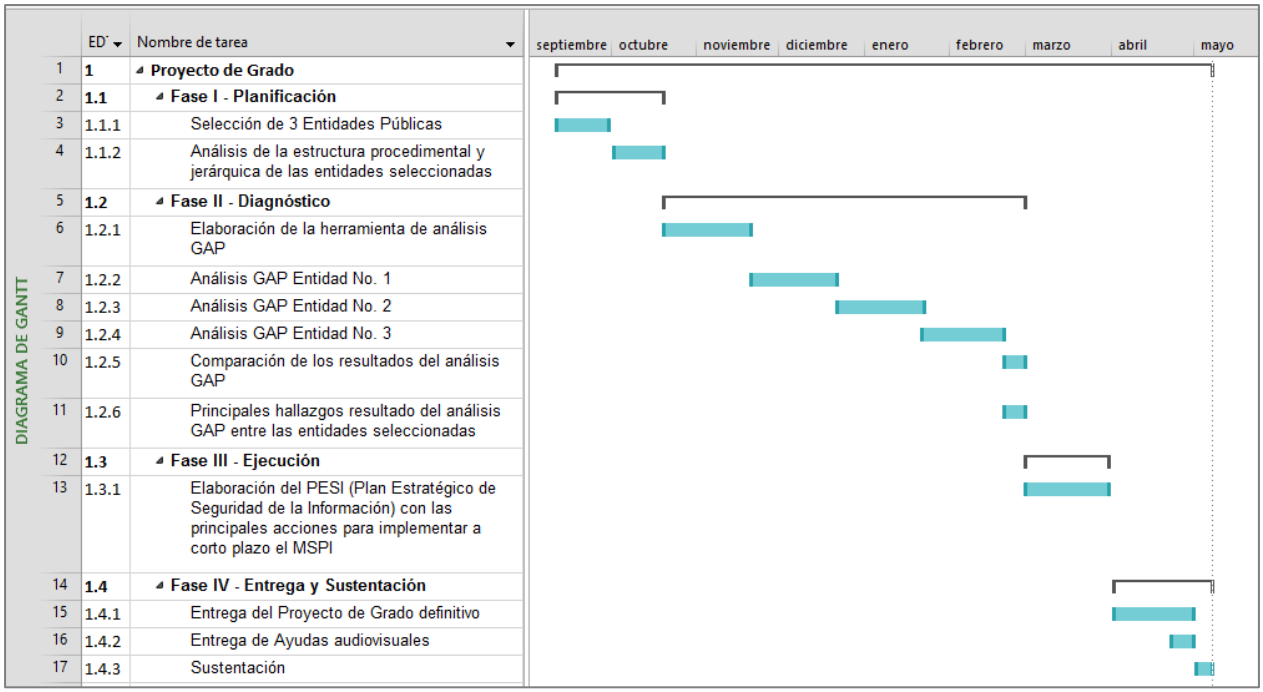
A continuación, se presenta las actividades propuestas para llevar a cabo el plan de trabajo:

EDT	Nombre de tarea	% completado	Comienzo	Fin
1.1	**Fase I - Planificación**	**0%**	**lun 11/09/17**	**jue 19/10/17**

EDT	Nombre de tarea	% completado	Comienzo	Fin
1.1.1	Selección de 3 Entidades Públicas	0%	lun 11/09/17	vie 29/09/17
1.1.2	Análisis de la estructura procedimental y jerárquica de las entidades seleccionadas	0%	lun 02/10/17	jue 19/10/17
1.2	**Fase II - Diagnóstico**	**0%**	**vie 20/10/17**	**mié 28/02/18**
1.2.1	Elaboración de la herramienta de análisis GAP	0%	vie 20/10/17	lun 20/11/17
1.2.2	Análisis GAP Entidad No. 1	0%	mar 21/11/17	jue 21/12/17
1.2.3	Análisis GAP Entidad No. 2	0%	vie 22/12/17	lun 22/01/18
1.2.4	Análisis GAP Entidad No. 3	0%	lun 22/01/18	mar 20/02/18
1.2.5	Comparación de los resultados del análisis GAP	0%	mié 21/02/18	mié 28/02/18
1.2.6	Principales hallazgos resultado del análisis GAP entre las entidades seleccionadas	0%	mié 21/02/18	mié 28/02/18
1.3	**Fase III - Ejecución**	**0%**	**jue 01/03/18**	**vie 30/03/18**
1.3.1	Elaboración del PESI (Plan Estratégico de Seguridad de la Información) con las principales acciones para implementar a corto plazo el MSPI	0%	jue 01/03/18	vie 30/03/18
1.4	**Fase IV - Entrega y Sustentación**	**0%**	**lun 02/04/18**	**lun 07/05/18**
1.4.1	Entrega del Proyecto definitivo	0%	lun 02/04/18	lun 30/04/18
1.4.2	Entrega de Ayudas audiovisuales	0%	lun 23/04/18	lun 30/04/18
1.4.3	Sustentación	0%	mié 02/05/18	lun 17/05/18

Tabla 9. Plan de Trabajo

Posteriormente se presenta el diagrama de Gantt del plan de trabajo propuesto:



	EDT	Nombre de tarea
1	**1**	**Proyecto de Grado**
2	**1.1**	**Fase I - Planificación**
3	1.1.1	Selección de 3 Entidades Públicas
4	1.1.2	Análisis de la estructura procedimental y jerárquica de las entidades seleccionadas
5	**1.2**	**Fase II - Diagnóstico**
6	1.2.1	Elaboración de la herramienta de análisis GAP
7	1.2.2	Análisis GAP Entidad No. 1
8	1.2.3	Análisis GAP Entidad No. 2
9	1.2.4	Análisis GAP Entidad No. 3
10	1.2.5	Comparación de los resultados del análisis GAP
11	1.2.6	Principales hallazgos resultado del análisis GAP entre las entidades seleccionadas
12	**1.3**	**Fase III - Ejecución**
13	1.3.1	Elaboración del PESI (Plan Estratégico de Seguridad de la Información) con las principales acciones para implementar a corto plazo el MSPI
14	**1.4**	**Fase IV - Entrega y Sustentación**
15	1.4.1	Entrega del Proyecto de Grado definitivo
16	1.4.2	Entrega de Ayudas audiovisuales
17	1.4.3	Sustentación

Ilustración 12. Diagrama de Gantt

3. ESTRATEGIA METODOLÓGICA

Como parte del desarrollo del plan de trabajo propuesto en el numeral *2.6 Plan de Trabajo*, a continuación, se expone la estrategia utilizada para la selección de las 3 entidades públicas que en adelante fueron objeto del análisis GAP.

EDT	Nombre de tarea	% completado	Comienzo	Fin
1.1	**Fase I - Planificación**	**0%**	**lun 11/09/17**	**jue 19/10/17**
1.1.1	Selección de 3 Entidades Públicas	0%	lun 11/09/17	vie 29/09/17
1.1.2	Análisis de la estructura procedimental y jerárquica de las entidades seleccionadas	0%	lun 02/10/17	jue 19/10/17

Tabla 10. Extracción del Plan de Trabajo propuesto

3.1. DESCRIPCIÓN DE LAS VARIABLES

Del numeral 1.1 DESCRIPCIÓN DE LA SITUACIÓN DE INTERÉS procedemos a extraer la *Tabla 2. Porcentaje de cumplimiento por Sector (FURAG, 2017),* la cual presenta el porcentaje obtenido en el componente de implementación totalizado por sectores:

Código	Sector	Porcentaje de Implementación
SC-1	Agricultura y Desarrollo Rural	62,6
SC-2	Ambiente y Desarrollo Sostenible	71,7
SC-3	Ciencia, Tecnología e innovación	66,7
SC-4	Comercio, Industria y Turismo	59,3
SC-5	Cultura	39,8
SC-6	Defensa	47,5
SC-7	Del Deporte, la Recreación, la Actividad Física y el Aprovechamiento del Tiempo Libre	55,0
SC-8	Educación	53,9
SC-9	Estadísticas	61,7
SC-10	Función Pública	47,1
SC-11	Hacienda y Crédito Público	52,5
SC-12	Inteligencia Estratégica y Contrainteligencia	100,0
SC-13	Interior	46,4
SC-14	Justicia y del Derecho	61,3
SC-15	Minas y Energía	60,1

Código	Sector	Porcentaje de Implementación
SC-16	Planeación	91,7
SC-17	Presidencia de la República	62,5
SC-18	Relaciones Exteriores	78,8
SC-19	Salud y Protección Social	54,9
SC-20	Tecnologías de la Información y las Comunicaciones	36,0
SC-21	Trabajo	73,8
SC-22	Transporte	59,2
SC-23	Vivienda Ciudad y Territorio	71,7
SC-24	Inclusión Social y Reconciliación	53,8

Tabla 11.Porcentaje de cumplimiento por Sector (FURAG, 2017)

A continuación, se procede a clasificar la información en cuadrantes de acuerdo con los siguientes criterios:

Nivel	Rango	Descripción
Alto	Mayor al 70%	Las entidades adscritas a este sector han desarrollado estrategias de implementación eficaces y es muy probable que hayan determinado los recursos necesarios para el mantenimiento del MSPI.
Medio	Mayor al 50% y menor o igual al 70%	Las entidades adscritas a este sector han desarrollado estrategias de implementación sin evaluar su eficacia y es probable que hayan determinado los recursos necesarios para el mantenimiento del MSPI.
Bajo	Menor o igual al 50%	Las entidades adscritas a este sector no han desarrollado estrategias de implementación por lo tanto no han determinado los recursos necesarios para el mantenimiento del MSPI.

Tabla 12. Criterios para la clasificación por cuadrantes (elaboración propia)

En adelante se presenta la clasificación de los sectores en los cuadrantes de acuerdo con el porcentaje de implementación:

Código	Sector	Porcentaje de Implementación	Nivel
SC-12	Inteligencia Estratégica y Contrainteligencia	100,0%	Alto
SC-16	Planeación	91,7%	
SC-18	Relaciones Exteriores	78,8%	
SC-21	Trabajo	73,8%	
SC-2	Ambiente y Desarrollo Sostenible	71,7%	
SC-23	Vivienda Ciudad y Territorio	71,7%	
SC-3	Ciencia, Tecnología e innovación	66,7%	Medio

Código	Sector	Porcentaje de Implementación	Nivel
SC-1	Agricultura y Desarrollo Rural	62,6%	
SC-17	Presidencia de la República	62,5%	
SC-9	Estadísticas	61,7%	
SC-14	Justicia y del Derecho	61,3%	
SC-15	Minas y Energía	60,1%	
SC-4	Comercio, Industria y Turismo	59,3%	
SC-22	Transporte	59,2%	
SC-7	Del Deporte, la Recreación, la Actividad Física y el Aprovechamiento del Tiempo Libre	55,0%	
SC-19	Salud y Protección Social	54,9%	
SC-8	Educación	53,9%	
SC-24	Inclusión Social y Reconciliación	53,8%	
SC-11	Hacienda y Crédito Público	52,5%	
SC-6	Defensa	47,5%	Bajo
SC-10	Función Pública	47,1%	
SC-13	Interior	46,4%	
SC-5	Cultura	39,8%	
SC-20	Tecnologías de la Información y las Comunicaciones	36,0%	

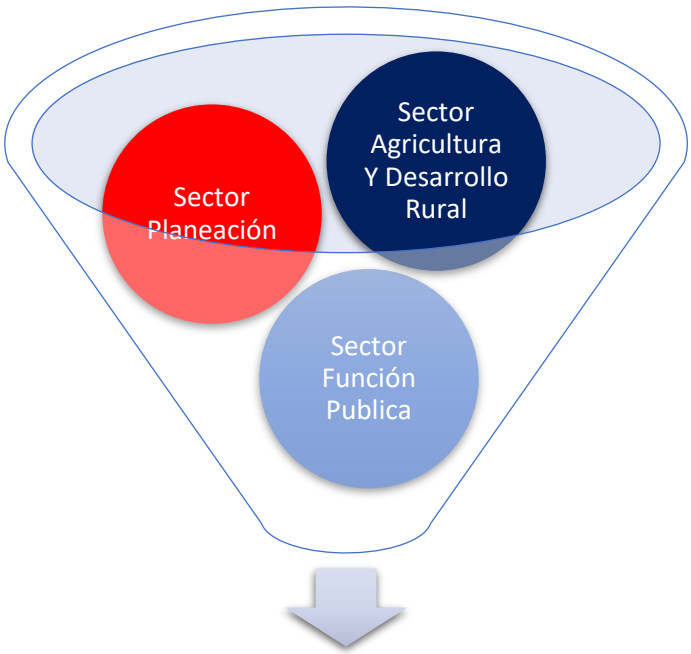
Tabla 13. Clasificación de sectores por cuadrantes

Posteriormente se procede a seleccionar un sector de cada cuadrante teniendo en cuenta el acercamiento y afinidad que hemos tenido con alguna de sus entidades adscritas, de dicho análisis se obtiene la siguiente selección:

Código	Sector	Porcentaje de Implementación	Nivel
SC-16	Planeación	91,7%	Alto
SC-1	Agricultura y Desarrollo Rural	62,6%	Medio
SC-10	Función Pública	47,1%	Bajo

Tabla 14. Selección de 3 sectores

De los sectores seleccionados, en conjunto se procede a seleccionar una entidad de cada sector con la cual se haya tenido conocimiento, afinidad o acercamiento en calidad de funcionario o contratista, o en su defecto como usuario de ésta:



1. Gestión de Servicios Publicos GSP
2. Organización Agropecuaria Nacional OAN
3. Centro Nacional de capacitación CNC

Tabla 15. Selección de 3 Entidades del Orden Nacional[3]

[3] La razón social de cada una de las entidades seleccionadas de orden nacional fue cambiada por un nombre ficticio para salvaguardar la confidencialidad de éstas.

3.2. ANÁLISIS DE LA ESTRUCTURA PROCEDIMENTAL Y JERÁRQUICA DE LAS ENTIDADES SELECCIONADAS

3.2.1. Gestión de Servicios Públicos – GSP

En el marco de la estructura del Estado colombiano, la entidad Gestión de Servicios públicos - GSP se encuentra adscrita al sector "Administración de Planeación", en cabeza del Departamento Nacional de Planeación.

- **Organigrama**

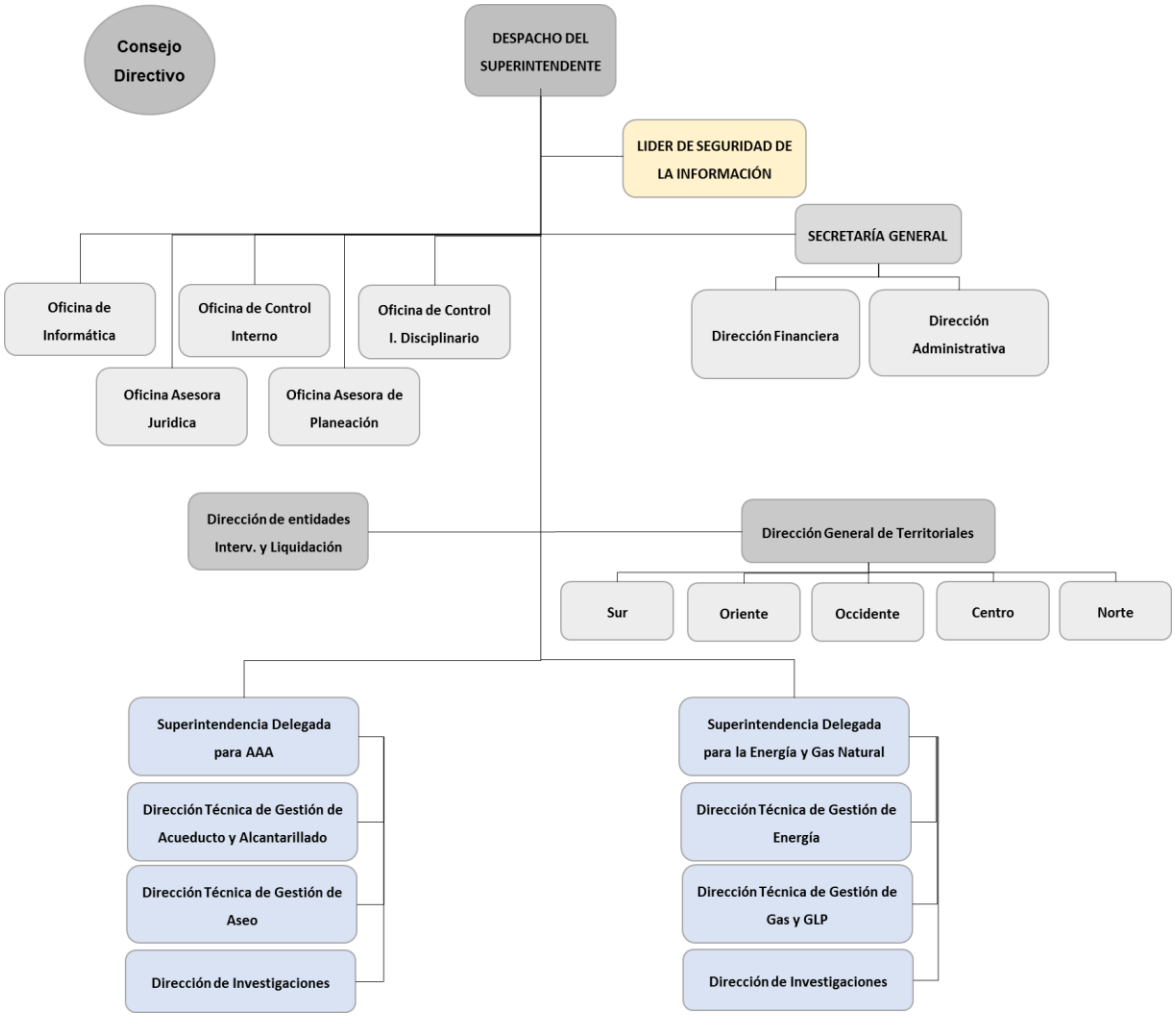


Ilustración 13. Organigrama GSP

- **Funciones generales de la organización**

Las funciones generales de la organización Gestión de Servicios Públicos, en lo que concierne a la inspección, vigilancia y control de las corporaciones u organizaciones prestadoras de servicios públicos de acueducto, alcantarillado, aseo, energía y gas; y la protección y cumplimiento de los derechos de los ciudadanos.

- Inspecciona, vigila y controla
- Interviene empresas en riesgo
- Certifica
- Sanciona
- Resuelve recursos
- Promueve la participación ciudadana
- Informa y da conceptos
- Determina sistemas de información

- **Servicios vigilados**

Ilustración 14. Servicios vigilados

- **Mapa De Procesos**

A continuación, se presenta el mapa de procesos de la entidad

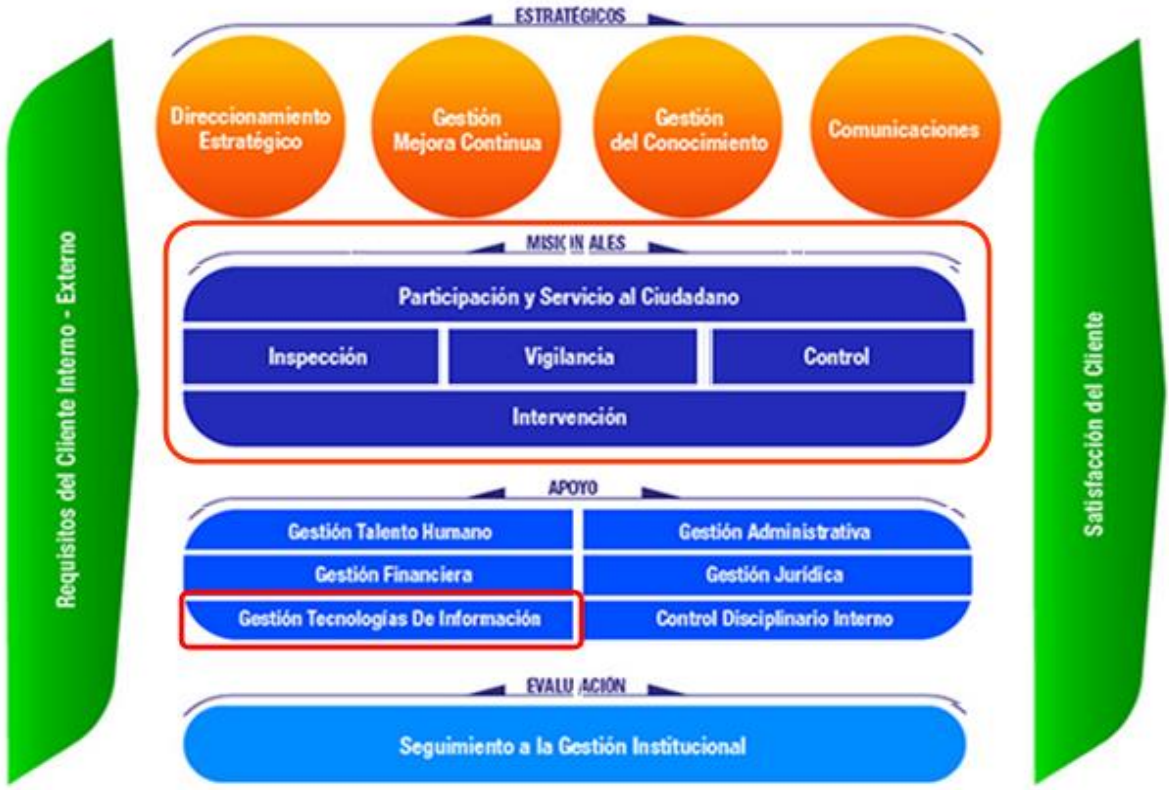


Ilustración 15. Mapa de procesos GSP

3.2.2. Organización Agropecuaria Nacional - OAN

La Organización Agropecuaria Nacional, en adelante OAN, es una organización de carácter público de orden nacional, que reporta a entidades de Agricultura y Desarrollo Rural.

En el desarrollo de sus funciones, la OAN diseña, desarrolla y ejecuta tácticas para reducir, controlar y prevenir los riesgos de carácter ambiental como biológicos y químicos para las variedades de animales y vegetales, que pueden afectar la producción agrícola, forestal, pesquera y acuícola de la nación.

Entre sus actividades están la de orientar a lograr los objetivos de producción agropecuaria más competitiva, con el fin de cumplir con las metas propuestas para la exportación. Así mismo, esta

organización es veedora de todos los productos agropecuarios, animales y vegetales, en las fronteras, aeropuertos y puertos.

- **Organigrama**

A continuación, se presenta la estructura organizacional de la entidad

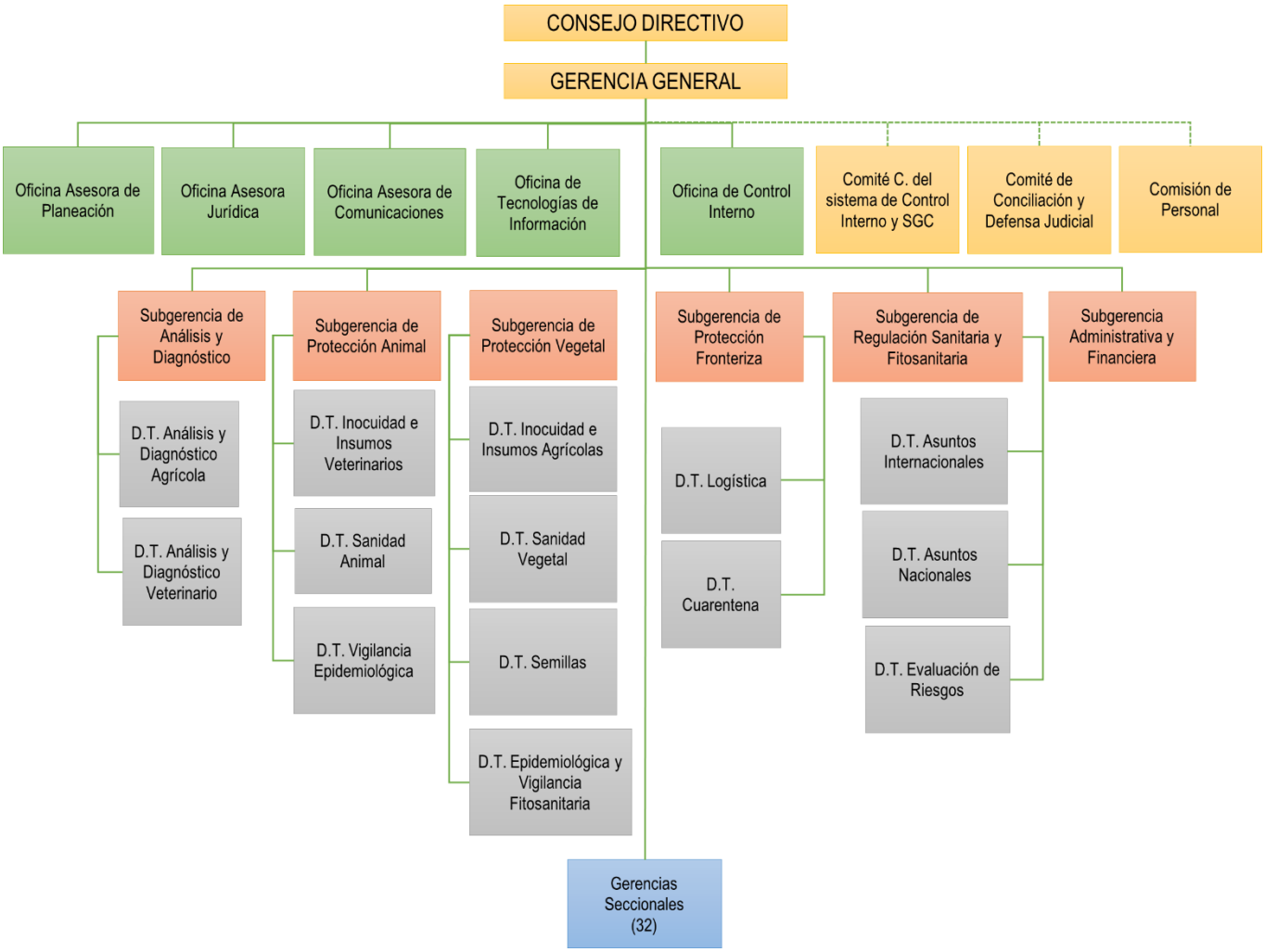


Ilustración 16. Organigrama OAN

- **Mapa de procesos**

En adelante se presenta la estructura procedimental de la entidad

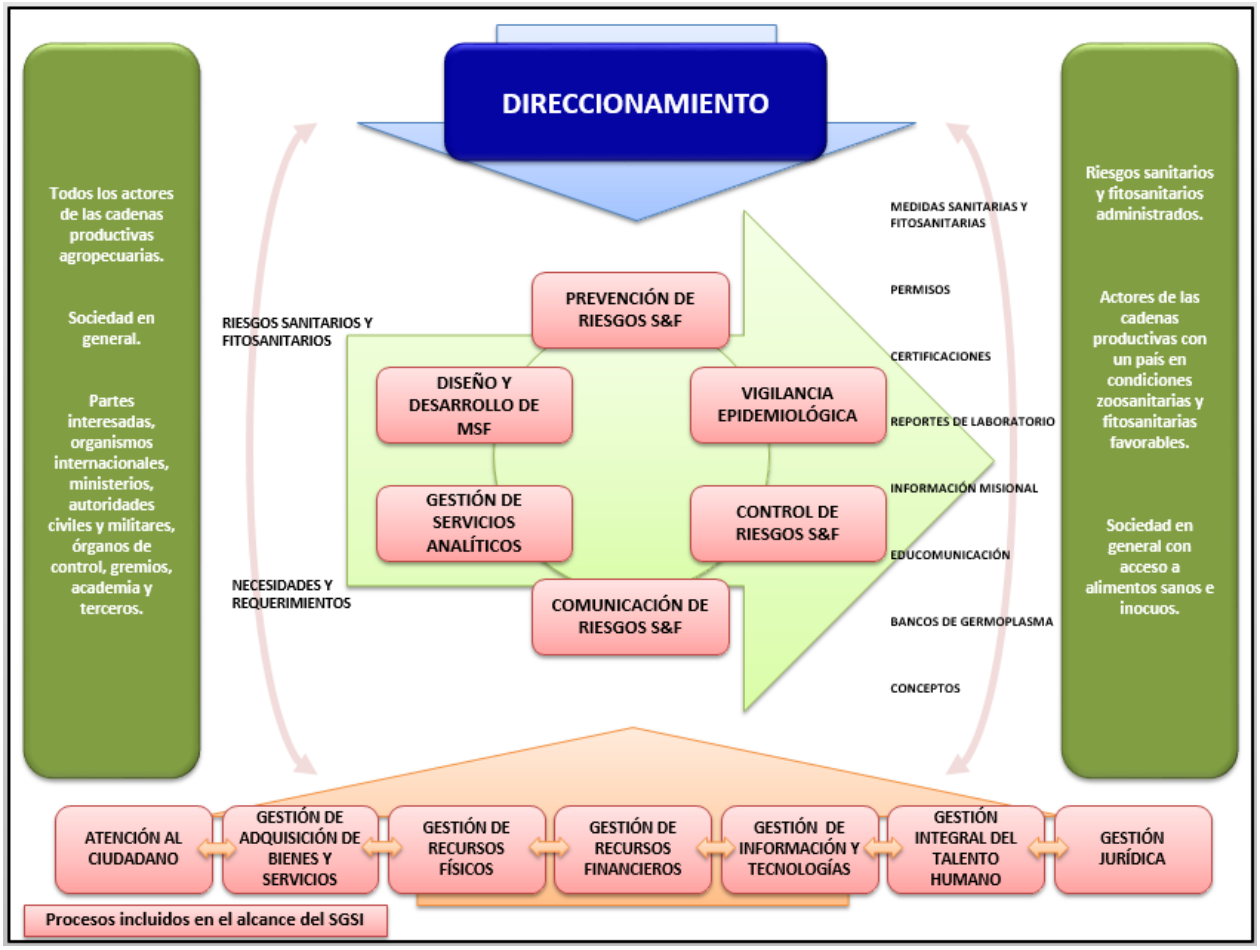


Ilustración 17. Mapa de procesos OAN

3.2.3. Centro Nacional de capacitación – CNC

El Centro Nacional de Capacitación, en adelante CNC fue creado como una organización de orden nacional, de carácter formativo adscrito a la entidad encargada de la gestión de funcionarios públicos, entidad autorizada para crear y ofrecer programas de capacitación en todos los niveles de educación superior. Cumple con funciones de entidad de capacitación de docencia e investigación. Posee autonomía académica, presupuestal, administrativa, financiera y cuenta con un patrimonio propio, conforme a la ley.

- **Organigrama**

A continuación, se presenta la estructura organizacional de la entidad

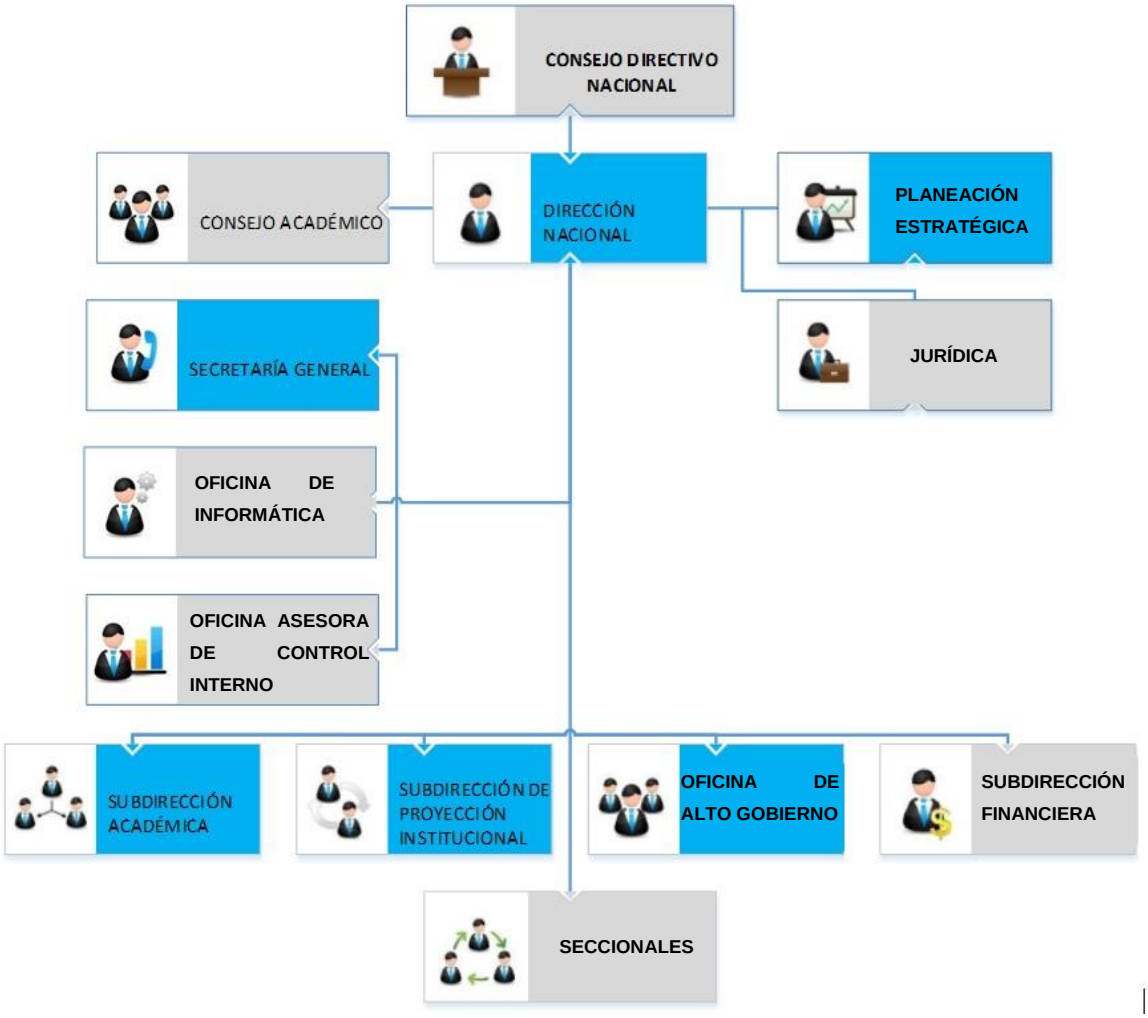
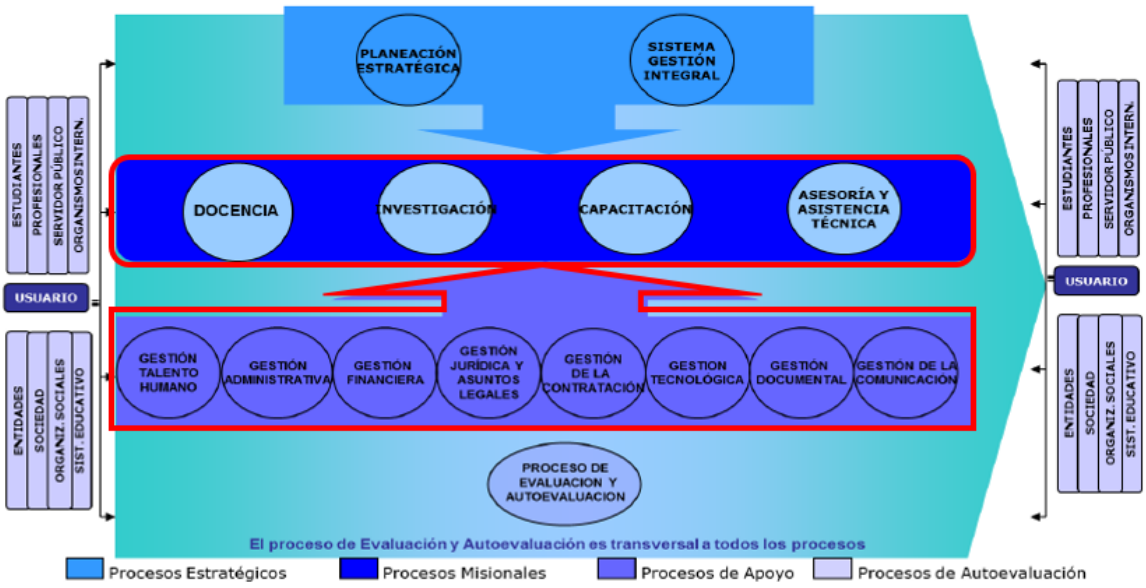


Ilustración 18. Organigrama CNC

- **Mapa de procesos**

En adelante se presenta la estructura procedimental de la entidad



Código : DC-S-GC-01 Fecha: 2016/10/31 Página 1 de 2 Versión 03

-------- Procesos que hacen parte del alcance del SGSI

Ilustración 19. Mapa de procesos CNC

4. DESARROLLO E IMPLEMENTACIÓN

En esta sección se da paso al desarrollo de las siguientes actividades descritas en el numeral 2.6 Plan de Trabajo:

EDT	Nombre de tarea	% completado	Comienzo	Fin
1.2	**Fase II - Diagnóstico**	**0%**	**vie 20/10/17**	**mié 28/02/18**
1.2.1	Elaboración de la herramienta de análisis GAP	0%	vie 20/10/17	lun 20/11/17
1.2.2	Análisis GAP Entidad No. 1	0%	mar 21/11/17	jue 21/12/17
1.2.3	Análisis GAP Entidad No. 2	0%	vie 22/12/17	lun 22/01/18
1.2.4	Análisis GAP Entidad No. 3	0%	lun 22/01/18	mar 20/02/18
1.2.5	Comparación de los resultados del análisis GAP	0%	mié 21/02/18	mié 28/02/18
1.2.6	Principales hallazgos resultado del análisis GAP entre las entidades seleccionadas	0%	mié 21/02/18	mié 28/02/18
1.3	**Fase III - Ejecución**	**0%**	**jue 01/03/18**	**vie 30/03/18**
1.3.1	Elaboración del PESI (Plan Estratégico de Seguridad de la Información) con las principales acciones para implementar a corto plazo el MSPI	0%	jue 01/03/18	vie 30/03/18

Ilustración 20. Plan de Trabajo

4.1. ELABORACIÓN DE LA HERRAMIENTA DE ANÁLISIS GAP

El GAP Análisis o Análisis de Brecha es una herramienta que ayuda a las organizaciones a evaluar el estado y desempeño real actual en tecnología, infraestructura, procesos, gestión del talento humano y situaciones en un momento dado, relacionando uno o varios puntos

seleccionados como referencias de variables en el orden local, regional, nacional y/o internacional.

El análisis de las variables son el resultado esperado, para la generación de estrategias y acciones para cumplir con los objetivos específicos de la norma NTC/ISO 27001 y el MSPI.

Ilustración 21. Pasos Metodología utilizada para el Análisis GAP

4.1.1. Elaboración de los cuestionarios

En esta fase se realizaron las siguientes actividades:

1. Revisión de la NTC/ISO 27001:2013 y del MSPI
2. Elaboración de un conjunto de preguntas por cláusula y dominio
3. Definición de niveles y criterios de madurez
4. Implementación de la herramienta

A continuación, se presentan los niveles y criterios teniendo en cuenta el MSPI[4]:

NIVEL	PORCENTAJE	CRITERIOS
Inexistente	0%	No se cuenta con la cláusula o control. No se evidencia la información como un activo necesario para el logro de la misión y visión de la organización.

[4] Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MSPI de la Estrategia de Gobierno en Línea - GEL

NIVEL	PORCENTAJE	CRITERIOS
Inicial	1-20%	El control esta implementado no obstante el modelo de seguridad de políticas, procedimientos y estándares de configuración no existe.
Repetible	21-40%	El control esta implementado y además es soportado por un documento que contiene una política de alto nivel y otras políticas operativas debidamente aprobadas.
Definido	41-60%	El control esta implementado y soportado por políticas, procedimientos y estándares de configuración debidamente publicados y socializados.
Administrado	61-80%	En este nivel se realizan mediciones sobre la efectividad de los controles.
Optimizado	81-100%	En este nivel se encuentran las organizaciones en las cuales se mide la efectividad de los controles con el fin de mejorarlos y optimizarlos.

Tabla 16. Niveles y Criterios de Madurez

4.1.2. Entrevistas e Inspecciones en Sitio

En esta fase se realizaron las siguientes actividades:

- Entendimiento de la estructura organizacional
- Revisión de los perfiles, cargos y caracterización de los procesos
- Elaboración agenda preliminar
- Revisión y aprobación de la agenda preliminar
- Ejecución de las entrevistas e inspecciones en sitio

4.1.3. Consolidación de Resultados

En esta fase se realizaron las siguientes actividades:

- Calificación del nivel de madurez de las cláusulas
- Calificación del nivel de madurez de los dominios
- Revisión de calificaciones

- Revisión de observaciones y hallazgos

4.1.4. Análisis de Resultados

En esta fase se realizaron las siguientes actividades:

- Cálculo del promedio por cada cláusula
- Cálculo del promedio por cada dominio
- Cálculo del promedio por cada control
- Elaboración de graficas de madurez y brecha
- Selección de hallazgos más críticos

Como parte de la metodología se realizan cinco (5) preguntas por cada control, cada una contribuyendo con un 20%. Estos valores son sumados para obtener el nivel de madurez del control de acuerdo. Para obtener el nivel de madurez por dominio se promedian los resultados obtenidos por control. Finalmente, para obtener el nivel de madurez para todos los dominios se promedian los resultados por dominio y para las cláusulas se promedian los resultados derivados por cláusula.

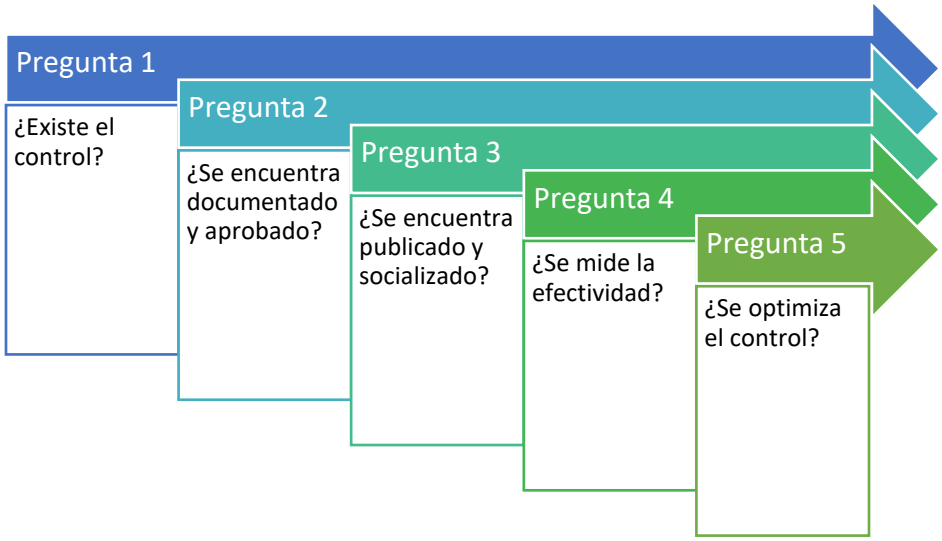


Ilustración 22. Ejemplo preguntas GAP

El promedio del dominio expresa cómo está la gestión de la seguridad de la información. El nivel *Optimizado* corresponde a un mayor nivel de madurez y en el otro extremo contrapuesto se encuentra el nivel Inexistente, lo que quiere decir que el nivel de cumplimiento y la madurez en

este control debe mejorarse con un nivel más alto de prioridad una vez se inicie la implementación de los controles de seguridad dentro del SGSI. Por cada dominio de la NTC/ISO 27001:2013 se debe determinar cuáles controles se van a implementar y a qué nivel de cumplimiento se quiere llegar en un tiempo razonable. La seguridad de la información no es un producto sino más bien un proceso continuo que debe integrarse dentro de la Entidad para garantizar la confidencialidad, la integridad y la disponibilidad de la información. La información es uno de los activos más importantes para poder cumplir con la misión organizacional.

4.2. PRESENTACIÓN DE RESULTADOS DE ANÁLISIS GAP

4.2.1. Gestión de Servicios Públicos – GSP

Analizando el siguiente gráfico, se puede observar que solo 4 de los 14 dominios se encuentran por encima o en estado ideal, los demás se encuentran por debajo del umbral del 70%, lo que indica que dichos controles requieren una atención inmediata sí de asegurar la conformidad de un SGSI se trata.

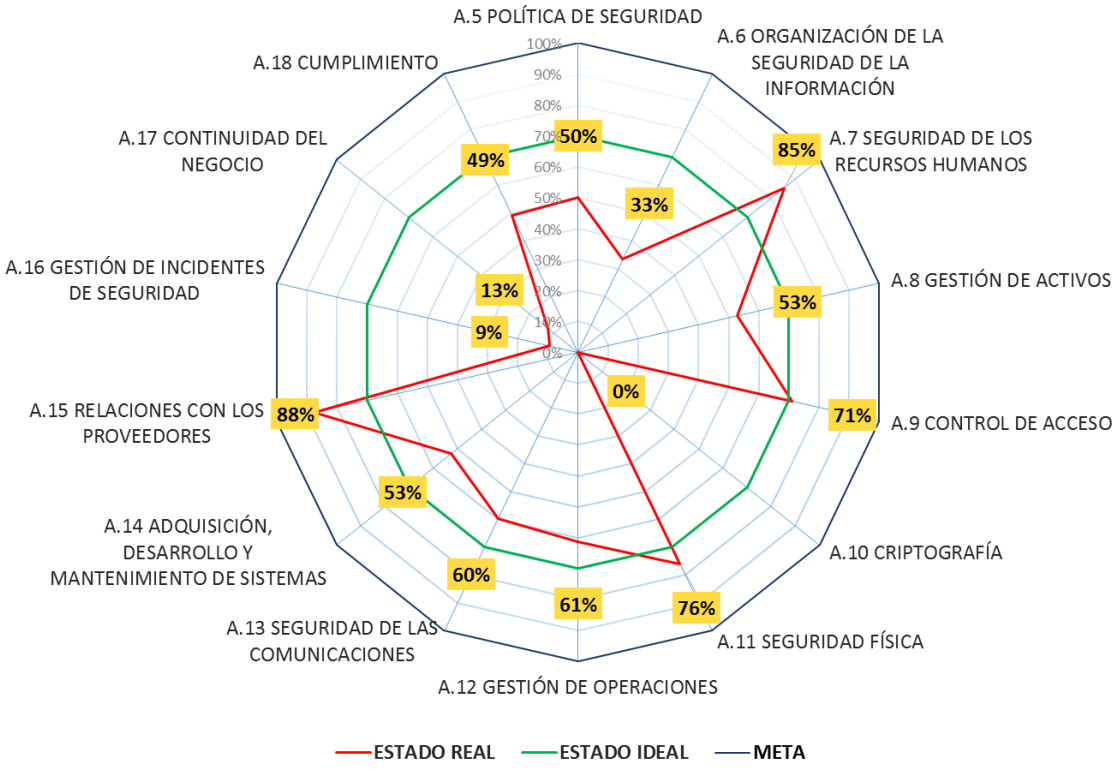


Ilustración 23. Estado real vs. Estado Ideal GSP

4.2.2. Organización Agropecuaria Nacional – OAN

Analizando el gráfico, se puede observar que el dominio con mayor nivel de madurez es el *A.7 Seguridad de los recursos humanos (Administrado)*, seguido de *A.11 Seguridad física (Repetible)*, *A.9 Control de acceso (Repetible)* y *A.5 Política de seguridad de la información (Repetible).* Los demás dominios se encuentran por debajo del **24%** que corresponde a un estado *Repetible*.

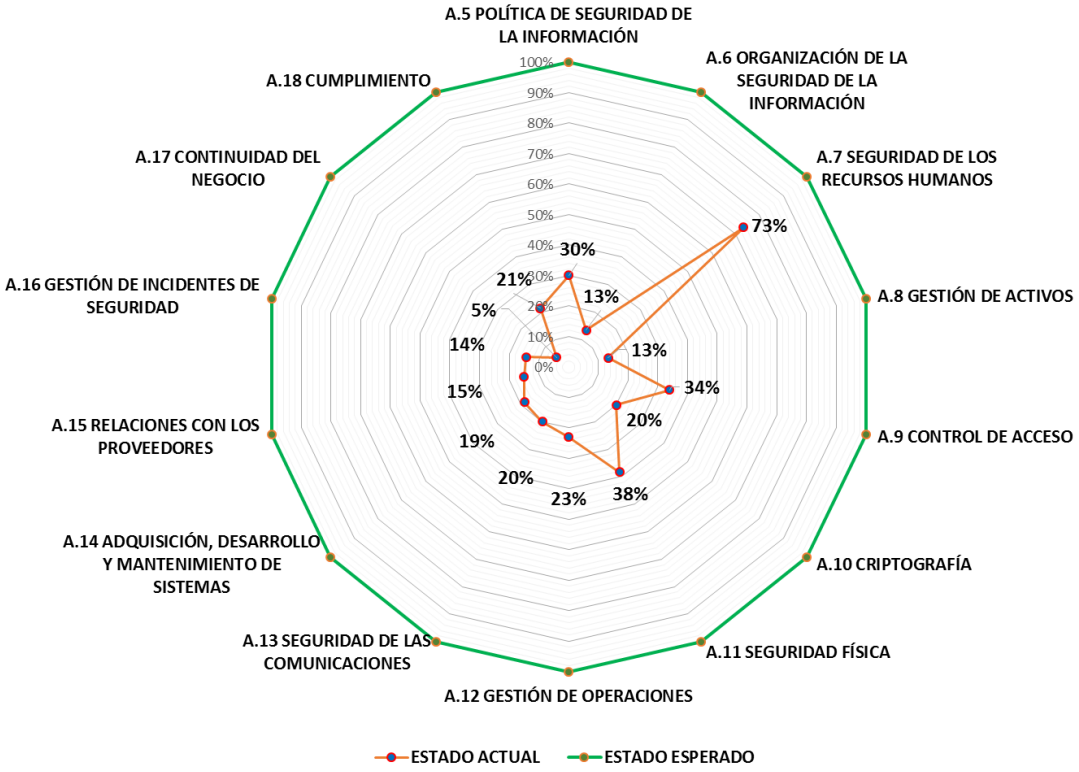


Ilustración 24. Estado real vs. Estado Ideal OAN

4.2.3. Centro Nacional de capacitación – CNC

Analizando el gráfico anterior se puede concluir que los dominios que se encuentran en el nivel Definido son: Seguridad en las comunicaciones, Relaciones con los proveedores, Gestión de operaciones y Adquisición, desarrollo y mantenimiento de sistemas. Por otra parte, los demás dominios se encuentran en los niveles *Inicial, Inexistente y Repetible*.

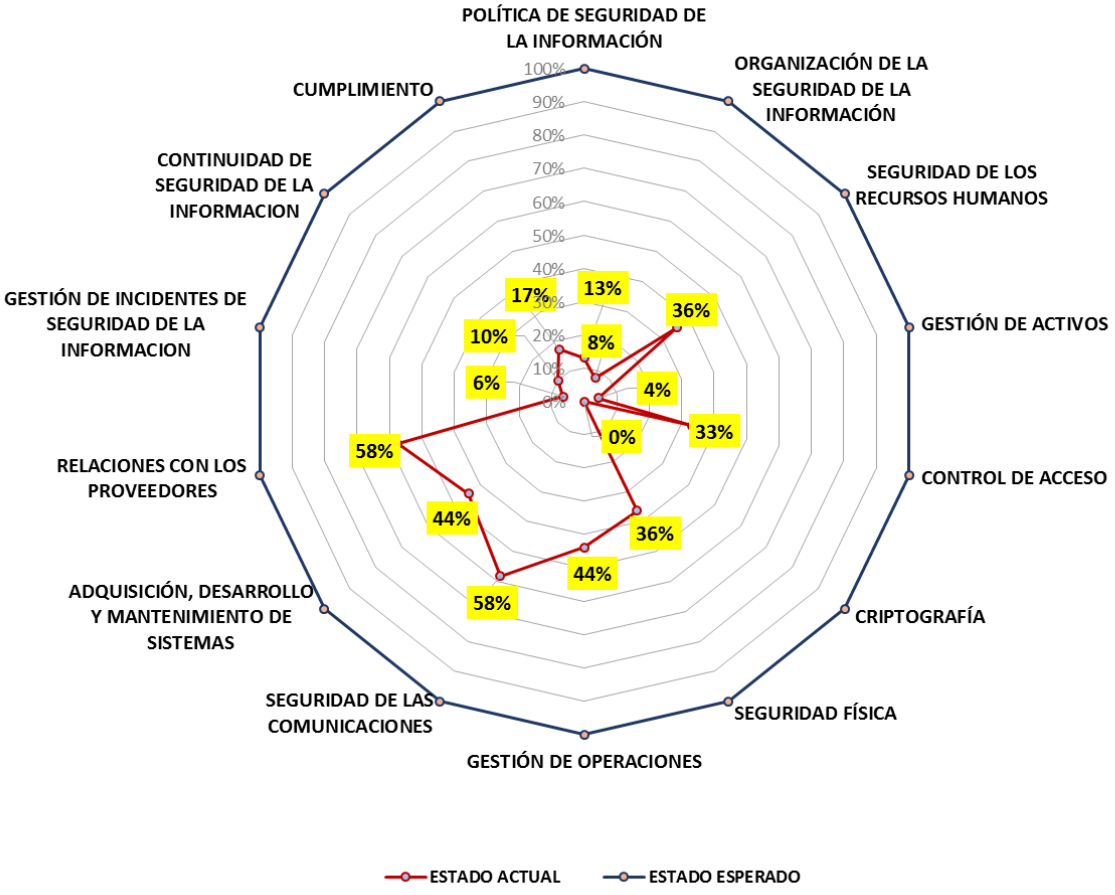


Ilustración 25. Estado real vs. Estado Ideal CNC

4.3. COMPARACIÓN DE LOS RESULTADOS DEL ANÁLISIS GAP

A continuación, se presenta un cuadro comparativo entre los resultados obtenidos con respecto a las cláusulas del 4 al 10 de la NTC/ISO 27001:

GRADO DE IMPLEMENTACIÓN Y CUMPLIMIENTO DE LAS CLAUSULAS	GSP	CNC	OAN
CONTEXTO DE LA ORGANIZACIÓN	13	0	0
LIDERAZGO	50	40	40
PLANIFICACIÓN	0	20	0
SOPORTE	57	29	40
OPERACIÓN	40	20	0
EVALUACIÓN DEL DESEMPEÑO	8	0	0
MEJORA	0	0	0
PROMEDIO	24%	16%	11%

Tabla 17. Cuadro comparativo entre resultados de cláusulas

En adelante se presenta el gráfico comparando los resultados obtenidos por las entidades a nivel de cláusulas:

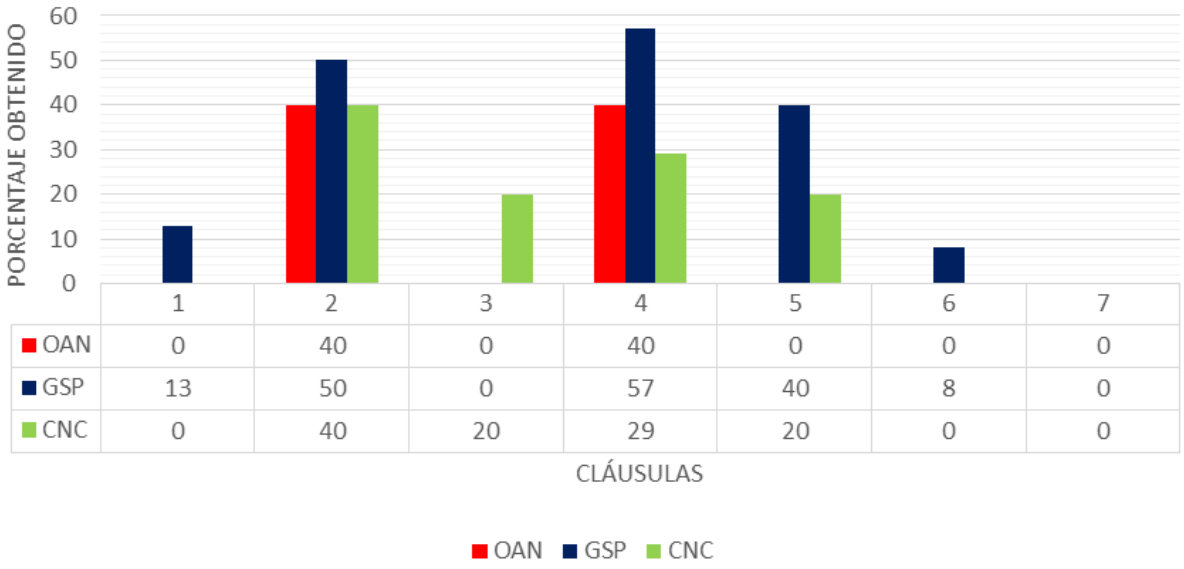


Ilustración 26. Gráfico comparativo entre los resultados de las cláusulas

Al analizar los resultados de obtenidos en el análisis GAP se puede evidenciar que de las 3 entidades evaluadas solo una, la GSP – Gestión de Servicios Públicos sobrepasa el 50% en 2 cláusulas obteniendo un promedio del 24% de cumplimiento en la evaluación de las Cláusulas. Para la evaluación de los Dominios se evidencia que esta misma entidad es la única que llega al 50% del total promediado de todos los Dominios.

Las entidades OAN y CNC no alcanzan al promedio del 20% para la evaluación de las Cláusulas y para la evaluación de los Dominios el promedio máximo de estas dos entidades no supera el 26%.

Analizando estos resultados vemos el poco desempeño que las entidades estatales han llevado hasta la vigencia 2017, evidenciando en parte la falta de compromiso y liderazgo que no supera el 50% para lograr los objetivos requeridos, podemos observar en todos los casos evaluados la falta de planificación, de evaluación del desempeño y mejora a los planes.

Ahora se presentan el cuadro comparativo entre los resultados obtenidos con respecto a los 14 dominios de la NTC/ISO 27001:

GRADO DE IMPLEMENTACION Y CUMPLIMIENTO DE LOS DOMINIOS	GSP	CNC	OAN
POLITICA DE SEGURIDAD DE LA INFORMACIÓN	50	13	30
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	33	8	13
SEGURIDAD DE LOS RECURSOS HUMANOS	85	36	73
GESTIÓN DE ACTIVOS	53	4	13
CONTROL DE ACCESO	71	33	34
CRIPTOGRAFÍA	0	0	20
SEGURIDAD FISICA	76	36	38
GESTION DE OPERACIONES	61	44	23
SEGURIDAD DE LAS COMUNICACIONES	60	58	20
ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	53	44	19
RELACION CON LOS PROVEEDORES	88	58	15
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	9	6	14
CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN	13	10	5
CUMPLIMIENTO	49	17	21
PROMEDIO	50%	26%	24%

Tabla 18. Cuadro comparativo entre resultados de los Dominios

En adelante se presenta el gráfico comparando los resultados obtenidos por las entidades a nivel de Dominios:

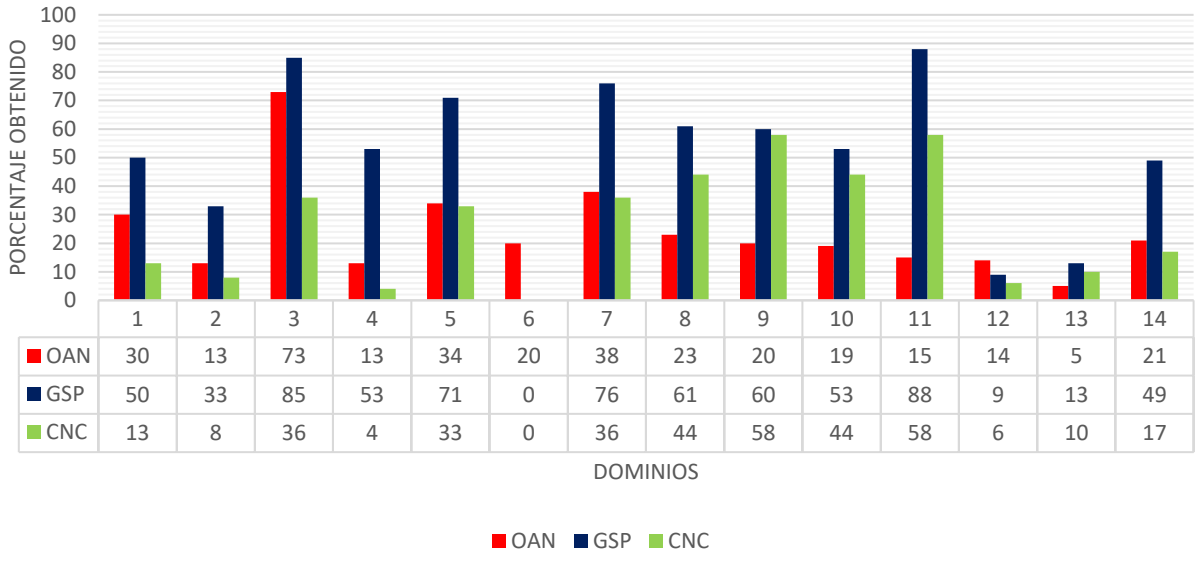


Ilustración 27. Gráfico comparativo entre los resultados de los Dominios

Para la evaluación por dominios vemos el poco progreso de implantación en la organización de la seguridad de la información, en la aplicación de controles criptográficos para mejorar la seguridad, en la gestión de los incidentes de seguridad de la información, continuidad del negocio y la falta de claridad en los planes para lograr los objetivos propuestos.

Como conclusión en la evaluación general de las cláusulas se puede decir que con un mejor liderazgo y unas evaluaciones constantes del desempeño y mejora en las entidades se puede llegar a cumplir con el objetivo establecido por el Gobierno.

4.4. PRINCIPALES HALLAZGOS

Teniendo en cuenta las cláusulas y dominios con menor nivel de madurez, se considera importante que éstas sean tratadas con mayor prioridad, por esta razón, a continuación, presentamos los principales hallazgos y recomendaciones.

Para la implementación del SGSI se recomienda:

- Entender claramente el contexto de la Entidad frente a seguridad de la información
- Contar con el apoyo de la alta dirección para la implementación del SGSI.
- Implementar un proceso de gestión de riesgos sobre los activos de información.
- Establecer los objetivos de seguridad de la información.
- Implementar un procedimiento de auditorías internas en seguridad de la información.
- Implementar un procedimiento para el tratamiento de no conformidades y acciones correctivas relacionadas con seguridad de la información.
- Establecer indicadores para medir el desempeño de la seguridad de la información y la eficacia del SGSI.

5. RESULTADOS

5.1. VARIABLES PARA DEFINIR EL PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI)

Una vez analizados los resultados del análisis GAP ejecutado en las 3 entidades de orden nacional seleccionadas, a continuación, se presenta las variables con las cuales se construyó el Plan Estratégico de Seguridad de la Información (PESI) diseñado para que cualquier entidad de orden nacional pueda cumplir con el Decreto 1078 de 2015 en un corto plazo y de manera eficiente.

Para ello fue necesario definir una serie de variables que ayudaron a la priorización de los diferentes dominios de la NTC/ISO 27001:2013. Los 14 dominios de la norma están conformados por 114 controles. El PESI propone una estrategia para la implementación basada en una serie

de variables que permiten inferir el orden de implementación de cada uno de los dominios teniendo en cuenta algunos aspectos asociados a cada uno de los controles. En la siguiente figura se presentan la matriz de valoración para cada una de las combinaciones posibles.

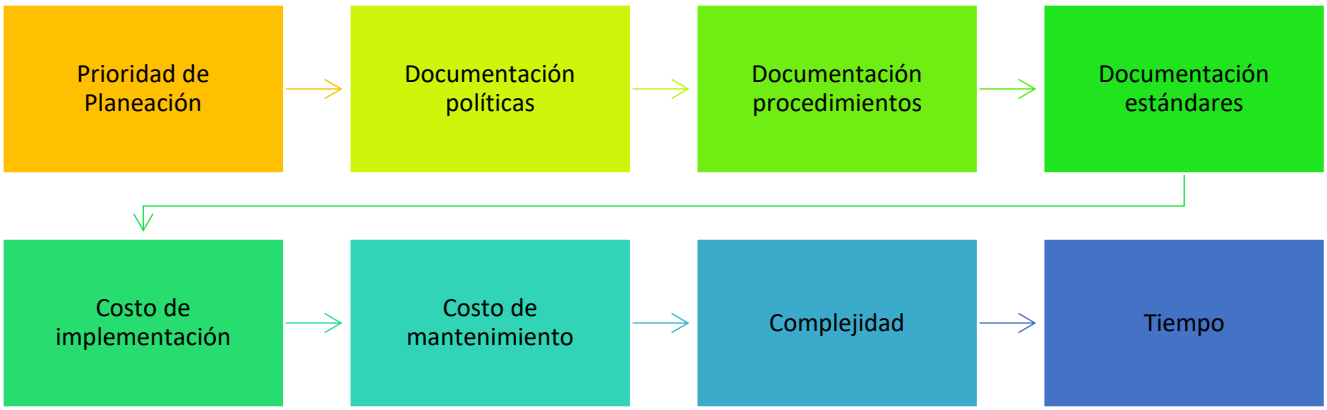


Ilustración 28. Variables analizadas.

Prioridad de Planeación: Esta variable considera los aspectos relacionados con el dominio desde el punto de vista de las categorías del tipo de control o dominio: administrativo (3), tecnológico (2) y físico (1) y los aspectos referentes a los niveles de planeación: estratégico (3), táctico (2) y operativo (1). Dependiendo de la conjunción de estos dos criterios (nivel de planeación y categorías del tipo del control o dominio) se asigna un valor que ayudará a definir la prioridad de implementación teniendo en cuenta la magnitud de este valor tal como se muestra en la siguiente figura (los valores de mayor a menor son: 9, 6, 4, 3, 2,1).

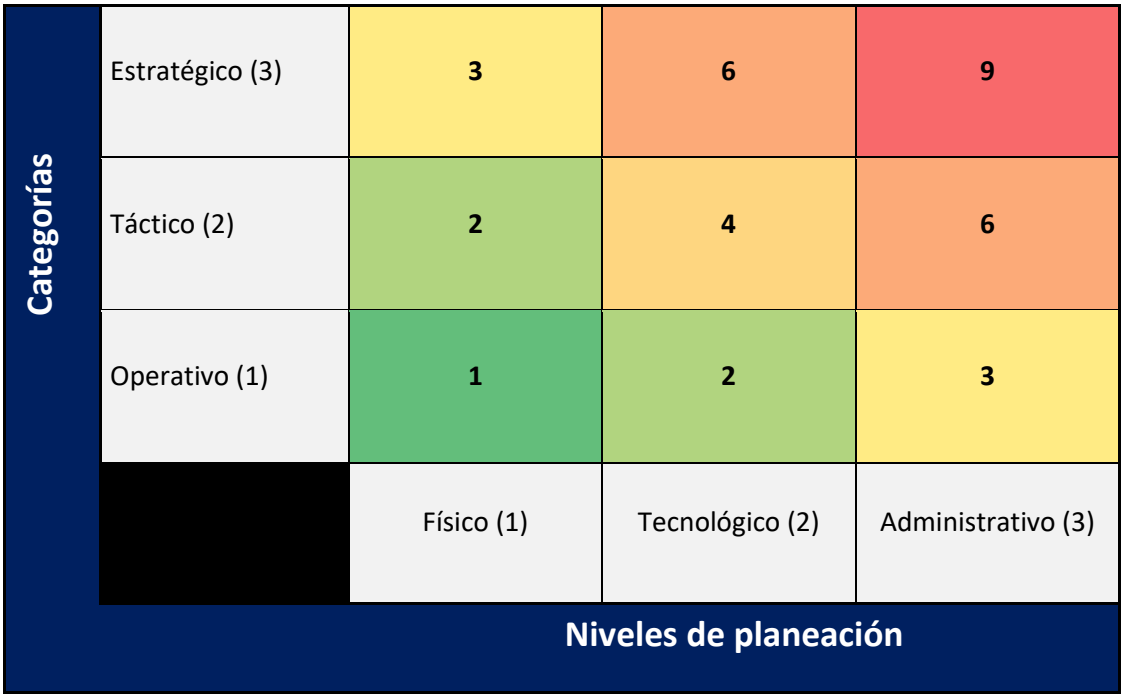


Ilustración 29. Prioridad

Documentación política: El esfuerzo asociado con la documentación de políticas por cada uno de los dominios se mide en esta variable. La cantidad de políticas y normas que hay que desarrollar por dominio es un estimativo que ayuda a estimar su prioridad de implementación.

Los niveles utilizados para calificar esta variable se muestran a continuación:

DOCUMENTACIÓN DE POLÍTICAS		
VALOR	**NIVEL**	**Rango Número de Políticas**
5	MUY ALTO	Entre 10 y 11
4	ALTO	Entre 7 y 9
3	MEDIO	Entre 5 y 6
2	BAJO	Entre 3 y 4
1	MUY BAJO	Entre 1 y 2

Tabla 19. Documentación de políticas

Documentación procedimientos: El esfuerzo requerido por cada dominio en el número de procedimientos requeridos para lograr la preservación de la seguridad de la información es uno de los aspectos considerados con el fin de asignarle una prioridad a la implementación de los

diferentes dominios. Los valores estimados de criticidad relacionados con el número de procedimientos estimado requerido se presenta a continuación:

DOCUMENTACIÓN DE PROCEDIMIENTOS		
VALOR	**NIVEL**	**Rango Número de Políticas**
5	MUY ALTO	Entre 8 y 9
4	ALTO	Entre 6 y 7
3	MEDIO	Entre 4 y 5
2	BAJO	Entre 2 y 3
1	MUY BAJO	Igual a 1

Tabla 20. Documentación de procedimientos

Documentación estándares: El esfuerzo requerido por cada dominio en el número de estándares requeridos para lograr la preservación de la seguridad de la información es uno de los aspectos considerados con el fin de asignarle una prioridad a la implementación de los dominios.

Los valores estimados de criticidad relacionados con el número de estándares estimado requerido se presenta a continuación:

DOCUMENTACIÓN DE ESTÁNDARES		
VALOR	**NIVEL**	**CRITERIOS (CANTIDAD)**
5	MUY ALTO	3
4	ALTO	2
3	MEDIO	1
2	BAJO	0
1	MUY BAJO	0

Tabla 21. Documentación de estándares

Costo de implementación: Cada uno de los dominios de la norma dependiendo de la cantidad de herramientas, software, servicios, infraestructura, horas hombre, entre otros aspectos, requerirá de unos esfuerzos financieros diferentes. De tal manera que se puede recomendar como parte de este Plan, que aquellos dominios con menor costo sean implementados en el menor tiempo posible con el fin de obtener lo que se conoce como ganancias tempranas lo que

a larga beneficiará la aceptación de todo lo concerniente a la seguridad de la información por parte de la entidad y mantendrá la motivación en niveles altos durante la fase de implementación del SGSI. La tabla utilizada para estimar de manera cualitativa el costo asociado a un dominio es la siguiente:

COSTO DE IMPLEMENTACIÓN		
VALOR	**NIVEL**	**CRITERIOS**
5	MUY ALTO	Mayor a 100.000$
4	ALTO	Entre 99.999$ y 60.000$
3	MEDIO	Entre 59.999$ y 20.000$
2	BAJO	Entre 19.999$ y 5.000$
1	MUY BAJO	Menor a 5000$

Tabla 22. Costos de implementación

Gasto de mantenimiento: Todo control asociado a un dominio tiene por su misma naturaleza unos gastos asociados en mantener su efectividad en el transcurso del tiempo. Estos gastos normalmente tienden a ser reiterativos y en algunos casos se requiere de un tercero para que cumpla con la función del mantenimiento.

La tabla utilizada para estimar de manera cualitativa los gastos asociados a un dominio es la siguiente:

GASTOS DE MANTENIMIENTO		
VALOR	**NIVEL**	**CRITERIOS**
5	MUY ALTO	Mayor a 100.000$
4	ALTO	Entre 99.999$ y 60.000$
3	MEDIO	Entre 59.999$ y 20.000$
2	BAJO	Entre 19,999$ y 5.000$
1	MUY BAJO	Menor a 5000$

Tabla 23. Gastos de mantenimiento

Complejidad: La variable complejidad considera las calificaciones requeridas en el recurso humano con el fin de acometer la implementación del dominio o control en cuestión, para ello se consideran los siguientes aspectos:

- Especialista
- Ingeniero
- Técnico
- Estudiante técnico o profesional
- Personal no calificado

La tabla utilizada para estimar de manera cualitativa la complejidad asociada a un dominio es la siguiente:

COMPLEJIDAD		
VALOR	**NIVEL**	**CRITERIOS**
5	MUY ALTO	Especialista
4	ALTO	Ingeniero
3	MEDIO	Técnico
2	BAJO	Estudiante técnico o profesional
1	MUY BAJO	Personal no calificado

Tabla 24. Complejidad

Tiempo: La variable tiempo le imprime al dominio unas restricciones importantes en lo referente al tema de cuándo se debe abordar su implementación. Se considera que si un control o dominio toma mucho tiempo para su implementación es recomendable abordarlo posteriormente para que de esta manera podamos implementar muchos más controles que sean de corta duración en su implementación y se aumenta rápidamente el porcentaje de cumplimiento de la norma de seguridad. No obstante, se debe considerar que estos controles de largo tiempo de implementación sean acometidos sin violar los requerimientos de tiempo de todo el proyecto.

La tabla utilizada para estimar de manera cualitativa el tiempo asociado a la implementación de un dominio determinado es la siguiente:

TIEMPO		
VALOR	**NIVEL**	**CRITERIOS**
5	MUY ALTO	Más de 1 mes
4	ALTO	entre 30 días y 15 días
3	MEDIO	Menos de una semana
2	BAJO	Menos de un día
1	MUY BAJO	Menos de 24 horas

Tabla 25. Tiempo

5.2. PESI

Con el fin de estimar las prioridades para cada uno de los dominios de la norma ISO 27001 se definieron una serie de variables que una vez calificadas se utilizaron para determinar la prioridad estratégica de implementación de los dominios y que fueron presentadas anteriormente. A continuación, se presenta la tabla con las variables que permiten estimar la Prioridad Estratégica de cada uno de los dominios de la norma. Esta Prioridad se estima en porcentaje lo que nos permitirá luego ordenar cada uno de los dominios y definir las 3 fases de implementación:

COSTO IMPLEMENTACIÓN (US$)	COSTO MANTENIMIENTO (US$)	COMPLEJIDAD	TIEMPO (meses)	Prioridad %	Fase
1	1	3	1	4,7%	1
1	1	3	1	4,7%	1

Tabla 26. Variables para el análisis de PESI

A continuación, se ilustra un ejemplo de la calificación en la matriz de Excel de los criterios de políticas y procedimientos frente a cada dominio y control:

# Dominio	Nombre dominio	# Control	Nombre control	Control			Dominio		
				Políticas	Procedimientos	Std	Políticas	Procedimientos	Std
A.5	Políticas de la seguridad de la información	**A.5.1.1**	Políticas para la seguridad de la información	0	0	0	1	1	0
A.5	Políticas de la seguridad de la información	**A.5.1.2**	Revisión de las políticas para la seguridad de la información	1	1	0			
A.6	Organización de la seguridad de la información	**A.6.1.1**	Roles y responsabilidades para la seguridad de la información.	1	1	0	7	7	2
A.6	Organización de la seguridad de la información	**A.6.1.2**	Separación de deberes.	1	1	0			
A.6	Organización de la seguridad de la información	**A.6.1.3**	Contacto con las autoridades	1	1	0			
A.6	Organización de la seguridad de la información	**A.6.1.4**	Contacto con grupos de interés especial	1	1	0			
A.6	Organización de la seguridad de la información	**A.6.1.5**	Seguridad de la información en la gestión de proyectos.	1	2	0			
A.6	Organización de la seguridad de la información	**A.6.2.1**	Política para dispositivos móviles	1	0	1			
A.6	Organización de la seguridad de la información	**A.6.2.2**	Teletrabajo	1	1	1			

Tabla 27. Ejemplo 1 Calificación de criterios en Excel

En seguida, se presenta un ejemplo de la calificación en la matriz de Excel de los criterios de costo de implementación, costo de mantenimiento, complejidad y tiempo, frente a cada dominio y control:

# Control	Nombre control	CALIFICACIÓN DE IMPLEMENTACIÓN por control			
		COSTO IMPLEMENTACIÓN (US$)	COSTO MANTENIMIENTO (US$)	COMPLEJIDAD	TIEMPO (meses)
A.5.1.1	Políticas para la seguridad de la información	300	100	4	0,5
A.5.1.2	Revisión de las políticas para la seguridad de la información	300	100	3	0,5
A.6.1.1	Roles y responsabilidades para la seguridad de la información.	150	50	4	0,25
A.6.1.2	Separación de deberes.	150	50	4	0,25
A.6.1.3	Contacto con las autoridades	150	50	4	0,25
A.6.1.4	Contacto con grupos de interés especial	150	50	4	0,25
A.6.1.5	Seguridad de la información en la gestión de proyectos.	150	50	4	0,25
A.6.2.1	Política para dispositivos móviles	150	50	4	0,25
A.6.2.2	Teletrabajo	150	50	4	0,25

Tabla 28. Ejemplo 2 Calificación de criterios en Excel

Con base en la prioridad estratégica procedemos a definir las diferentes fases que conformarán el proceso de implementación de los dominios de la norma. Se determinaron tres (3) fases principales para la implementación de todos los dominios. El tiempo estimado aproximado para la finalización de estas fases es de un año teniendo en cuenta aspectos legales, contractuales y la experiencia nuestra en proyectos similares, obviamente contando con la dedicación del líder de seguridad y los dos analistas. También a todo lo anteriormente expresado subyace la premisa de implementar los controles que toman menos tiempo y requieren menor esfuerzo, según lo reflejado por las variables definidas para el análisis del PESI.

En seguida, se presenta la prioridad y las fases de implementación, arrojadas por la herramienta luego de aplicar los criterios anteriormente definidos:

Fase	# Dominio	Nombre dominio	Prioridad %
Fase 1	**A.5**	Políticas de la seguridad de la información	4,7%
	A.6	Organización de la seguridad de la información	4,7%
Fase II	**A.10**	Criptografía	5,5%

Fase	# Dominio	Nombre dominio	Prioridad %
	A.15	Relaciones con los proveedores	5,5%
	A.16	Gestión de incidentes de seguridad de la información	5,5%
	A.18	Cumplimiento	5,5%
	A.7	Seguridad de los recursos humanos	7,0%
	A.8	Gestión de activos	7,0%
	A.14	Adquisición, desarrollo y mantenimiento de sistemas	7,0%
	A.9	Control de acceso	7,8%
	A.12	Seguridad de las operaciones	7,8%
	A.13	Seguridad de las comunicaciones	7,8%
Fase III	**A.17**	Aspectos de seguridad de la información de la gestión de continuidad de negocio	11,7%
	A.11	Seguridad física y del entorno	12,5%

Tabla 29. Ejemplo Prioridades y Fases de Implementación arrojadas por la herramienta

En la siguiente gráfica se pueden observar los dominios asociados por cada una de las fases consideradas, teniendo en cuenta la prioridad estratégica calculada para los dominios. Los dominios de la Fase I son: A5, A.18, A.16, A.10, A.15, los de la Fase II son: A.17, A.6, A.12, A.8, A.7, A.13 y los de la última fase son: A.14, A.9, A.11.

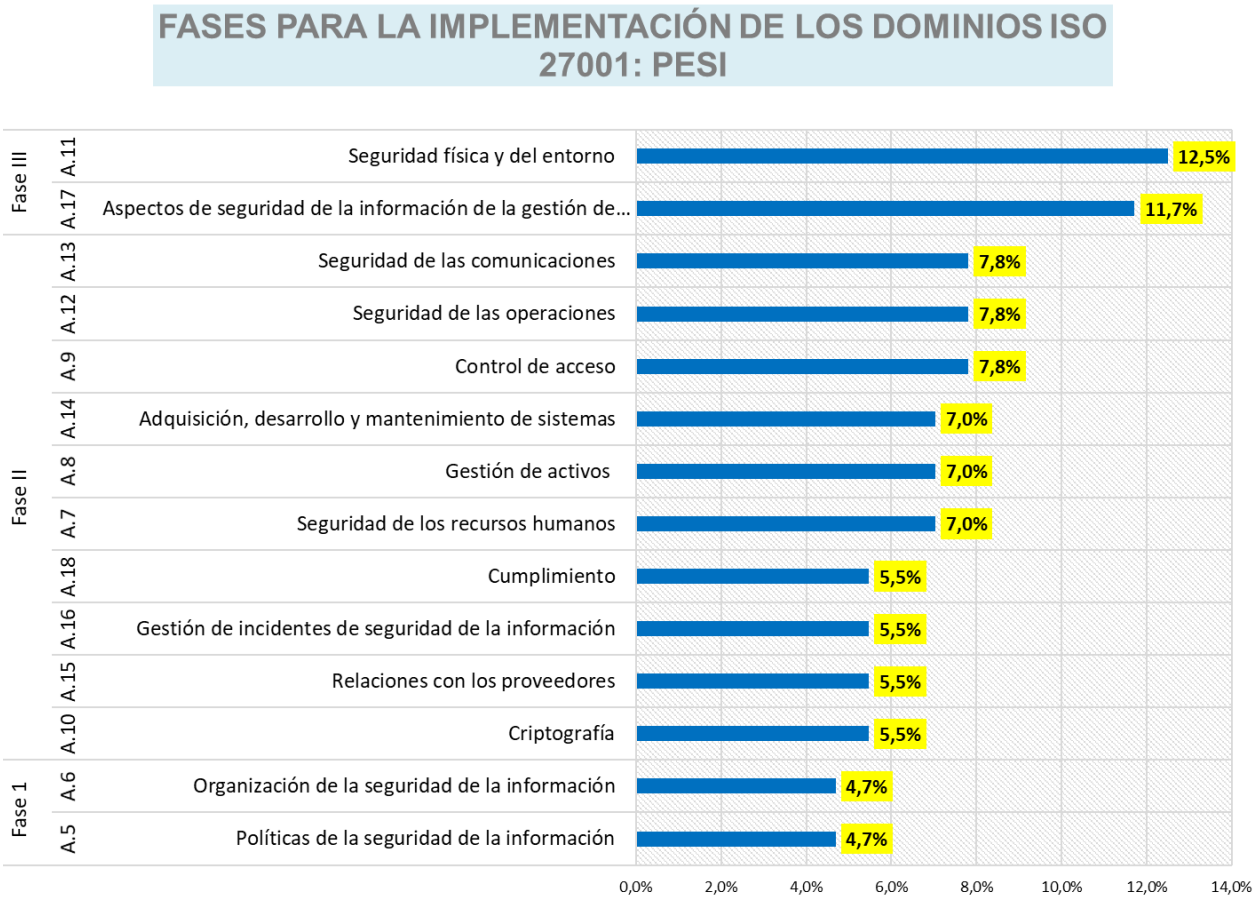


Ilustración 30. Fases de la implementación de los dominios ISO 27001

5.3. APLICACIÓN DEL PESI EN EL CNC

El PESI fue aplicado en el Centro Nacional de Capacitación CNC, una de las entidades analizadas; sí la entidad implementara el PESI, ésta podría aumentar su cumplimiento hasta en un **49%** frente a los resultados obtenidos en el Análisis GAP, del **26%** pasaría al **75%** de cumplimiento, lo que confirma la eficacia de la herramienta.

A continuación, se presenta la evolución que tendría la entidad una vez inicie la implementación del PESI:

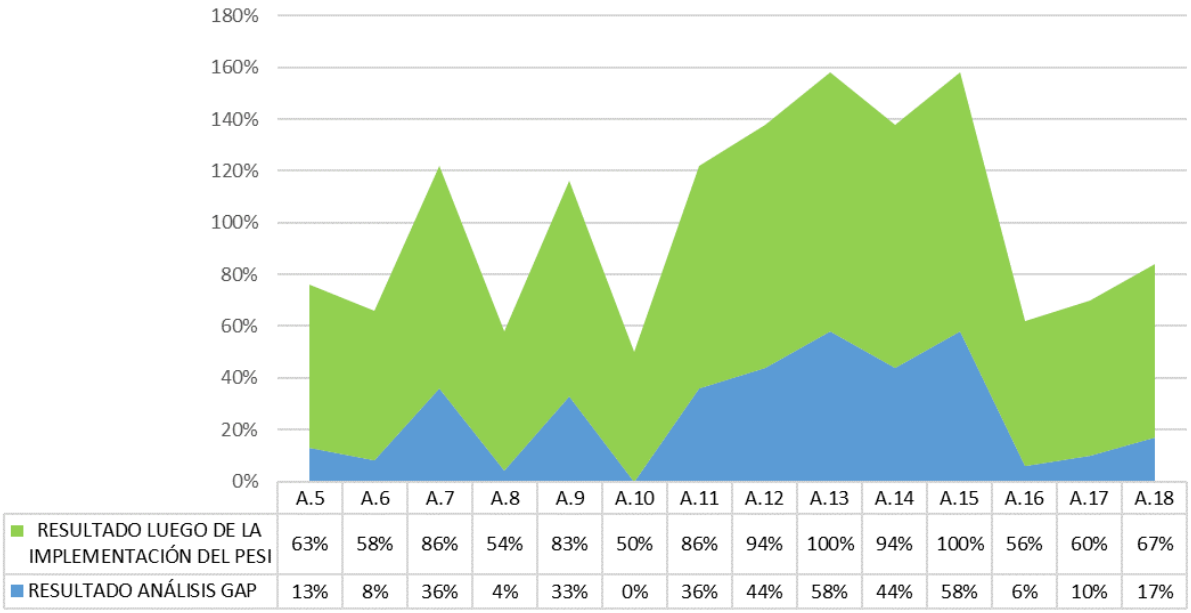


Ilustración 31. Análisis GAP vs. PESI de la CNC

En seguida se presenta un cuadro comparativo entre los resultados del análisis GAP vs. Los resultados que la entidad obtendrá sí, implementa el PESI bajo los criterios simulados:

GRADO DE IMPLEMENTACIÓN Y CUMPLIMIENTO DE LOS DOMINIOS	RESULTADO ANÁLISIS GAP	RESULTADO LUEGO DE LA IMPLEMENTACIÓN DEL PESI
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	13%	63%
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	8%	58%
SEGURIDAD DE LOS RECURSOS HUMANOS	36%	86%
GESTIÓN DE ACTIVOS	4%	54%
CONTROL DE ACCESO	33%	83%
CRIPTOGRAFÍA	0%	50%
SEGURIDAD FÍSICA	36%	86%
GESTIÓN DE OPERACIONES	44%	94%
SEGURIDAD DE LAS COMUNICACIONES	58%	100%
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	44%	94%
RELACIÓN CON LOS PROVEEDORES	58%	100%
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	6%	56%
CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN	10%	60%
CUMPLIMIENTO	17%	67%
PROMEDIO	**26%**	**75%**

Tabla 30. Incremento en cumplimiento por PESI

5. DISCUSIONES Y CONCLUSIONES

- Una vez desarrollado el plan de trabajo propuesto, se concluye que el PESI responde a las necesidades de las entidades de orden nacional con respecto a la implementación del MSPI enmarcado en el Decreto 1078 de 2015.
- Se dio cumplimiento al objetivo propuesto, la metodología y el plan de trabajo se desarrolló de acuerdo a lo proyectado, como resultado de ello se diseñó y se presentó el PESI.
- Los resultados obtenidos de la implementación del PESI en la CNC, confirman que el análisis, la metodología y el plan de trabajo desarrollado fueron asertivos y acorde con la naturaleza, tamaño y estructura de las entidades de orden nacional analizadas, lo que representa una herramienta útil y oportuna para la implementación del MSPI.
- Si bien el PESI se ajusta al actual modelo MSPI, es importante que las entidades de orden nacional que lo adopten lo actualicen sí se presenta algún cambio en el Decreto o en las cuestiones internas y externas que las rodean.
- Para la implementación del PESI, las entidades de orden nacional deben tener una estructura organizativa compuesta al menos por:
    - Un **comité de seguridad de la información** en el cual se debe integrar la alta gerencia. Este comité es el órgano máximo del modelo de seguridad. Sus funciones principales, entre otras, podrían ser:
        - Definir los lineamientos y estrategias de Seguridad de la información en función de los objetivos del negocio.
        - Aprobar el modelo de seguridad de la entidad (políticas, normas, procedimientos, etc.).
        - Aprobar el PESI, así como los resultados de su implementación.
    - **Líder de seguridad de la Información de la Entidad.** Es el encargado de coordinar todo el modelo de seguridad. Debe estar dedicado tiempo completo a temas de seguridad y debe velar por el mejoramiento continuo del modelo de seguridad. Debe establecer comunicación constante con las autoridades pertinentes, así como los organismos de interés en temas de seguridad.
    - **Analista de seguridad de la información.** Son funcionarios dedicados tiempo completo a temas de seguridad de la información y que realizan labores operativas del modelo de seguridad. Son dirigidos por el líder de seguridad de la información. En lo posible, la entidad debe contar como mínimo con dos funcionarios para este rol.

      Otros roles sugeridos a futuro dentro de la entidad de seguridad podrían ser:

- Administrador de recursos informáticos
- Administrador de control de acceso lógico
- Operador de seguridad de la información
- Líder de seguridad física
- Líder de recursos humanos
- Líder de organización y métodos o líder del sistema de calidad
- Auditor de Seguridad
- Asesor legal

- El PESI presentado se diseñó de acuerdo con las necesidades de las 3 entidades analizadas, no obstante, el PESI es una herramienta flexible y dinámica, es decir, cada entidad puede reevaluar las variables aquí proyectadas y adaptarlo de acuerdo a sus expectativas.

6. ANEXOS

- Herramienta PESI en Excel.

7. GLOSARIO

- **Amenaza**: Posible acción de un incidente inesperado, que puede afectar a un sistema u organización.
- **Análisis**: Estudio de forma meticulosa para determinar mediciones de las características y cualidades de un objeto, medio, reporte, estudio o de una cosa para sacar conclusiones o verificar su estado e identificar los componentes de un todo.
- **Análisis GAP:** Gap Analysis (del inglés, análisis de brecha) herramienta que ayuda a las organizaciones a evaluar el estado y desempeño real actual en tecnología, infraestructura, procesos, gestión del talento humano y situaciones en un momento dado, relacionando uno o varios puntos seleccionados como referencias de variables en el orden local, regional, nacional y/o internacional.
- **Ataque**: Es la acción de Intentar destruir, falsificar, difundir, inutilizar, hurtar u obtener acceso no autorizado o hacer un uso no autorizado de un activo.
- **Autoridad**: Es el derecho de emprender acciones y tomar decisiones.
- **Confidencialidad**: Es un atributo de la información, esta se limita su disposición y no es revelada a terceros sin previa autorización.
- **Contratista**: Persona natural o jurídica que se vincula a la entidad con el objeto de prestar al Instituto un bien o un servicio determinado.
- **Control**: Medida que modifica el riesgo.
- **Dato personal**: Es la información personal que determina a los individuos y está almacenada en medios físicos, virtuales o electrónicos y contiene información de carácter público, semiprivado o privado e íntimo, esta información es vinculada a una o varias personas naturales.
- **Disponibilidad**: se refiere a la posibilidad de que un sistema sea asequible a individuos o entidades y que hace posible dar respuestas o resolver problemas o mostrar un resultado de una consulta con autorización cuando lo requieran.
- **FURAG**: Formulario único de reporte de avances y gestión.
- **Integridad**: Propiedad de Salvaguardar la exactitud y estado completo de los activos.
- **MinTic**: Ministerio de la Información y las Comunicaciones.

- **MSPI**: Modelo de Seguridad y Privacidad de la Información reglamentado por el Decreto 1078 de 2015.
- **PESI:** Plan Estratégico de Seguridad de la Información.
- **Seguridad de la Información**: Son el conjunto de parámetros de prevención y control que las organizaciones en sus sistemas de información y sistemas tecnológicos emplean para asegurar los activos de información y garantizar la confidencialidad, disponibilidad e integridad de los mismos.
- **Subcontratar**: Hacer un arreglo donde una organización externa realiza parte de una función o proceso de las organizaciones.
- **Vulnerabilidad:** Es el riesgo que un activo o un control puede sufrir frente a un peligro donde no tiene defensas necesarias en caso de ataques.

8. REFERENCIAS

Cisco 2016 Informe anual de seguridad 2 Resumen ejecutivo. (2016), 87. Retrieved from https://www.cisco.com/c/dam/m/es_mx/assets/offers/pdfs/cisco_2016_asr_011116_es-xl.pdf

Cisco. (2017). *Informe anual sobre ciberseguridad 2017*.

Marulanda Echeverry, C. E., López Trujillo, M., & Valencia Duque, F. J. (2017). Gobierno y gestión de ti en las entidades públicas. *AD-Minister*, (31), 75–92. https://doi.org/10.17230/ad-minister.31.5

El Tiempo. (2016). Cuántos delitos informáticos se denuncian en Colombia - Archivo Digital de Noticias de Colombia y el Mundo desde 1.990 - eltiempo.com. Retrieved May 6, 2018, from http://www.eltiempo.com/archivo/documento/CMS-16493604

Resultados del Índice GEL 2016 en entidades del orden nacional y territorial - Estrategia GEL. (n.d.). Retrieved May 5, 2018, from http://estrategia.gobiernoenlinea.gov.co/623/w3-article-54794.html

Fortalecimiento TI. (n.d.). Retrieved from http://www.mintic.gov.co/gestionti/615/w3-channel.html

POLICIA NACIONAL DE COLOMBIA. (2017). Amenazas de Cibercrimen en Colombia 2016-2017. Retrieved from https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

MinTIC. (2014). Decreto Número 2573 de 2014, 1–9.