UNIVERSIDAD EAN
FACULTAD DE ESTUDIOS EN AMBIENTES VIRTUALES
MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN Y PROYECTOS TECNOLÓGICOS

DISEÑO DE LOS EJES TEMÁTICOS DE LA ESTRATEGIA GOBIERNO EN LÍNEA TIC SERVICIOS Y SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA EL CONCEJO DISTRITAL DE CARTAGENA

AUTORES
MILADIS ISABEL BLANCO CARRILLO
YORLADIS ESTELA BLANCO CARRILLO

DIRECTOR TRABAJO DE GRADO
JUAN GABRIEL GANTIVA VERGARA

CARTAGENA DE INDIAS, 27 DE MAYO DE 2018

DEDICATORIA

A Dios que está en los cielos y nos permitió cursar esta Maestría, creemos que sin el padre celestial no hubiese sido posible.

A las personas que nos aman y amamos quienes sacrificaron su tiempo para apoyarnos en este gran logro.

A nuestros esposos a nuestros hijos que nos apoyaron para lograr este triunfo.

Los autores.

AGRADECIMIENTOS

Queremos expresar nuestros más sinceros agradecimientos a:

A nuestro Director de trabajo de grado Juan Gabriel Gantiva Vergara por su apoyo, guía y aportes durante la realización del trabajo de grado.

Al Ministerio de las tecnologías de la información por el apoyo para el desarrollo de la Maestría.

A la Universidad EAN por permitirnos cursar en su prestigiosa institución.
Al Concejo Distrital de Cartagena y

A todas las personas que contribuyeron con la realización de este proyecto

A todas infinitas gracias,

Los autores

RESUMEN

El presente trabajo tiene como objetivo diseñar los Ejes Temáticos de la Estrategia Gobierno en Línea TIC servicios y Seguridad y Privacidad de la Información para el Concejo Distrital de Cartagena, en base a la estrategia Gobierno en Línea con el fin de apoyar a la entidad en el cumplimiento de la Normatividad en materia de Gobierno digital establecida por el Estado Colombiano.

A través del Diseño de los ejes temáticos Tic Servicios y Seguridad y privacidad de la información El Concejo Distrital de Cartagena contará con una herramienta que le permitirá brindar trámites y servicios electrónicos con calidad, teniendo en cuenta las necesidades del ciudadano, además de lograr que la entidad proteja la información que genera, sensibilizando a los funcionarios de la importancia que la seguridad de la información tiene para la permanencia de la empresa en el mercado y la protección de los activos de información de las áreas administrativa, financiera y atención al usuario que le garantice altos niveles de confidencialidad, integridad y disponibilidad.

El diseño de los ejes temáticos de la estrategia gobierno en línea TIC servicios y seguridad y privacidad de la información para el Concejo Distrital de Cartagena parte de un diagnóstico inicial donde se revisa el estado de los trámites, servicios de acuerdo a los logros establecidos en la Estrategia Gobierno en línea y la seguridad de la información tomando como referencia el MSPI el cual toma como marco la Norma ISO 27001:2013, a través de este diagnóstico se determina el nivel de madurez de los ejes y se plantean las estrategias que permitirán la mejora en la prestación de los servicios, tramites digitales, protección de los activos de información y asignación de roles para la seguridad de la información.

Se realiza la valoración de los activos de información y sus riesgos siguiendo la metodología Margerit, así mismo se dan las recomendaciones para proteger la información de la entidad, lograr la mejora de los procesos y procedimientos de las distintas áreas que intervienen tales como administrativa, financiera y atención al usuario.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE IMÁGENES

LISTA DE GRÁFICOS

LISTA DE ANEXOS

1. INTRODUCCIÓN

Entendiendo que la globalización y el auge tecnológico está transformando el orden de las cosas en todas las esferas de la sociedad, logrando grandes cambios (Munster Infante, 2003), que permiten innovar científica y tecnológicamente, marcando una nueva era, la era de la información y el conocimiento, así también el estado ha sufrido grandes transformaciones, que le ha permitido cambiar la manera de operar y la forma en que se relaciona con la sociedad (Mintic, 2012). Es así que la globalización ha demandado innovación y desarrollo de nuevos procesos basados en las tecnologías para el estado.

Teniendo en cuentas que estas (las Tecnologías de la Información y las Comunicaciones) deben servir al interés general y es deber del estado promover su acceso eficiente y en igualdad de oportunidades a todos los habitantes del territorio nacional. (Ley N° 1341 de 2009).

En este contexto nace para el estado Colombiano **La estrategia Gobierno en línea** con el fin de modernizar y fortalecer la administración pública, buscando eficiencia y eficacia, siendo obligatorio para todas las entidades nacionales, departamentales y municipales su adopción y desarrollo con el fin de lograr aumentar la eficiencia de la gestión pública, mejorar los servicios ofrecidos a los ciudadanos y proveer a las acciones del gobierno en un marco mucho más transparente" (Sánchez y Rincón, 2012).

Para el estado colombiano es de gran importancia brindar a la ciudadanía nuevas formas de realizar sus trámites y servicios, generando una relación más fácil, con menores costos y que genere mayor confianza y satisfacción (mintic, 2012).

Sin embargo, muchas entidades aún no han desarrollado la estrategia gobierno en línea, de ahí la decisión de realizar este proyecto, el cual emerge cuando se ve la necesidad que tiene el Concejo Distrital de Cartagena de prestar servicios adecuados a la ciudadanía. Que la entidad disponga de trámites y servicios en línea donde el ciudadano se sienta satisfecho, ahorre tiempo y dinero y se proteja la información, todo esto utilizando las tecnologías de la información y las comunicaciones disminuyendo los riesgos los cuales generan retrasos, inconformismos dentro y fuera de la organización.

En el presente proyecto se **desarrolla el Diseño de los ejes temáticos TIC servicios y seguridad y privacidad de la información** de la estrategia gobierno en línea del estado Colombiano dentro de Concejo Distrital de Cartagena para determinar los factores necesarios que permitan el diseño de esta estrategia dentro de la entidad, con el fin de que se realice un adecuado uso de las TIC en sus relaciones con los ciudadanos y determinar qué medidas tomar que permitan garantizar la seguridad y privacidad de la información.

El presente documento se encuentra organizado por veinte dos capítulos en donde se desarrolla el proyecto denominado Diseño de los Ejes Temáticos de la Estrategia Gobierno en línea TIC servicios y seguridad y privacidad de la Información para el Concejo Distrital de Cartagena.

Inicialmente se encuentra el resumen, este le permite adentrarse al lector en el proyecto que se desarrolla.

En el primer capítulo del trabajo se encuentra la introducción en la cual se realiza una descripción por componente y elementos claves de los cuales consta el proyecto.

En el segundo capítulo se encuentra la formulación de problema de investigación, el cual contiene la descripción, la justificación, las preguntas y los objetivos de investigación dejando en evidencia la importancia que tiene para la entidad Concejo Distrital de Cartagena de Indias, la protección de su activo más importante como es la información, en este ítem se detalla además el alcance y las limitaciones que se tienen al realizar el proyecto de investigación.

Para el Concejo Distrital de Cartagena de Indias es de gran importancia diseñar los ejes temáticos TIC servicios y Seguridad y privacidad de la información no solo por requerimientos de los entes de control como la Contraloría Distrital de Cartagena en donde se establece en el último informe de auditoría realizada en el 2017 las siguientes observaciones (Contraloría Distrital de Cartagena, 2017).

Observación numero 9: “No se evidencia que la entidad auditada haya definido plan de acción y/o mapa de ruta para la vigencia 2016, el cual contenga los servicios y trámites para ser dispuestos en línea, proyectos de mejoramiento para gestión institucional e interinstitucional con el uso de modelos electrónicos y demás acciones que requieran

priorizar para masificar la oferta de gobierno en línea con base en lo señalado en cada componente de la estrategia”

Observación N° 13 “La entidad no cuenta con una política de manejo y control de la información hallazgo de la auditoria anterior además de no cumplir con el lineamiento POLÍTICAS Y ESTÁNDARES PARA LA GESTIÓN Y GOBERNABILIDAD DE TI – es necesario identificar y definir las políticas y estándares que faciliten la gestión y la gobernabilidad de TI, contemplando por lo menos los siguientes temas: Continuidad, seguridad, gestión de la información, adquisición tecnológica, desarrollo e implantación de los sistemas de información, acceso a la tecnología y uso de las facilidades por parte de los usuarios. Así mismo debe contar con un proceso integrado entre las instituciones del sector que permitan asegurar el cumplimiento y actualización de las políticas y estándares TI”.

Si no también los innumerables beneficios del uso de las tecnologías de la información, que van desde poder ofrecer nuevos servicios, nuevas tareas y cubrir múltiples necesidades a concebir nuevas ideas y oportunidades para el crecimiento de la empresa lo que permite mejorar los servicios que se prestan aumentando la competitividad.

La implantación de un gobierno corporativo TIC establecido en el decreto nacional 2573 de 2014 apoya la creación de un estado más eficiente, más transparente y más participativo gracias a la TIC, prestando los mejores servicios en línea al ciudadano, logrando la excelencia en la gestión, empoderando y generando confianza en los ciudadanos e impulsando y facilitando las acciones requeridas para avanzar en los objetivos de desarrollo sostenible ODS - facilitando el goce efectivo de los derechos a través del uso de las TIC. (Mintic, 2018).

Además de traer los siguientes beneficios para la entidad (Ballester Fernández, 2018):

- Adecuada aplicación y operación de activos de TIC.
- Asignación de responsabilidades.
- Continuidad del negocio
- Sostenibilidad.
- Alineación de TIC con los objetivos del negocio.
- Asignación eficiente de recursos.

- Innovación en los servicios, los mercados y las empresas.
- Mejora de imagen y reputación en el mercado frente a los reguladores, agentes sociales y con los Stakeholder.
- Optimización en los costes de una organización
- Inversión efectiva en TIC
- Cumplimiento legal.

El objetivo del proyecto es mejorar la prestación de servicios de la entidad, salvaguardando los datos de los ciudadanos, para esto se realiza un diagnostico donde se presenta la situación actual del Concejo Distrital de Cartagena frente a la estrategia Gobierno en línea en los Ejes Temáticos tic servicios y seguridad y privacidad de la Información a través de este se diseñan las estrategias para cumplir con lo establecido en la Estrategia Gel así:

- Caracterización de los ciudadanos.
- Accesibilidad y usabilidad de los trámites y servicios que presta la entidad.
- Estrategias de promoción de los trámites electrónicos.
- Criterios de evaluación de la satisfacción del usuario de trámites y servicios electrónicos.
- Protocolos de atención para canales electrónicos.
- Manual de políticas de seguridad de la información.
- Roles y responsabilidades de la seguridad y privacidad de la información.
- Clasificación de los activos de información de los procesos de Atención al Usuario, Administrativa y Financiera.
- Valoración de los riesgos de seguridad que permita definir planes de tratamiento de riesgos de acuerdo a la metodología señalada.

El alcance del proyecto está dirigido a mejorar los trámites y servicios del Concejo Distrital de Cartagena que respondan a las necesidades de los ciudadanos y elaborar el manual de las políticas de seguridad a seguir por los colaboradores del Concejo, con esta investigación plantearemos todos los controles que sean imperiosos para aminorar los riesgos identificados, realizando la valoración de activos de información con su respectiva matriz de riesgos, asignando roles y responsabilidades. El trabajo de investigación es institucional diseñando una propuesta enfocada en los procesos de

atención al usuario, dirección administrativa y dirección financiera, áreas claves donde se desarrolla la misión institucional, revisando los trámites y servicios que presta la entidad en la actualidad y los trámites y servicios que requiere la ciudadanía y que se puedan prestar dentro de la estrategia gobierno en línea. En el área de seguridad y privacidad de la información se revisará la protección de los activos de información de los procesos de gestión financiera, gestión administrativa y atención al usuario, definiendo políticas y procedimientos que permitan el mejoramiento de la seguridad y privacidad de la información.

La entidad cuenta actualmente con nueve procesos correspondiente al 100% de los procesos que se desarrollan en la entidad de estos se excluye el 66,6% revisando un 33,3% de estos, los cuales corresponde a los procesos de Atención al usuario, administrativa y financiera, los procesos que se excluyen son los siguientes procesos: acciones y control político, control interno, evaluación independiente, gestión jurídica y direccionamiento estratégico, estos se desarrollaran en fases futuras, igualmente al tratarse de un diseño no abarca etapas de implementación, revisión, mantenimiento y mejora.

El tercer capítulo muestra la metodología que se sigue para el desarrollo del Diseño de los Ejes Temáticos de la Estrategia Gobierno en Línea TIC Servicios y Seguridad y Privacidad de la información definiendo el enfoque, el tipo de investigación, tipo de estudio, población y muestra, variables e hipótesis a demostrar, además de los diferentes métodos que se utilizaran para obtener la información.

En el cuarto capítulo se realiza un esquema del marco teórico siendo un abre bocas para el desarrollo del trabajo, detallando la normatividad que aplica en seguridad de la información y se profundiza con más detalles los temas referentes a los ejes temáticos de la estrategia además de lo concerniente a Tic Servicios y seguridad y privacidad de la información como son:

- Estrategia Gobierno en Línea
- TIC Servicios
- Seguridad de la información
- Gobierno de las tecnologías de comunicación

- Norma ISO 27001: 2013 documentación, requisitos
- COBIT
- Gobierno electrónico
- Metodología de análisis de riesgos

En el quinto capítulo se detalla el marco teórico de la investigación como es: Gobierno en Línea, alcance, normatividad, componentes de la estrategia, logros, tic servicios y modelo de seguridad y privacidad de la información.

Los resultados esperados se exponen en el sexto capítulo citando las actividades puntuales que se realizaran para llevar nuestro objetivo. En el séptimo capítulo el lector puede encontrar el plan de implementación contribuciones originales esperadas, viabilidad de la investigación, plan de acción para la intervención, Índice tentativo del proyecto, cronograma de desarrollo del trabajo de grado. El análisis de la estructura funcional y organizacional del Concejo Distrital de Cartagena se encuentra en el capítulo octavo, donde se describe la cadena de valor, estructura organizacional, planeación estratégica, valores, funciones y el estado del arte del proyecto.

El diagnóstico de los ejes temáticos TIC Servicios y Seguridad y Privacidad de la Información se desarrolla en el noveno capítulo del proyecto, donde se realiza análisis de los resultados de las encuestas realizadas a los funcionarios y visitantes del Concejo Distrital de Cartagena.

En los capitulo diez y once se observa la situación actual del Concejo Distrital de Cartagena frente a la Estrategia gobierno en línea y en el capítulo doce se definen cuáles serían las estrategias a diseñar para establecer un gobierno corporativo basado en las TICS en el Concejo Distrital de Cartagena frente a la estrategia gobierno en línea.

En los capítulos trece, catorce, quince, dieciséis y diecisiete se desarrollan las estrategias para el desarrollo del eje temático Tic Servicios de acuerdo a los objetivos, se realiza la caracterización de usuarios, se definen las características de usabilidad y accesibilidad de la página web, se establecen las estrategias de promoción de trámites y servicios, se diseña la guía para establecer los criterios de evaluación de los trámites y servicios, se definen un protocolo de atención al ciudadano digital.

El desarrollo de las estrategias para el eje temático seguridad y privacidad de la información se da en los capítulos dieciocho, diecinueve y veinte, definiendo en estos los roles y las responsabilidades para la seguridad de la información, diseñando las políticas de seguridad y privacidad de la información y se realiza la clasificación de activos y plan de tratamiento de riesgos.

Como se dijo anteriormente el diseño se trabajará en base al 33,3% de los procesos los cuales corresponde a los procesos de Atención al usuario, administrativa y financiera, excluyendo el 66,6% de los procesos los cuales corresponden a:

- Acciones y control político,
- Control interno,
- Evaluación independiente,
- Gestión jurídica y
- Direccionamiento estratégico,

Estos se desarrollarán en fases futuras, igualmente al tratarse de un diseño no abarca etapas de implementación del modelo, sin embargo, se incluye un plan de implementación en el capítulo veintiuno, el cual señala:

- Actividades
- Objetivos
- Responsables de la implementación
- Riesgos y medidas de tratamientos
- Costos de implementación

Este Plan de intervención cual puede ser usado a futuro por parte de la alta dirección en miras a cumplir con la normatividad y mejorar la imagen y seguridad de la entidad.

Por ultimo encontramos las conclusiones, recomendaciones y bibliografía del trabajo.

2. FORMULACIÓN DEL PROBLEMA

2.1. Descripción del problema de investigación

Al no contar el Concejo Distrital de Cartagena de Indias con el **Diseño de la Estrategia Gobierno en Línea** en el área de TIC servicios y seguridad y privacidad de la información entidad no cuenta con los recursos necesarios para ser una entidad acorde a las exigencias del estado trayendo como consecuencia ineficiencia en la prestación de los trámites y servicios, además de colocar en riesgos sus activos de información, teniendo en cuenta que la Estrategia Gobierno en Línea busca construir un Estado más eficiente, más transparente y más participativo gracias a las TIC. (Mintic, 2017).

Con esta estrategia el estado Colombia busca:

- Prestar mejores servicios en línea al ciudadano
- Logra excelencia en la gestión
- Empoderar y generar confianza en el ciudadano
- Impulsar y facilitar las acciones requeridas para avanzar en los objetivos de desarrollo sostenible – ODS, Facilitando el goce efectivo de derechos a través del uso de las TIC.

De acuerdo al decreto 2573 de 2014 expedido por el Ministerio de las tecnologías de Comunicación es necesario que las entidades de administración pública como el Concejo Distrital de Cartagena adopten la estrategia Gobierno en Línea en sus componentes estableciendo en el artículo 10 del mismo Decreto, Plazo para el año 2017 a las entidades del nivel A que se establecen en el decreto:

Gobernaciones de categoría Especial y Primera; alcaldías de categoría y demás sujetos obligados la Administración Pública en el mismo nivel.

Plazo para TIC Servicios: 100% para el 2017

Plazo para seguridad y privacidad de la información: 80% para el 2017

Teniendo en cuenta que la ciudad de Cartagena de Indias pertenece a la Categoría A por ser municipio de categoría Especial (Periódico el Universal, 2011), la entidad Concejo Distrital de Cartagena estaría dentro de estos plazos establecidos y no lograría cumplir violando flagrantemente el decreto.

También es de gran importancia tener en cuenta que la entidad no cuenta con una política que reglamente la seguridad de la información y la protección de sus recursos tecnológicos tal como lo establece el Informe de Auditoria Modalidad Regular Vigencia 2015 de la Contraloría Distrital de Cartagena en el “Hallazgo Administrativo N° 11 “ No existe política que reglamente la seguridad de la información y la protección de recursos tecnológicos utilizados para su procesamiento; esta situación se daría por negligencia descuido de la administración; lo que podría generar una posible violación al cumplimiento de la confidencialidad, integridad, y disponibilidad de los datos y sistemas de información, haciéndola vulnerable a accesos no autorizados y destrucción deliberada accidental”.(Contraloría Distrital de Cartagena, 2015).

Siendo reiterativo ya que el Informe de Auditoria Modalidad Regular Vigencia 2014 de la Contraloría Distrital de Cartagena en el “Hallazgo Administrativo N° 2 establece “ En el Concejo Distrital de Cartagena de Indias, el área de sistemas no se encuentra debidamente establecida, por la inexistencia de un espacio físico y la falta de procedimientos y controles en la administración de los recursos tecnológicos hardware y software; constituyéndose en un alto riesgo para la seguridad de la información por posibles acceso no autorizados y destrucción accidental o deliberada, de los datos y equipos de la entidad” . ”. (Contraloría Distrital de Cartagena, 2014).

El Concejo Distrital de Cartagena expone en un alto grado su permanencia en el mercado al no contar con un sistema de gestión de seguridad de la información exponiendo sus sistemas y recursos tecnológicos a riesgos y amenazas existentes tales como virus, uso malintencionado, perdida de información, etc. Por ejemplo, el riesgo de no contar con una política de seguridad de la información clara y definida, lleva inevitablemente al acceso no autorizado a una red informática o a los equipos que en ella se encuentran y puede ocasionar en la gran mayoría de los casos graves problemas, el principal riesgo es el robo de información sensible y confidencial, el cual puede ocasionar hasta el cierre de una compañía solida financieramente (Gonzales Agudelo, 2014).

Es necesario que la entidad cuente con estrategias claras de seguridad de la información que le permita el cumplimiento de sus objetivos estratégicos.

A través del Diseño de los Ejes Temáticos de la Estrategia Gobierno en Línea Tic Servicios y Seguridad y Privacidad de la Información para el Concejo Distrital de Cartagena, la entidad mejorará los trámites y servicios en línea para responder a las necesidades más apremiantes de los ciudadanos de acuerdo a TIC Servicios y desarrollara un sistema de protección de la información de la empresa estableciendo políticas, procedimientos y controles en los objetivos del negocio, apoyando la toma de decisiones trascendentales a la alta gerencia que garantice la permanencia de la entidad y el cumplimiento de los requerimientos del ente de control y a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno en línea.

Actualmente el Concejo Distrital de Cartagena carece de servicios y tramites electrónicos para los ciudadanos, la página web www.concejodecartagena.gov.co de la entidad se encuentra temporalmente fuera de servicio con un mensaje "página en renovación" desde el mes de junio de 2017 tal como lo observamos en la imagen N°1, lo que imposibilita ofrecer trámites y servicios electrónicos en forma oportuna a los ciudadanos y usuarios de los servicios de la entidad.

Imagen N° 1. Imagen Pagina Web Concejo Distrital de Cartagena

Fuente. Imagen tomada el día 18 de febrero de 2018 de www.concejodecartagena.gov.co

Al no contar con la posibilidad de realizar los trámites servicios en forma electrónica los ciudadanos deben desplazarse en forma física a la entidad lo que genera malestar, incomodidad y da una baja percepción de eficiencia a la ciudadanía.

En cuanto a la seguridad de la información y protección de los activos de información, la entidad no cuenta con políticas de seguridad en los sistemas de información, no existen protocolos de seguridad tanto físicos como a la documentación, actualmente el 0% de la documentación está protegida de ahí la importancia del Diseño de los ejes temáticos de la Estrategia Gobierno en Línea TIC servicios Seguridad y privacidad de la información.

2.2. Pregunta de Investigación

2.2.1. Pregunta General de Investigación

- Cuáles son los elementos del diseño de los ejes temáticos de la estrategia Gobierno en línea tic servicios y seguridad y privacidad de la Información en el Concejo Distrital de Cartagena.

2.2.2. Preguntas Específicas

- ¿Cuál es la situación actual del Concejo Distrital de Cartagena frente a los Ejes Temáticos de la Estrategia Gobierno en línea tic servicios y seguridad y privacidad de la Información, que permita conocer la calidad de los servicios que actualmente presta la entidad y como se realiza la protección de los activos de información, en aras de salvaguardar la continuidad de la entidad?

- ¿Qué elementos del eje temático tic servicios permitirán al Concejo Distrital de Cartagena proveer servicios ciudadanos adecuados a la población Cartagenera, con el fin de mejorar la calidad de servicios a los ciudadanos, garantizando mejoras en los tiempos de respuesta, satisfacción y calidad de los servicios, y tramites atendidos oportunamente?

- ¿Cómo se aplica el Modelo de Seguridad y privacidad de la información de la estrategia GEL para que garantice la protección de los recursos tecnológicos en el Concejo Distrital de Cartagena, permitiendo la salvaguarda de la información y continuidad de la entidad?

- ¿Qué elementos del eje temático tic seguridad y privacidad de la información permitirán al Concejo Distrital de Cartagena la seguridad y protección de sus recursos tecnológicos, mejorando la disponibilidad, confidencialidad e integralidad de la información?

- ¿Qué elementos del Modelo de Seguridad y privacidad de la información de la estrategia GEL permitirán realizar el eje temático tic seguridad y privacidad de la información del Concejo Distrital de Cartagena, garantizando la protección y salvaguarda de los activos de información de la empresa con el fin de mantener la confidencialidad, Integridad, disponibilidad y control de la información que producen los procesos de atención al usuario, financiera y administrativa?

- ¿Cómo se realiza una clasificación adecuada de los activos de información de los Procesos de Atención al Usuario, Administrativa y Financiera del Concejo Distrital de Cartagena que permita determinar los riesgos en la seguridad de la información y definir los planes de tratamiento de los riesgos, con el fin de evitar la pérdida de información importante para el funcionamiento de la entidad garantizando la integridad, confidencialidad y disponibilidad de la información?

- ¿Cuál es la Política de Seguridad de la Información adecuada que permita disminuir los riesgos de la entidad de acuerdo al Modelo de Seguridad y privacidad de la información de la estrategia GEL, que logré el diseño de procedimientos adecuados para el manejo de la información, contando con información inmediata y de calidad?

- ¿Con el diseño de políticas de seguridad de la información se podrá dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno en línea, protegiendo la información y los sistemas de información de acceso, uso, divulgación, interrupción o destrucción no autorizada?

2.3. Objetivos De La Investigación

2.3.1. Objetivo General

Diseñar los Ejes Temáticos de la Estrategia Gobierno en línea tic servicios y seguridad y privacidad de la Información para El Concejo Distrital de Cartagena de Indias, que mejore en un 90% la prestación de servicios de la entidad, salvaguardando los datos de los ciudadanos.

2.3.2. Objetivos Específicos

- Realizar el diagnóstico de la situación actual del Concejo Distrital de Cartagena con respecto a los Ejes Temáticos de la Estrategia Gobierno en línea tic servicios y seguridad y privacidad de la Información que permita conocer la calidad de los servicios que actualmente presta la entidad y como se realiza la protección de los activos de información, en aras de salvaguardar la continuidad de la entidad.

- Determinar las estrategias para el diseño con el propósito de cumplir con los ejes temáticos Tic Servicios y Seguridad y privacidad de la información establecido por la Estrategia GEL.

- Identificar las características de los diferentes grupos objetivos del Concejo Distrital de Cartagena con él fin de aumentar el conocimiento sobre nuestros usuarios y diseñar estrategias para mejorar la comunicación e incrementar la satisfacción de los mismos.

- Diseñar directrices de accesibilidad y usabilidad para ser implementado en los trámites y servicios electrónicos que permita a los usuarios tener una experiencia agradable al acceder a los servicios electrónicos de la entidad

- Diseñar estrategias de promoción de los trámites y servicios disponibles por medios electrónicos.

- Establecer criterios para la evaluación de la satisfacción del usuario de los servicios y tramites electrónicos, con el fin de contar con una guía que marque la ruta a seguir.

- Definir las pautas para la elaboración de protocolos de atención en el canal digital y electrónico donde se le preste servicio a los ciudadanos con calidad y oportunidad.

- Verificar el nivel de cumplimiento de la entidad frente a los requisitos del Modelo de Seguridad y Privacidad de la información de la estrategia Gel definiendo las acciones a seguir para su cumplimiento dentro de la entidad.

- Realizar la asignación de los roles y responsabilidades en la estructura organizacional en cuanto a seguridad y privacidad de la información.

- Definir las políticas de la Seguridad de la Información de la entidad tomando como base Modelo de Seguridad y Privacidad de la información de la estrategia Gel, que defina las acciones a seguir para el manejo de la información y de los sistemas de información.

- Definir el alcance y los objetivos del Modelo de Seguridad y Privacidad de la información de la estrategia Gel para el Concejo Distrital de Cartagena.

- Realizar la clasificación de los activos de información de los procesos de Atención al Usuario, Administrativa y Financiera que permita determinar los riesgos en la seguridad de la información y definir los planes de tratamiento de los riesgos, con el fin de evitar la pérdida de información importante para el funcionamiento de la entidad garantizando la integridad, confidencialidad y disponibilidad de la información.

- Valorar los riesgos de seguridad que permita definir planes de tratamiento de riesgos de acuerdo a la metodología señalada, buscando la protección de la información y los sistemas de información del acceso, uso, divulgación, interrupción o destrucción no autorizada

2.4. Alcances y Limitaciones Del Proyecto

2.4.1. Alcance

Diseño de los Ejes Temáticos de la Estrategia Gobierno en Línea Tic Servicios y Seguridad y Privacidad de la Información para el Concejo Distrital de Cartagena de acuerdo a la Estrategia Gobierno en Línea, se observará la situación actual de la entidad frente a la estrategia GEL, se hará un análisis de los servicios que se presta a la ciudadanía, caracterizando a la población objetivo para establecer acciones que atiendan sus necesidades de servicios tecnológicos, se definirán las pautas para elaborar protocolos de atención en los diferentes canales por los cuales se preste servicios la ciudadanía (Mintic, 2017)

A través del modelo de seguridad y privacidad de la información se revisará lo concerniente a los activos de información, seguridad física y ambiental, controles de acceso y riesgos en los activos de información cumpliendo los principios de confidencialidad, integridad, y disponibilidad.

El alcance de este proyecto incluye la caracterización de los usuarios del Concejo Distrital de Cartagena con el fin de conocer de una manera detallada las necesidades y

características de los usuarios, ciudadanos y grupos de interés de forma tal que las actividades de diseño, rediseño, comunicación y mejoramiento de trámites y servicios respondan a éstas y la elaboración de un manual que contenga las políticas de seguridad a seguir por los colaboradores del concejo, determinar un modelo de Gobierno de Tecnología Informática que mantenga los servicios críticos en funcionamiento con el fin de dar soporte a los procesos misionales y de apoyo, crear unos métodos para la identificación, análisis, valoración y manejo de los riesgos y así implantar unas estrategias para el manejo de estos. Con esta investigación plantearemos todos los controles que sean imperiosos para aminorar los riesgos identificados.

Los aspectos precisos que comprende la investigación del modelo de seguridad y privacidad de la información están referidos a la protección de los activos de información del proceso de Financiera el cual contiene los sistemas de información Zeus y Safe, y los procesos de Administrativa y de Atención al Usuario definiendo políticas y procedimientos que permitan dar un respaldo adecuado a la seguridad de la información.

2.4.2. Limitaciones

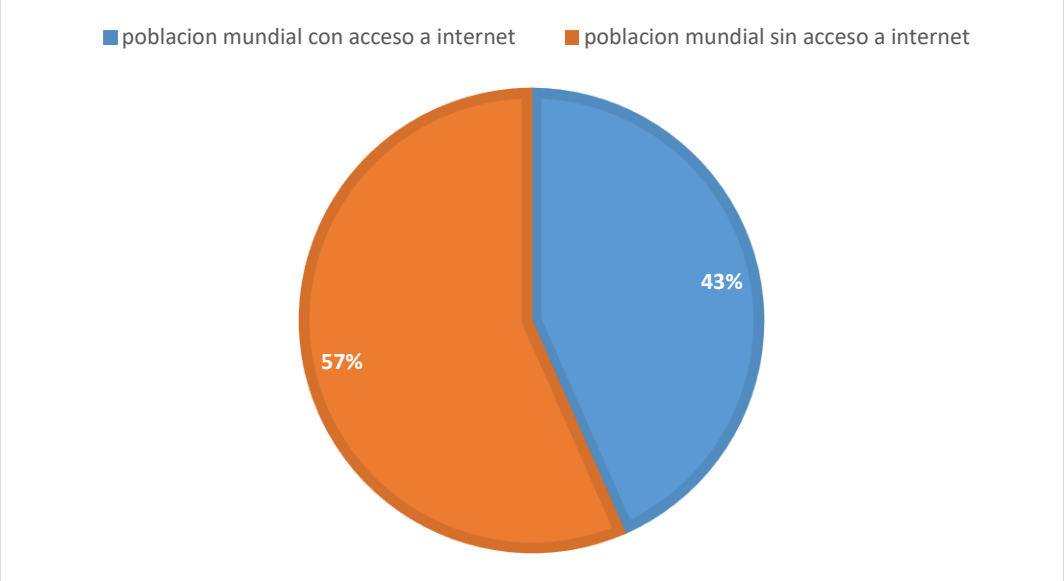
El proyecto solo abarca Diseño de los Ejes Temáticos de la Estrategia Gobierno en Línea Tic Servicios y Seguridad y Privacidad de la Información para el Concejo Distrital de Cartagena de acuerdo a la Estrategia Gobierno en Línea, no contemplan fases de implementación, revisión y mejora del mismo.

Sesgos por parte de los funcionarios: las respuestas que se obtendrán en las encuestas dependerán del grado de conocimiento en TIC Servicios y Seguridad de la información, teniendo en cuenta que existe muy poco conocimiento del tema por ser un tema técnico esto limitara la capacidad de respuesta de los funcionarios.

2.5. Justificación

De acuerdo al informe de **International Telecommunication Unión Place des Nations,** (2015). En el que se indica que 3.200 millones de personas están a partir de ahora en línea, lo cual representa el 43,4% de la población mundial, en tanto que el número de suscripciones al servicio móvil celular asciende a casi 7.100 millones en todo el mundo, y más del 95% de la población mundial puede recibir una señal móvil celular, informe que muestra el gran crecimiento de tecnologías de comunicaciones e información en el mundo actual.

Imagen N° 2. Población mundial con o sin acceso a internet



Fuente. Los autores en base al informe International Telecommunication Unión Place des Nations, (2015)

Este crecimiento de las tecnologías de información y de las comunicaciones muestra una situación positiva porque impacta en alto grado el desarrollo de las empresas y las formas de comunicación, de ahí la necesidad que tienen las instituciones del estado de aprovechar estas tecnologías para el mejoramiento de su gestión administrativa logrando una modernización adecuada del estado a través de la implementación de las Tecnologías de la información.

Las TIC son una plataforma formidable para estimular innovación acelerada, en lograr inmensas y rápidas ganancias de eficiencia en la prestación de servicios críticos y en la gestión pública en Colombia. (Castro, Devis y Olivera, 2011).

Es así como en el objetivo número ocho de los objetivos del milenio “Fomentar la alianza mundial para el desarrollo se reconoce a las tecnologías de la información y las comunicaciones (TIC) como parte esencial del desarrollo de los países debido a que esta contribuye al cierre de brechas sociales por medio de la democratización de la información y el conocimiento. Las TIC de acuerdo a los objetivos de desarrollo del milenio permiten que la comunicación se realice en todos los lugares del mundo entre la población geográficamente marginada y los epicentros. (Pnud, 2015)

Pero, así como impacta en forma positiva el desarrollo de las organizaciones también es vital observar las amenazas y vulnerabilidades a las que se exponen las empresas en un mundo interconectado.

Las vulnerabilidades son una debilidad en la tecnología o en los procesos relacionados con la información y son propios de los sistemas de información y las características que contiene. Las amenazas son cualquiera situación o evento que pueda afectar la posibilidad de las organizaciones o las personas para desarrollar sus actividades afectado la información o los sistemas que procesa tales como virus informáticos o códigos malicioso, fallas en los sistemas de procesamiento de la información, desastres naturales y actos malintencionados. (Tarazona, 2007).

Si el **Concejo Distrital de Cartagena no cuenta con medidas de protección** contra estas amenazas y vulnerabilidades a las que se expone puede desaparecer pues afectaría 100% el desarrollo de sus objetivos organizacionales al dejar sin protección un activo tan valioso como es la información, de ahí la necesidad que se diseñen estos mecanismos de protección que permitan contar con procesos adecuados y personal con conocimiento en el manejo de seguridad de la información que aseguren la confiabilidad, integridad y disponibilidad de está, permitiendo a la entidad ser más competitiva en el tiempo.

Ante este contexto de las TIC surge la necesidad para las entidades públicas de diseñar una Estrategia que permita la construcción de un estado Eficiente, más transparente, más seguro, más participativo y que preste mejores servicios a los

ciudadanos y a las empresas, mediante el aprovechamiento de las Tecnologías de la Información y las Comunicaciones. Mintic (2010). Esta estrategia conocida como Gobierno en Línea presenta cuatro ejes temáticos así (Mintic, 2017):

- TIC para el Gobierno Abierto: Busca construir un Estado más transparente y colaborativo, donde los ciudadanos participan activamente en la toma de decisiones gracias a las TIC.
- TIC para servicios: Busca crear los mejores trámites y servicios en línea para responder a las necesidades más apremiantes de los ciudadanos.
- TIC para la gestión: Busca darle un uso estratégico a la tecnología para hacer más eficaz la gestión administrativa.
- Seguridad y privacidad de la información: Busca guardar los datos de los ciudadanos como un tesoro, garantizando la seguridad de la información.

Con el fin de avanzar en los Objetivos de Desarrollo Sostenible. Al término del 2015, las entidades del Estado del orden nacional y territorial como el Concejo Distrital de Cartagena debe presentar avances frente a la estrategia de Gobierno en Línea, dividida en cuatro subcategorías: TIC para el gobierno abierto, TIC para servicios, TIC para la gestión y seguridad de la información. (Periódico el Tiempo, 2015).

Teniendo en cuenta que el decreto 2573 de 2014 expedido por el Ministerio de las Tecnologías de Comunicación establece en su artículo 10, el año 2017 para el logro de la implementación a las entidades del nivel A como el Concejo Distrital de Cartagena plazos así:

- Plazo para tic servicios: 100% para el 2017
- Plazo para seguridad y privacidad de la información: 80% para el 2017

Es necesario que la entidad diseñe los Ejes Temáticos de la Estrategia Gobierno en línea tic servicios y seguridad y privacidad de la Información cumpliendo los plazos establecidos por el Gobierno Colombiano.

El Diseño de los Ejes Temáticos de la Estrategia Gobierno en línea tic servicios y seguridad y privacidad de la Información permitirá al Concejo Distrital de Cartagena ofrecer a los Cartageneros una estrategia tecnológica que le permita la provisión de trámites y servicios a través de los canales electrónicos, enfocados a dar solución a las

principales necesidades y demandas de los usuarios y empresas en condiciones de calidad, facilidad de uso y mejoramiento continuo. (Mintic, 2017).

A través del **Diseño de los Ejes Temáticos de la Estrategia Gobierno en línea tic servicios y seguridad y privacidad de la Información del Concejo Distrital de Cartagena** identificará las características, necesidades, intereses, expectativas y preferencias de la población Cartagenera a la cual está dirigida, permitiendo ajustar la oferta institucional y presentar ofertas de servicios focalizadas para responder satisfactoriamente el mayor número de requerimientos, así como obtener retroalimentación y lograr la participación activa de la ciudadanía para el logro de los objetivos de las entidades y la satisfacción de derechos ciudadanos. (Mintic, 2011).

A través del **Diseño de los Ejes Temáticos de la Estrategia Gobierno en línea tic servicios y seguridad y privacidad de la Información el Concejo Distrital de Cartagena** garantizará que los ciudadanos cuenten con un canal de atención y comunicación con la entidad a través del sitio web, que permita realizar el seguimiento de PQRD y desarrollar acciones de mejoramiento continuo a partir de la evaluación de la satisfacción del usuario (Mintic, 2017).

A través **del Diseño de los Ejes Temáticos de la Estrategia Gobierno en línea tic servicios y seguridad y privacidad de la Información el Concejo Distrital de Cartagena** facilitará a los ciudadanos y grupos de interés la disposición y diligenciamiento y/o envío de formularos requeridos para la realización de trámites y servicios (Mintic, 2017). De esta forma la ciudadanía cartagenera interesada en realizar trámites con el Concejo Distrital de Cartagena podrá acceder a la entidad sin necesidad de desplazarse ni realizar tediosos procesos mejorando así la relación entidad-ciudadano.

Por medio del **Diseño de los Ejes Temáticos de la Estrategia Gobierno en línea tic servicios y seguridad y privacidad de la Información para el Concejo Distrital de Cartagena de Indias** podrá establecer políticas y procedimientos en relación a los objetivos del negocio de la entidad, disminuyendo el nivel de exposición de riesgo que la organización ha decidido asumir (ISO, 2013).

A través **del Diseño de los Ejes Temáticos de la Estrategia Gobierno en línea tic servicios y seguridad y privacidad de la Información para el Concejo Distrital de Cartagena de indias** la entidad definirá los roles y responsabilidades de Seguridad y Privacidad de la información dentro de la Entidad lo que permitirá trabajar con eficiencia y eficacia para el cumplimiento de los objetivos organizacionales brindando los mecanismos adecuados de protección de la información garantizando así la permanencia en el tiempo. (Mintic, 2016). Además, con este la Administrativa y la Financiera del Concejo Distrital de Cartagena a través de los contratistas del área de sistemas podrán emplear técnicas precisas de seguridad de la información, sensibilizaran y concientizaran a los funcionarios de todas las dependencias acerca de las amenazas a las que se enfrentan con el uso de las tecnologías y sistemas de información.

Con la Planeación y del Diseño de los Ejes Temáticos de la Estrategia Gobierno en línea Tic Servicios y Seguridad y Privacidad de la Información se definirán los lineamientos para las demás etapas precisando el alcance, las políticas y los objetivos generales, lo que permitirá a la administrativa y a la presidencia del Concejo Distrital de Cartagena cumplir con los requerimientos establecidos por los entes de control en este caso la Contraloría Distrital de Cartagena y la normatividad vigente, es por esto perentorio Diseñar los Ejes Temáticos de la Estrategia Gobierno en línea Tic Servicios y Seguridad y Privacidad de la Información para el Concejo Distrital de Cartagena con el fin de que la entidad proteja su información brindando confianza a los diferentes usuarios tanto internos como externos ofreciendo un mejor servicio, una mejor cobertura de la información, logrando mayor competitividad con la protección adecuada de los datos del negocio, sus clientes, empleados proyectando una imagen adecuada y además el cumplimiento de los requerimientos de los entes de control.

Con la realización de este proyecto se busca diseñar los Ejes Temáticos de la Estrategia Gobierno en línea Tic Servicios y Seguridad y Privacidad de la Información para el Concejo Distrital de Cartagena, este permitirá establecer un gobierno en línea que direccione en forma adecuada los objetivos misionales y estratégicos de la entidad, además de generar amplios beneficios tales como:

- Cumplir la Misión organizacional y alcanzar la visión.
- Brindar a la ciudadanía trámites y servicios a través de medios electrónicos.
- Ofrecer servicios y trámites centrados en el usuario.
- Accesibilidad hacia los diferentes tramites que ofrece la entidad.
- Brindar protección a la información y asegurarla en forma adecuada logrando una clara gestión de los procesos de toda la entidad.
- Imagen positiva de la entidad, con compromiso y responsabilidad
- Disminución de riesgos por pérdida de información.
- Cumplimiento de los requerimientos de los entes de control.
- Debida protección de los datos e información.

Estos beneficios impactan en un 100% los procesos estratégicos, misionales, técnicos y operativos de la entidad logrando que se generen las condiciones para establecer un Gobierno en línea, transparente y de seguridad de la información que genere un manejo eficiente y seguro de los datos por parte de los usuarios de los Sistemas de Información del Concejo Distrital de Cartagena, de ahí la importancia de conocer cuáles son los elementos que permitirán realizar el Diseño de los ejes temáticos tic servicios y Seguridad y privacidad de la Información para la entidad que sirvan como herramientas de fortalecimiento para Concejo Distrital de Cartagena de Indias.

3. METODOLOGÍA

3.1. Diseño General

3.1.1. Enfoque

El Diseño de los Ejes Temáticos de la Estrategia Gobierno en Línea Tic Servicios y Seguridad y Privacidad de la Información para el Concejo Distrital de Cartagena de acuerdo a la Estrategia Gobierno en Línea, es una investigación donde se observará la realidad de la organización en su forma natural para después analizarlos

sin manipulación de la realidad por esto se considera una investigación con un enfoque no experimental. La investigación no experimental es observar fenómenos tal y como se dan en su contexto natural, para después analizarlos. Como señala Kerlinger (1979).

3.1.2. Tipo de Investigación

La investigación es de tipo cualitativo dado que se pretende estudiar la realidad en su contexto natural, tal como sucede, intentando sacar sentido de, o interpretar, los fenómenos de acuerdo con los significados que tienen para las personas implicadas. (Rodríguez Gómez, Gil Flores y García Jiménez, 1996).

3.1.3. Tipo de Estudio

Al ser el Diseño de los Ejes Temáticos de la Estrategia Gobierno en Línea Tic Servicios y Seguridad y Privacidad de la Información para el Concejo Distrital de Cartagena de acuerdo a la Estrategia Gobierno en Línea un procedimiento investigativo donde se identificaran hechos, situaciones y se efectuará un diagnóstico y un Diseño, el tipo de estudio que se realizara será un estudio Descriptivo, de acuerdo a Danhke, (1989) (Citado por Hernández, Fernández y Baptista, 2003) los estudios descriptivos “miden, evalúan, o recolectan datos sobre diversos aspectos, dimensiones o componentes del fenómeno a Investigar (Hernández, Fernández y Baptista, 2003).

El estudio es de nivel aplicativo de corte transversal porque tiene como objetivo la generación de conocimiento con aplicación directa y mediano plazo en la sociedad o en el sector productivo (Lozada, 2014). Esto con el fin de recolectar toda la información que obtengamos para poder llegar al resultado de la investigación.

3.1.4. Universo y Muestra

3.1.4.1. Población

La investigación será realizada en el Concejo Distrital de Cartagena la cual es una corporación política – administrativa cuenta con 19 concejales y 50 empleados de planta. El Concejo Distrital de Cartagena de Indias es una corporación pública de elección popular. Es el foro natural para discutir temas inherentes al Distrito. Está integrado por 19 concejales, para un período de cuatro años. (Funcicar, 2017)

La entidad se encuentra ubicada en Cartagena de Indias, Getsemaní, Cl 24 10-08 Edif. Galeras de la Marina Colombia, Cartagena - Bolívar.

Las dependencias básicas del objetivo de investigación la conforman los empleados y Concejales de la empresa Concejo Distrital de Cartagena así:

- Mesa Directiva y Concejales: 19
- Secretaria General: 4
- Oficina de Comunicaciones y Protocolo: 4
- Técnica Comunal 7
- Financiera: 7
- Administrativa: 19
- Oficina Asesora Jurídica: 5
- Oficina Asesora de Control Interno :4
- Contratista sistemas y: 1
- Unidades de apoyo a concejales (Contratistas por prestación de servicios): 58

También se tomó información de los usuarios que visitaron la entidad en la fecha 18 de agosto de 2017.

3.1.4.2. Muestra

Teniendo en cuenta que para realizar el estudio se tomaran las áreas que desarrollan los procesos de Atención al Cliente(misional) y Financiera (apoyo) y Administrativa (Apoyo) las cuales son áreas críticas para el manejo de información de la entidad, además de tener un rol ejecutor en la toma de decisiones.

El número de funcionarios en el área de financiera es: 7 funcionarios de planta.

El número de funcionarios en el área de administrativa que intervienen en el proceso de atención es: 9 funcionarios de planta y 1 de sistemas (contratista).

Para un total de 16 funcionarios de planta y 1 contratista.

Y ciudadanos que asistieron a la entidad el día 18 de agosto de 2018.

Para el diagnostico se desarrollarán encuestas de preguntas cerradas y abiertas.

3.1.5. Hipótesis

3.1.5.1. Hipótesis General

Teniendo en cuenta el marco de referencia en los temas de Gobierno en Línea, se garantizará al Concejo Distrital de Cartagena la mejora de su gestión frente a la ciudadanía de la ciudad de Cartagena.

3.1.5.2. Hipótesis Específica

Establecer el alcance del Diseño de los Ejes Temáticos de la Estrategia Gobierno en Línea Tic Servicios y Seguridad y Privacidad de la Información de acuerdo a la Estrategia Gobierno en Línea permitirá brindar a los ciudadanos contar con una oferta de trámites, servicios y espacios de comunicación a través de canales electrónicos usables y accesibles que responden a sus necesidades y expectativas.

Establecer el alcance de los Ejes Temáticos de la Estrategia Gobierno en Línea Tic Servicios y Seguridad y Privacidad de la Información de acuerdo a la Estrategia Gobierno en Línea permitirá al Concejo Distrital de Cartagena aplicar los controles y mecanismos de protección al proceso de financiera, atención al ciudadano y los procesos de administrativa de la entidad, para proteger la información.

La Declaración de la política de seguridad de la información de la entidad lograra dispositivos adecuados de seguridad para que los procedimientos se desarrollen de una manera segura.

El desarrollo del plan de tratamiento de riesgos permitirá identificar las amenazas y vulnerabilidades que pueden afectar la integridad, disponibilidad y confiabilidad de la información y tomar las medidas adecuadas para su mitigación.

3.2. Métodos Específicos.

Métodos e instrumentos que utilizará para la recolección de la información

3.2.1. Fuente de información

Para el desarrollo de la tesis se tendrán en cuenta las siguientes fuentes de información:

- **Información Primaria**: Está compuesta por la información que será recolectada por medio de encuestas, entrevistas, observación directa a los funcionarios y usuarios externos. La Información primaria Es aquella que el investigador recoge directamente a través de un contacto inmediato con su objeto de análisis. (Gallardo y Moreno, 1999) y
- **Información Secundaria**: Se utilizará información proveniente de los lineamientos del Ministerio de las Tecnologías de la Información para la Estrategia Gobierno en Línea, el Manual de Gobierno en Línea Tic Servicios y Seguridad y privacidad de la Información (Mintic, 2017), las Metodologías de Análisis y valoración del Riesgo. La información secundaria es aquella que el investigador recoge a partir de investigaciones ya hechas por otros investigadores con propósitos diferentes. La información secundaria existe antes de que el investigador plantee su hipótesis, y por lo general, nunca se entra en contacto directo con el objeto de estudio. (Gallardo y Moreno, 1999).

3.2.2. Instrumento para recolectar la información

Un instrumento de medición adecuado es aquel que registra datos observables que representan verdaderamente a los conceptos o variables que el investigador tiene en mente. (Gallardo y Moreno 1999, por lo tanto, para obtener información confiable es necesario que los instrumentos sean confiables y arrojen datos válidos para el desarrollo de esta investigación se utilizaran los siguientes instrumentos:

- **Encuestas:**

Con el fin de obtener la información se aplicarán encuestas a las personas que manejan los procesos de Atención al usuario, financiera y Administrativa, teniendo en cuenta los requisitos del Modelo de Seguridad y privacidad de la información establecido por la Estrategia Gobierno en Línea, además se realizaran encuestas a los diferentes grupos poblacionales interesados en los tramites que realiza la entidad de acuerdo a TIC Servicios.

- **Marcos de Referencia:**

Para realizar el procedimiento concerniente a la recolección de datos, se utilizará el método de diagnóstico exploratorio, por cuanto el interés es realizar un análisis y diagnóstico de la situación actual de los elementos tic servicios y tic seguridad y privacidad de la información del Concejo Distrital de Cartagena, para así diseñar los proyectos que se deben implementar para el mejoramiento de los procesos de la entidad.

Por esto se realiza en primer lugar un análisis teórico, conceptual y legal del tema de Gobierno en línea a nivel latinoamericano, nacional y local.

Se realiza una comparación con los marcos de referencia establecidos en gobierno electrónico.

Finalmente se diseña una encuesta para realizar el diagnóstico.

Para obtener la información se elabora la encuesta en base a los lineamientos de gobierno en línea Tic servicios y Seguridad y privacidad de la información.

El diseño de los instrumentos de recolección de la información se elaboró en la etapa de recolección y análisis de la información teniendo en cuenta los objetivos del trabajo y a los estándares de la estrategia gobierno en línea para Colombia, utilizando

metodologías cuantitativas y cualitativas con el fin de conocer la realidad institucional frente a la estrategia.

Como se puede detallar en el documento, para el desarrollo de los objetivos del proyecto se elaboraron varios instrumentos de recolección de información.

A partir de la Tabla N° 1 se puede observar las encuestas realizadas en la entidad y a la ciudadanía:

Tabla N° 1. Encuestas y análisis realizado

Encuestas	Análisis de contenido
TIC SERVICIOS Se realizaron: 7 encuestas a funcionarios de dirección Financiera 9 encuestas a funcionarios de dirección Administrativa 1 Contratista del área de sistemas 20 encuestas a ciudadanos visitantes de la entidad	Se realizó análisis de contenido a la normatividad concerniente a la Estrategia Gobierno en línea en el área de TIC servicios
SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Se ejecutaron: 7 encuestas a funcionarios de dirección Financiera 9 encuestas a funcionarios de dirección Administrativa 1 Contratista del área de sistemas	Se realizó análisis de contenido a la normatividad concerniente a la Estrategia Gobierno en línea en el área de Seguridad y privacidad de la información.

Fuente. Los autores

El instrumento de tic servicios (ficha técnica) se elaboró en base a la encuesta nacional a las entidades sobre tic servicios con 18 preguntas en un formato escala Likert para las preguntas cerradas, si, no, No sabe o no responde (ns/nr). Y una pregunta abierta acerca de los trámites a implementar.

En el instrumento tic seguridad y privacidad de la información se utilizó la encuesta diagnóstica de seguridad y privacidad de acuerdo a la ISO 27001, en función de los objetivos con el propósito de preguntar a los sujetos de estudio a través de un cuestionario realizado con preguntas cerradas. El cuestionario consta de (103) preguntas en un formato escala Likert, si, no, No sabe o no responde (ns/nr), con el fin de diagnosticar como se encuentra la seguridad de la información en el Concejo Distrital de Cartagena.

Las preguntas también enmarcan los concernientes a riesgos y amenazas a la confiabilidad, integralidad, disponibilidad de la información están basadas en los requerimientos de la entidad teniendo en cuenta los objetivos de control de la norma ISO 27001: 2013 la cual se basa el Modelo de Seguridad y privacidad de la información.

- **Entrevistas:**

Se realizará entrevistas a los directores del área financiera, de secretaria general, administrativa y al contratista del área de sistemas con el fin de tener información real acerca de la estructura de la seguridad de la información del Concejo Distrital de Cartagena y analizar así los resultados de las encuestas, con base a los requerimientos establecidos en el Modelo de Seguridad y privacidad de la información.

- **Observación**

Por medio de la observación se podrá detallar claramente el procedimiento y manejo de la seguridad de la información del Concejo Distrital de Cartagena de Indias y el manejo de los trámites que realiza la entidad.

- **Diagnóstico de la intervención**

Con el fin de ejecutar una adecuada intervención en el Concejo Distrital de Cartagena será necesario realizar un análisis acerca de los diferentes tramites que realiza la entidad y que población objetivo se le satisfará las necesidades, además de detallar claramente los dominios, objetivos de control Controles de Seguridad (ISO/IEC 27002:2013) en base al Anexo A del estándar ISO 27001:2013 tal como lo establece el Modelo de Seguridad y privacidad de la información de la estrategia GEL, este análisis mostrara claramente las falencias que presentan los procesos de Atención al Usuario, Financiera y Administrativa de la entidad observando el ambiente inicial frente a la seguridad de la información con el objetivo de verificar el nivel de cumplimiento frente al estándar ISO/IEC 27001:2013.

Se utilizará un documento de Excel que detalle los Dominios, Objetivos de Control y Controles de Seguridad del estándar ISO/IEC 27002:2013 generando gráficas y estadísticas para cada uno de los dominios de la norma, con este proceso se detallará

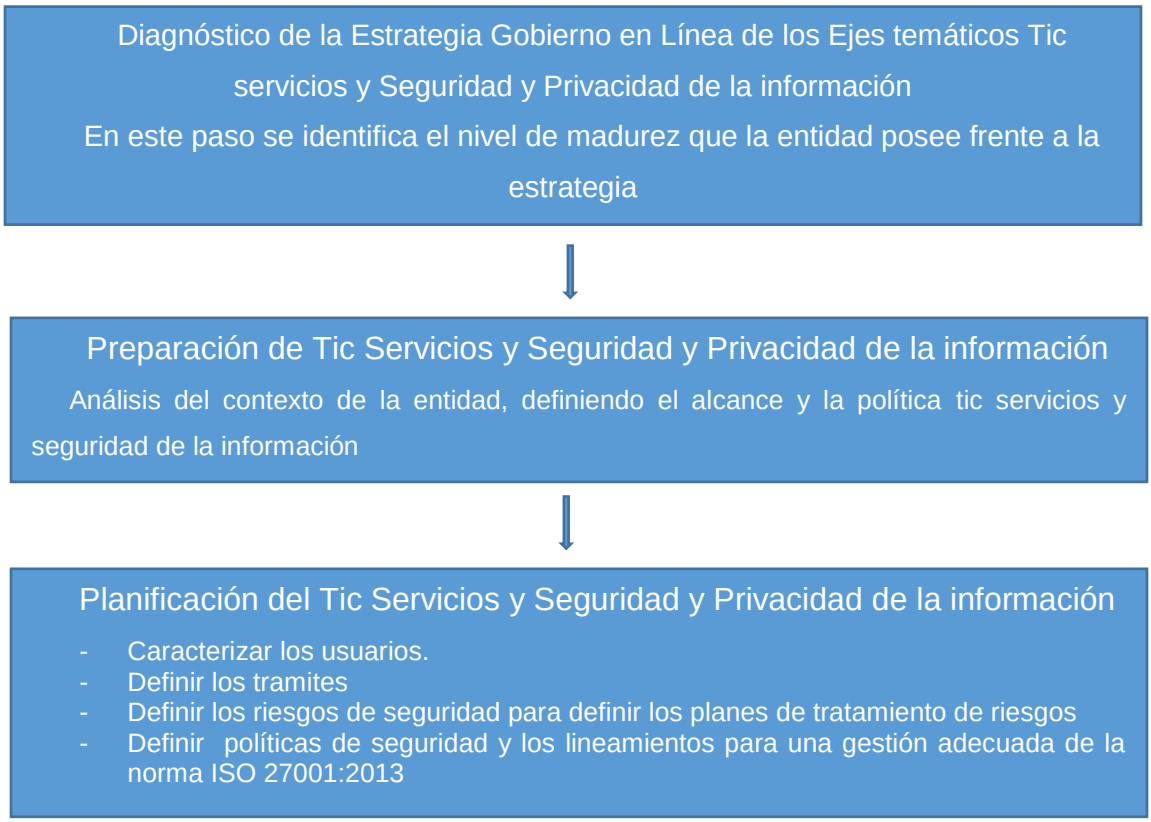
la ruta a seguir para lograr el cumplimiento de los numerales requeridos del estándar ISO/IEC 27001:2013.

Se utilizarán la guía de caracterización de usuarios establecida por la estrategia Gel, las matrices de medición de riesgos señaladas en la metodología de análisis y valoración del riesgo apropiada para el Diseño de los Ejes Temáticos de la Estrategia Gobierno en Línea Tic Servicios y Seguridad y Privacidad de la Información para el Concejo Distrital de Cartagena.

3.3. Metodología para el desarrollo del Proyecto

Observando Los requerimientos de la Estrategia Gobierno en Línea para Diseñar los Ejes Temáticos Tic Servicios y Seguridad y Privacidad de la Información para el Concejo Distrital de Cartagena, se definen las siguientes etapas para el desarrollo del Diseño:

Figura N° 1. Etapas para el Diseño de los Ejes Temáticos de la Estrategia Gobierno en Línea Tic Servicios y Seguridad y Privacidad de la Información



Fuente. Autores de acuerdo a la Estrategia GEL

3.3.1. Metodología Específica por Pregunta y Objetivo Específico

Tabla N° 2. Metodología Específica por Pregunta y Objetivo Específico.

METODOLOGÍA		
PREGUNTA DE INVESTIGACIÓN	**OBJETIVOS**	**METODOLOGÍA ESPECÍFICA**
¿Cuál es la situación actual del Concejo Distrital de Cartagena frente a los Ejes Temáticos de la Estrategia Gobierno en línea tic servicios y seguridad y privacidad de la Información, que permita conocer la calidad de los servicios que actualmente presta la entidad y como se realiza la protección de los activos de información, en aras de salvaguardar la continuidad de la entidad?	Realizar el diagnóstico de la situación actual del Concejo Distrital de Cartagena con respecto a los Ejes Temáticos de la Estrategia Gobierno en línea tic servicios y seguridad y privacidad de la Información que permita conocer la calidad de los servicios que actualmente presta la entidad y como se realiza la protección de los activos de información, en aras de salvaguardar la continuidad de la entidad.	Se realizará visita en campo en las instalaciones de la entidad, para recolectar la información, en especial a las áreas de atención al usuario, gestión financiera y gestión administrativa. Se elaborarán encuestas a los empleados y visitantes sobre Tecnologías de la información y de las comunicaciones de Servicios. Se aplicará la encuesta de seguridad y privacidad de la información solo a los empleados. Se realizará entrevista a los directores de área y jefes de proceso. Se realizará la tabulación de la encuesta y se analizaran los resultados.
Qué elementos del eje temático tic servicios permitirán al Concejo Distrital de Cartagena proveer servicios adecuados a la población Cartagenera, con el fin de mejorar la satisfacción y calidad de servicios, garantizando mejoras en los tiempos de respuesta, tramites atendidos oportunamente y transparencia	Determinar las estrategias para el diseño con el propósito de cumplir con los ejes temáticos Tic Servicios y Seguridad y privacidad de la información establecido por la Estrategia GEL.	Para diagnosticar la estrategia Tecnologías de la información y de las comunicaciones de Servicios se encuestarán a 17 empleados de la entidad pertenecientes a las áreas de financiera, secretaria general y administrativa, además de los ciudadanos concurran a la entidad el día 29 de agosto de 2017, se aplicarán 37 encuestas. Se revisarán diferentes fuentes de información de los trámites que se tienen en el Concejo Distrital de

METODOLOGÍA		
PREGUNTA DE INVESTIGACIÓN	**OBJETIVOS**	**METODOLOGÍA ESPECÍFICA**
		Cartagena, SUIT (Sistema Único de Información y Trámites del Gobierno Colombiano) y Página Web de la entidad. Se definirán los trámites y servicios en línea de acuerdo al diagnóstico de la encuesta y a la caracterización de usuarios.
	Identificar las características de los diferentes grupos objetivos del Concejo Distrital de Cartagena con él con el fin de aumentar el conocimiento sobre nuestros usuarios y diseñar estrategias para mejorar la comunicación e incrementar la satisfacción de los mismos.	Se realizará un análisis a los expedientes de los registros de PQRD almacenados en los que se consigna la información de los usuarios que han solicitado información a lo largo de los meses de enero a octubre de 2017. Se seleccionarán las siguientes variables de acuerdo a la guía de caracterización de usuarios de Ministerio de las Tecnologías de la información 2011 fueron: **-** Variable Geográfica - Variable Demográfica - Variables intrínsecas. A partir de las cuales se identificarán las motivaciones de los ciudadanos para acceder a los servicios, de esta manera la entidad podrá realizar una adecuada oferta de servicios focalizada en el usuario, lo que permitirá la participación de la ciudadanía repercutiendo en el logro de los objetivos de la entidad.

METODOLOGÍA		
PREGUNTA DE INVESTIGACIÓN	**OBJETIVOS**	**METODOLOGÍA ESPECÍFICA**
	Diseñar directrices de accesibilidad y usabilidad para ser implementado en los trámites y servicios electrónicos, que permita a los usuarios tener una experiencia agradable al acceder a los servicios electrónicos de la entidad.	Se revisará y analizarán los estándares en cuanto a accesibilidad y usabilidad tales como gobierno en línea los W3C e ISO 25000. De acuerdo a estos estándares se realizó el diseño de la página web mediante mockups señalando cuales serían las características de la página web para lograr una mejor experiencia en los servicios electrónicos ofrecidos por la entidad al ciudadano.
	Diseñar estrategias de promoción de los trámites y servicios disponibles por medios electrónicos, que permita mejorar la relación ciudadano- entidad a través de la prestación de calidad de los servicios.	Se realizará la caracterización de los usuarios, determinando las preferencias para acceder a los servicios de la entidad. Se diseñará un plan de comunicaciones destinado para promocionar los trámites y servicios de la entidad.
	Establecer criterios para la evaluación de la satisfacción del usuario de los servicios y tramites electrónicos, con el fin de contar con una guía que marque la ruta a seguir.	Se verificará si la entidad cuenta con la guía para evaluar la satisfacción del usuario. Teniendo en cuenta que se requiere alcanzar la satisfacción de los trámites y servicios digitales así se establecen los criterios de evaluación y con estos se elaboraran las preguntas para realizar la evaluación de la satisfacción del usuario,

METODOLOGÍA		
PREGUNTA DE INVESTIGACIÓN	**OBJETIVOS**	**METODOLOGÍA ESPECÍFICA**
		presentando una serie de pasos que permitan identificar los criterios. Se identificará la satisfacción de los servicios digitales prestados.
	Definir las pautas para la elaboración de protocolos de atención en el canal digital y electrónico donde se les preste servicio a los ciudadanos con calidad y oportunidad.	Con los resultados arrojados de la encuesta se establecerá si la entidad Concejo Distrital de Cartagena cuenta con protocolos de atención por cada tramite en línea, se puntualizará el proceso y el procedimiento de los servicios y tramites ofrecidos por la página web que permitan contar con servicios de calidad a la ciudadanía en el marco de un buen servicio.
¿Qué elementos del eje temático tic seguridad y privacidad de la información permitirán al Concejo Distrital de Cartagena la seguridad y protección de sus recursos tecnológicos, garantizando la protección y salvaguarda de los activos de información de la empresa con el fin de mantener la confidencialidad, Integridad, disponibilidad y control de la información que producen los procesos de atención al usuario, financiera y administrativa?	Definir el alcance y los objetivos del Modelo de Seguridad y Privacidad de la información de la estrategia Gel para el Concejo Distrital de Cartagena, que permita cumplir con el eje temático tic seguridad y privacidad de la información.	De acuerdo a la guía del modelo de seguridad y privacidad de la información de la Estrategia Gobierno en Línea, se precisará el alcance y los objetivos para el Concejo Distrital de Cartagena.
	Realizar la asignación de los roles y responsabilidades en la estructura organizacional en cuanto a seguridad y privacidad de la información.	Se evaluarán los puestos de trabajo, definiendo dentro de la estructura organizacional del Concejo Distrital de Cartagena, los roles y responsabilidades para la seguridad y privacidad de la información de las personas que intervienen en las distintas dependencias de la entidad.

METODOLOGÍA		
PREGUNTA DE INVESTIGACIÓN	**OBJETIVOS**	**METODOLOGÍA ESPECÍFICA**
¿Cómo se aplica el Modelo de Seguridad y privacidad de la información de la estrategia GEL para que garantice la protección de los recursos tecnológicos en el Concejo Distrital de Cartagena, permitiendo la salvaguarda de la información y continuidad de la entidad?	Verificar el nivel de cumplimiento de la entidad frente a los requisitos del Modelo de Seguridad y Privacidad de la información de la estrategia Gel definiendo las acciones a seguir para su cumplimiento dentro de la entidad	Se encuestarán a 17 personas (16 Funcionarios de planta y un (1) contratista del área de sistemas, en base al modelo de seguridad y privacidad de la información. Se tabulará y se verificará el nivel de cumplimiento en la entidad, se publicarán los resultados arrojados. Se diseñaran estrategias con el fin de lograr la aplicación del modelo de seguridad y privacidad de la información dentro del Concejo Distrital de Cartagena.
¿Cómo se realiza una clasificación adecuada de los activos de información de los Procesos de Atención al Usuario, Administrativa y Financiera del Concejo Distrital de Cartagena, que permita determinar los riesgos en la seguridad de la información y definir los planes de tratamiento de los riesgos, con el fin de evitar la pérdida de información importante para el funcionamiento de la entidad garantizando la integridad, confidencialidad y disponibilidad de la información?	Realizar la clasificación de los activos de información de los procesos de Atención al Usuario, Administrativa y Financiera que permita determinar los riesgos en la seguridad de la información y definir los planes de tratamiento de los riesgos, con el fin de evitar la pérdida de información importante para el funcionamiento de la entidad garantizando la integridad, confidencialidad y disponibilidad de la información.	Se llevará a cabo un inventario de los activos de información del Concejo Distrital de Cartagena de Indias en los procesos de atención al usuario, dirección administrativa y dirección financiera. Se perpetrará un levantamiento de inventario para la caracterización y valoración de los activos de información existentes en los procesos de atención al usuario, dirección administrativa y dirección financiera, se realizará de acuerdo al Libro II de la metodología MAGERIT versión 3, en donde nos presenta el catálogo de elementos:
	Valorar los riesgos de seguridad que permita definir planes de	Con la finalidad de proteger la confidencialidad, integridad y

METODOLOGÍA		
PREGUNTA DE INVESTIGACIÓN	**OBJETIVOS**	**METODOLOGÍA ESPECÍFICA**
	tratamiento de riesgos de acuerdo a la metodología señalada, buscando la protección de la información y los sistemas de información del acceso, uso, divulgación, interrupción o destrucción no autorizada.	disponibilidad y hacer el análisis y gestión de los riesgos de información se toma como método de análisis y gestión de riesgos informáticos la Metodología MAGERIT 37 versión 3.0, esta metodología de la mano con la norma ISO/IEC 27001 de 2013, la cual permite identificar amenazas y estimar impacto y probabilidad de forma cualitativa. Con la utilización de la metodología Margerit se definen estrategias que permitirán proteger la información y establecer un plan de mitigación de riesgo, donde se diseñarán los controles para el tratamiento.
¿Cuál es la Política de Seguridad de la Información adecuada que permita disminuir los riesgos de la entidad de acuerdo al Modelo de Seguridad y privacidad de la información de la estrategia GEL, que defina las acciones a implementar en la privacidad y seguridad de la información de la entidad?	Definir las políticas de la Seguridad de la Información de la entidad tomando como base Modelo de Seguridad y Privacidad de la información de la estrategia Gel, que defina las acciones a seguir para el manejo de la información y de los sistemas de información, protegiéndolos del acceso, uso divulgación y destrucción no autorizada-	Para la definición de las políticas de seguridad de la información se asentará en el modelo de seguridad y privacidad de la información aplicándolas al contexto del Concejo Distrital de Cartagena.
¿Con el diseño de políticas de seguridad de la información se podrá dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la		

METODOLOGÍA		
PREGUNTA DE INVESTIGACIÓN	**OBJETIVOS**	**METODOLOGÍA ESPECÍFICA**
información de la estrategia de gobierno en línea, protegiendo la información y los sistemas de información del acceso, uso, divulgación, interrupción o destrucción no autorizada?		

Fuente. Los autores de acuerdo a la metodología utilizada para el desarrollo del trabajo

3.3.2. Tratamiento de los datos

Con la información que se obtengan de los instrumentos de recolección tales como encuestas y entrevistas se procederá a realizar el análisis de las respuestas, en el análisis de las encuestas se realizara la tabulación con el fin de obtener la información precisa para la toma de decisiones.

La encuesta se elaborará para TIC servicios en base a:

- Guía para la caracterización de usuarios de las entidades públicas. (Mintic, 2011).
- Guía de atención al ciudadano cliente por múltiples canales. Mintic (2011)

Para Seguridad y privacidad de la información se realizará en base a los objetivos de control del Anexo a dela ISO 27001:2013 establecidos en el Modelo de Seguridad de la Información de GEL así:

- Políticas de seguridad de la información
- Organización de la seguridad de la información
- Seguridad de los recursos humanos
- Gestión de activos
- Control de acceso
- Criptografía
- Seguridad física y del entorno
- Seguridad de las operaciones
- Seguridad de las comunicaciones

- Adquisición, desarrollo y mantenimiento del sistema
- Relación con los proveedores
- Gestión de incidentes de la seguridad de la información
- Aspectos de seguridad de la información de la gestión de continuidad de negocio
- Cumplimiento
- Riesgos de los activos de información de los procesos de Atención al usuario, financiera y Administrativa.

Esto con el fin de evaluar las amenazas a la integridad, confiabilidad y disponibilidad de la información, una vez que se obtengan los datos provenientes de la encuesta dirigido a los procesos de atención al usuario, Financiera y Administrativa y se procederá su tabulación teniendo en cuenta el criterio escogido para la evaluación.

Se utilizará la estadística descriptiva que permite representaciones graficas de acuerdo a los ejes temáticos Tic Servicios y Seguridad y Privacidad de la información y el marco teórico de la investigación.

4. FUENTES DE INFORMACIÓN: ESBOZO MARCO TEÓRICO

Tabla N° 3. Esbozo del Marco Teórico

Temas	Modelo, Teoría y Concepto	Fuentes	Autor
Gobierno en línea	Gobierno en línea es el nombre que recibe la estrategia de gobierno electrónico (e-government) en Colombia, que busca construir un Estado más eficiente, más transparente y más participativo gracias a las TIC.	Mintic, (2016), Estrategia Gobierno en Línea Recuperado en http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.html	Mintic, 2016
Gobierno electrónico o gobierno en línea	Innovación continua de los servicios, la participación de los ciudadanos y una forma de gobernar mediante la transformación de las relaciones externas e internas a través de la tecnología, el Internet y los nuevos medios de comunicación.	Rodríguez Gladys (2004). Gobierno Electrónico: hacia la modernización y transparencia de la gestión pública recuperado en http://ciruelo.uninorte.edu.co/pdf/derecho/21/1_GOBIERNO%20ELECTRONICO_DERECHO_No%2021.pdf	Rodríguez Gladys(2004)
Modelo de Seguridad y Privacidad de la información	Comprende el proceso de construcción de una política de privacidad por parte de la entidad, que permita fijar los criterios que seguirán para proteger la privacidad de la información y los datos, así como de los procesos y las personas vinculadas con dicha información.	Recuperado en https://www.mintic.gov.co/gestionti/615/articles-International	(Mintic, 2015).
Seguridad de la Información	El SGSI basado en ISO/IEC 27001 permite la gestión y control de los riesgos de la seguridad de la información en las organizaciones para las cuales la información y la	(Icontec, 2013) Recuperado en http://www.icontec.org/Ser/EvCon/Paginas/PCS/ci27001.aspx	Icontec, 2013

Temas	Modelo, Teoría y Concepto	Fuentes	Autor
	tecnología son activos importantes de su negocio.		
Seguridad de la Información	La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma	Wikipedia(2017), https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n	Wikipedia(2017)
Sistema de Gestión de seguridad de la información	SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMOS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración	López Neira y Ruiz Spohr (2012) Recuperado http://www.iso27000.es/download/doc_sgsi_all.pdf	López Neira y Ruiz Spohr (2012)
Sistema de Gestión de seguridad de la información	Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión,	Icontec(2013), recuperado de https://tienda.icontec.org/wp-	Icontec, 2013.

Temas	Modelo, Teoría y Concepto	Fuentes	Autor
	mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos aspectos y sus sistemas de apoyo cambien con el tiempo. Se espera que la implementación de un SGSI se ajuste de acuerdo con las necesidades de la organización, por ejemplo, una situación simple requiere una solución de SGSI simple	content/uploads/pdfs/NTC-ISO-IEC27001.pdf	
Requisitos de la norma ISO-IEC 27001:2013.	La norma ISO/IEC 27001 especifica los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información (SGSI).	Icontec, (2013) recuperado de http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf	Icontec, 2013.
Documentos obligatorios para el estándar ISO/IEC 27001:2013	Son los documentos obligatorios que necesita elaborar la empresa si quiere cumplir con la norma ISO 27001: 2013.	KOSUTIC, D. (2013) “Lista de documentación obligatoria requerida por ISO/IEC 27001”. Disponible en ISO 27001 Academy: https://advisera.com/27001academy/es/knowledgeb	Kosutic, 2013

Temas	Modelo, Teoría y Concepto	Fuentes	Autor
		ase/lista-de-documentos-obligatorios-exigidos-por-la-norma-iso-27001-revision-2013/	
Gobierno de la Tecnología Informática	El gobierno de TI es el proceso por el cual las decisiones se toman alrededor de las tecnologías. Cómo se toman las decisiones, quién toma las decisiones, quién es responsable y cómo. Los resultados de las decisiones son medidos y monitoreados por parte del gobierno de TI.	SYMONS, C. "IT (2005), Governance Framework: Structures, Processes, And Communication". Disponible en Forrester Research: (http://i.bnet.com/whitepapers/051103656300.pdf)	Symons, 2005
COBIT	El COBIT es un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso	ISACA. (2007). COBIT 4.1. Rolling Meadows: ISACA. Disponible en: http://goo.gl/8xbivE	Isaac, 2007
Ley 1273 de 2009. Delitos informáticos	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.	Congreso de la república de Colombia, (2009), Recuperado en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492	Congreso de la república de Colombia, 2009
Ley 1581 de 2012	La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las INFORMACIÓN es que se hayan recogido sobre ellas en	Congreso de la república, (2012),Recuperado en http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html	Congreso de la república, 2012

Temas	Modelo, Teoría y Concepto	Fuentes	Autor
	bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.		
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.	Congreso de la república, (2013), Recuperado en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646	Congreso de la Republica, 2013
Metodología Octave	OCTAVE es una técnica de planificación y consultoría estratégica en seguridad basada en el riesgo.	CERT – Software Engineering Institute (2008). OCTAVE. Disponible en: http://www.cert.org/octave/	Duque Ochoa, 2010
Metodología Margerit	La metodología MAGERIT desarrolla el Proceso de Gestión de Riesgos de las tecnologías de la información dentro de la Norma ISO 31000, Sección 4.4 “Implementación de la Gestión de los Riesgos”	Gobierno de España, (2012) MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información recuperado de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WSNGX5KGOvE	Gobierno de España, 2012
DAFP-	El Departamento Administrativo de la Función Pública ha desarrollado la Guía de Administración del riesgo dirigida a las entidades estatales.	Dafp, 2011 Guía de Administración del riesgo recuperado en http://www.funcionpublica.gov.co/documents/41853	Dafp, 2011

Temas	Modelo, Teoría y Concepto	Fuentes	Autor
		7/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba	
ISO 31000	La norma UNE-ISO 31000 “Gestión del riesgo. Principios y directrices” es un estándar desarrollado en colaboración por ISO e IEC que provee principios y directrices genéricas sobre la gestión del riesgo. Se trata de una norma general, de aplicación a cualquier organización independientemente del tamaño o sector y que no es certificable.	https://www.isotools.org/2013/12/06/los-11-principios-de-la-iso-31000-la-gestion-de-riesgos/	ISO 31000:2009.
Riesgo	El riesgo es un elemento consustancial a la propia actividad de la empresa y, aún más, en sus diferentes manifestaciones está presente en cualquier tipo de actividad; en la mayor parte de los casos no es posible establecer mecanismos para su completa eliminación, por lo que se hace absolutamente imprescindible gestionarlo de forma adecuada.	http://www.unagaliciamoderna.com/eawp/coldata/upload/mapa_de_riesgos_19_06_13.pdf	Revista Atlántica de Economía – Volumen 2 – 2013
Mapa de Riesgos	Es sintetizar la información relativa a las indeterminaciones que afronta la empresa y colaborar en las estrategias destinadas a mitigar la exposición y los daños potenciales GARCÍA 1994.	http://www.unagaliciamoderna.com/eawp/coldata/upload/mapa_de_riesgos_19_06_13.pdf	Revista Atlántica de Economía – Volumen 2 – 2013.

Temas	Modelo, Teoría y Concepto	Fuentes	Autor
El Decreto 1151 de 2008	El manual para la implementación de la estrategia de gobierno en línea determina los lineamientos para cumplir con lo establecido en el Decreto 1151 del 14 de abril de 2008 e incorpora recomendaciones del documento de “Políticas y Estándares para publicar información del Estado colombiano en Internet” del año 2000, las cuales dejan de tener vigencia a partir de la publicación del Manual. (Mintic, 2008)	https://www.mintic.gov.co/portal/604/articles-3643_documento.pdf	(Mintic, 2008)

Fuente. Elaboración propia

5. MARCO TEÓRICO

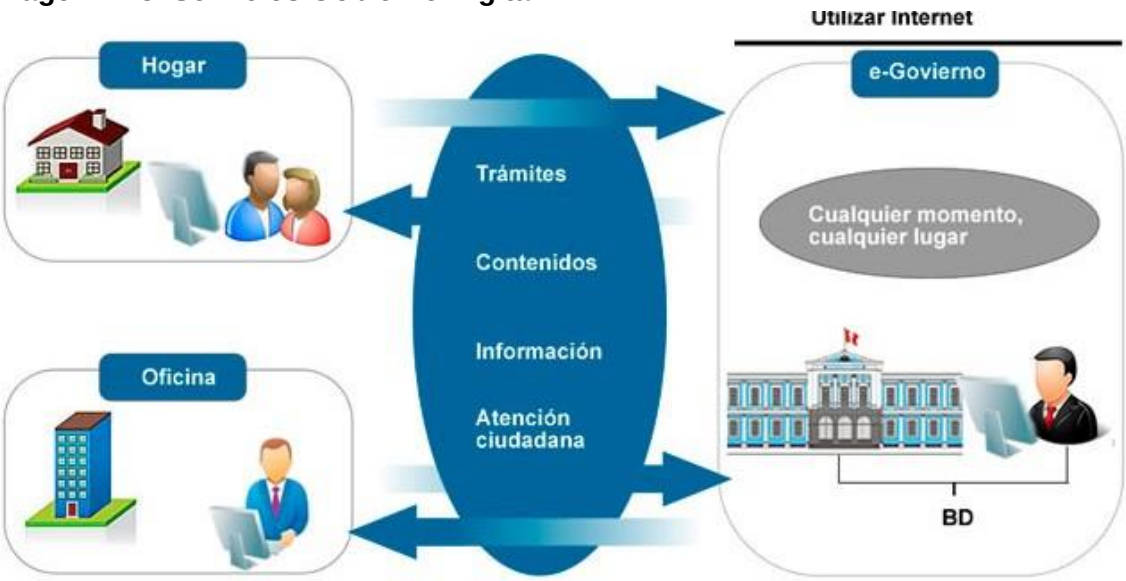
Con la evolución permanente de las tecnologías de la información y comunicaciones, la velocidad de los cambios y la dependencia de las empresas a estas (tecnologías de la información y comunicaciones), para el manejo de sus negocios es de vital importancia que las organizaciones tanto públicas como privadas cuenten con herramientas que le permitan una innovación continua de los servicios, la participación de los ciudadanos y una forma de gobernar mediante la transformación de las relaciones externas e internas a través de la tecnología, el Internet y los nuevos medios de comunicación. (Abraham, 2001), de igual forma que le garantice la seguridad de la información teniendo en cuenta que a diario se enfrentan con una amplia gama de amenazas y vulnerabilidades. (Tarazona, 2007).

Entendiendo que el Gobierno trabaja en pro del beneficio de la ciudadanía es necesario que este se transforme o modernice de acuerdo a las nuevas tendencias tales como son las TIC, para esto es de vital importancia diseñar estrategias, planes y políticas apropiados que permitan a la sociedad civil intervenir activamente en la ejecución del proceso citado, así como apuntar a constituir al ciudadano en una especie de «guardián eterno» de los eventuales logros reformistas (Ocampo, 2003).

Y como puede lograr esto el Gobierno, a través de la prestación de servicios adecuados con innovación, calidad, eficientes y transparente que mejore las relaciones con los ciudadanos a través de las tecnologías de la información y comunicación, transformando el gobierno en un Gobierno digital o electrónico.

Si los gobiernos y sus administraciones públicas logran prestar estos servicios a los ciudadanos podrán lograr una mayor accesibilidad logrando una unión del sector público y el privado para obtener así una integración de los servicios que se le brindan a la ciudadanía, con menores costos lo que facilitaría crear más y mejores servicios a la ciudadanía.

Imagen N° 3. Servicios Gobierno Digital



Fuente. Imagen de http://www.jcmagazine.com/gobierno-digital-tramites-mas-simples-y-en-menos-tiempo/.

Es así que el gobierno digital podrá entregar a la ciudadanía (A Naser, G Concha, 2011):

- Transparencia y rendición de cuentas. Publicación de rendición de cuentas donde se informan los gastos de las entidades y su manejo presupuestal.
- Servicios en Línea: Diversos trámites para los ciudadanos, disminuyendo cosos y tiempos debido a la disponibilidad inmediata.
- Participación Ciudadana: buzones de quejas y peticiones, consulta de temas de interés general para la ciudadanía.
- Capacitación y Educación a Distancia. Capacitación a través de medios electrónicos para la ciudadanía y funcionarios

5.1. ¿Qué Es Gobierno Electrónico?

Un Gobierno Electrónico es esta herramienta que se necesita para lograr esta modernización entendiendo este como un esquema de gestión pública basado en la utilización de la tecnología de la información y de las comunicaciones, teniendo como objetivos mediatos optimizar la gestión pública y desarrollar un enfoque de gobierno centrado en el ciudadano (Ocampo, 2003:2).

En definitiva, garantizar al usuario el poder deliberar y discutir sobre la gestión pública se puede apreciar que, en cualquier escenario, una de las virtudes más importantes del gobierno electrónico es la posibilidad de mantener canales de comunicación permanentemente abiertos entre el Estado y los ciudadanos. Rodríguez Gladys (2004).

5.1.1. Alcance de gobierno electrónico

Externo: El estado se relaciona con los ciudadanos, esto se denota en la prestación de los servicios por parte de todas las entidades del estado ya sea ministerios y de los organismos públicos descentralizados adscritos a éstos. Aquí el Internet es prioritario a través de los denominados «portales» o «web site». Incluso hay quienes manifiestan que la figura del portal está llamada a cumplir una función de «ventanilla única» en la administración pública, a través de la cual se puede desde brindar información al ciudadano hasta constituirse en una mesa de partes «virtual» para recibir documentos, quejas y / o sugerencias; e incluso para recibir el pago de un servicio determinado o derivado del cumplimiento de una obligación a cargo del ciudadano. Rodríguez Gladys (2004).

Interno: Este está dirigido a la entidad estatal buscando la eficiencia en la gestión administrativa interna vi vinculada con el funcionamiento de los sistemas administrativos.

5.1.2. Características gobierno electrónico

Las características principales de Gobierno Electrónico son (Rodríguez Gladys (2004): Uso de las tecnologías de información y comunicaciones.

- La prestación de servicios por parte del Estado en forma ágil y eficiente,
- La participación de los ciudadanos en el proceso de toma de decisiones (gestión pública), dentro de un marco de transparencia que favorezca el ejercicio de la democracia deliberativa y
- Soporte jurídico de apoyo

5.1.3. Principios de gobierno electrónico

Los principios de Gobierno electrónico de acuerdo a lo establecido por los investigadores son (Rodríguez G, 2004):

- **Transformador o renovación**: Nueva forma de actuar de la administración pública. En donde el estado brinda a todos los ciudadanos servicios en forma electrónica, considerando una dimensión geográfica (dónde se accede), una social (quién accede) y una horaria (cuándo se accede), y asegurando que dichas dimensiones sean equitativas.
- **Fácil de usar**: Busca que los servicios provistos mediante TIC por parte del Estado sean simples y sencillas, evitando confusiones y trámites complejos.
- **Conveniente**: Implica que el beneficio que signifique para los ciudadanos el demandar un servicio a través de las TIC, sea superior al que recibe de obtenerlo en forma presencial en las dependencias públicas.
- **Seguridad, privacidad y registro**: Significa disponer de los niveles adecuados de seguridad que garanticen a los ciudadanos la privacidad en el acceso a la información y de las transacciones realizadas por ellos.
- Participación del sector privado: Con la participación del sector privado se asegura que sea exitoso el proceso ya que facilitaría el suministro de tecnologías y capacitación de los funcionarios públicos, sino porque con su

intervención se pueden medir las preferencias de los ciudadanos y así satisfacer sus demandas.

- **Desconcentración**: La administración, mantenimiento y actualización de las TIC será responsabilidad de cada servicio, salvo en aquellos casos que involucra la participación de varios servicios.
- **Interoperabilidad del servicio electrónico**: El gobierno electrónico debe garantizar que todos los ciudadanos puedan tener acceso a los servicios ofrecidos en la red, así como asegurar la posibilidad de presentar sus quejas, denuncias y solicitudes.

Todos estos principios y características de gobierno digital buscan modernizar las relaciones de servicio entre los ciudadanos y las autoridades logrando importantes beneficios para la ciudadanía y la administración principalmente en sectores sensibles como (Arnaud Laurans, 2012):

• **Sector fiscal**: Con base en nuevas tecnologías de información, el gobierno pone al alcance de sus ciudadanos herramientas en línea que permiten una mejor identificación de sus obligaciones, facilitando a su vez un mejor control del padrón de contribuyentes del Gobierno.

• **Sector salud**: Expedientes médicos electrónicos, telemedicina, seguimiento electrónico a pacientes con enfermedades crónicas, entre otros, son beneficios con impacto directo en la salud de los ciudadanos, al mismo tiempo que reducen costos para los gobiernos.

• **Sector social**: Identificación y mejora en la gestión de apoyos a los beneficiarios de programas gubernamentales.

• **Mejora administrativa**: Modernización de los registros civiles, rapidez en servicios de identificación ciudadana (expedición de visas, pasaportes), mejora en servicios provistos por autoridades locales.

Estas nuevas relaciones entre los ciudadanos y la administración pública imponen uno de los mayores retos de los gobiernos “La Transparencia”, es importante que Gobierno y la Administración se muestren abiertos y accesibles a la ciudadanía trabajando de la mano de estos y no a sus espaldas.

Para lograr esta transparencia de los procesos es preciso brindar toda la información hacia los ciudadanos públicamente guardando los principios de seguridad de la información, es así que se encuentran movimientos de gran importancia para el logro de este objetivo, movimientos como Open Data y Open Government, que permiten el intercambio y la aportación de datos a la ciudadanía, frecuentemente a través de la web y en formato no textual.

Estos datos permanecen abiertos al público para que los distintos agentes sociales puedan hacer uso de ellos. (Enerlis, Ernst and Young, Ferrovial and Madrid Network, 2012).

5.1.4. Acciones para implantar un gobierno electrónico

Para lograr un gobierno electrónico es necesario aplicar unos lineamientos y políticas las cuales deben ser aplicadas por las entidades en miras a cumplir con las dimensiones (Rodríguez G, 2004):

- **Generales**: Es necesario que dentro del gobierno exista un ente encargado el cumplimiento que deben hacer las entidades con relación a las instrucciones que desde el Poder Ejecutivo (presidencial) se indiquen y se establezcan en el futuro referidas al desarrollo del gobierno electrónico.
- **Atención al ciudadano**: Las diferentes dependencias administrativas deben progresivamente introducir el uso de TIC en todos los procesos asociados a brindar prestaciones a los ciudadanos, debiendo considerar la interrelación que tengan con otras dependencias públicas. Se debe fomentar y promover el acceso de los ciudadanos a los servicios e informaciones gubernamentales mediante las TIC. a la vez es necesario garantizar seguridad y velocidad, indicadores de calidad de servicio al ciudadano, utilización de estándares que aseguren compatibilidad, protección de bases de datos, privacidad en línea y sistemas de monitoreo de la gestión a los ciudadanos.

- **Buen gobierno**: Los servicios públicos deben mejorar su eficiencia operacional, mediante el uso de las TIC, simplificando y rediseñando los procesos que implementen.

- **Hacer más eficiente el uso de los recursos financieros disponibles**: Una estrategia válida en la concreción de proyectos que utilicen TIC y que resulte infactible para un único servicio desarrollado.
- **Desarrollo de la ciberdemocracia o democracia digital**: Se debe considerar las medidas para facilitar a la ciudadanía la información pertinente, la consideración de sus opiniones y sugerencias, así como facilitar instancias de participación ciudadana y transparencia.

5.1.5. Estrategia de gobierno electrónico en Latinoamérica

Uno de los grandes factores para mejorar la eficiencia y la efectividad en los servicios públicos prestados por el gobierno es emplear Gobierno electrónico.

Emplear el gobierno electrónico para mejorar la eficacia y la efectividad de la prestación de los servicios públicos en las estructuras gubernamentales es uno de los aspectos de la sostenibilidad económica.

El modelo de gobierno electrónico según el Estudio de las Naciones Unidas sobre el Gobierno Electrónico (2012) busca centralizar el acceso en la prestación de servicios, mediante un solo portal donde los ciudadanos tengan a disposición todos los servicios que provee el gobierno, independientemente de la autoridad gubernamental que los provea. De ahí la importancia que tiene su desarrollo para el cumplimiento de los objetivos gubernamentales y como los países latinoamericanos ha desarrollado la estrategia en comparación con los demás países del globo.

De acuerdo con las clasificaciones del Estudio de las Naciones Unidas sobre el gobierno electrónico 2012, la República de Corea es el líder mundial (0,9283), seguido por los Países Bajos (0,9125), el Reino Unido (0,8960) y Dinamarca (0,8889) y, bastante cerca, por los Estados Unidos de América, Canadá, Francia, Noruega, Singapur y Suecia.

Los datos para el año 2014, muestran que el ranking de países según su gobierno electrónico, es liderado por Corea del Sur, seguido de Australia y Singapur. Completan los diez primeros lugares: Francia, Holanda, Japón, Estados Unidos, Reino Unido e Irlanda del Norte y Nueva Zelanda. (Naciones unidas, 2014).

En cuanto a los países de América Latina para el año 2012 se puede observar en la tabla número 2 que Chile (0,6769) es el líder subregional en Sudamérica, seguido por Colombia (0,6572). Aunque, en forma conjunta, la subregión para el periodo mejoró su desarrollo del gobierno electrónico en 13%, de los 12 países que integran esta subregión todos descendieron en las clasificaciones mundiales, excepto Brasil (0,6167) y Suriname (0,4344), lo que indica que los países de la región, y de todo el mundo, están invirtiendo más en servicios -y expandiéndolos con más rapidez- que los países de esta subregión.

Tabla N° 4. Desarrollo del Gobierno electrónico en América del Sur

	Índice de desarrollo del gobierno electrónico		Clasificación mundial en desarrollo del gobierno electrónico	
País	2012	2010	2012	2010
Chile	0.6769	0.6014	39	34
Colombia	0.6572	0.6125	43	31
Uruguay	0.6315	0.5848	50	36
Argentina	0.6228	0.5467	56	48
Brasil	0.6167	0.5006	59	61
Venezuela	0.5585	0.4774	71	70
Perú	0.5230	0.4923	82	63
Ecuador	0.4869	0.4322	102	95
Paraguay	0.4802	0.4243	104	101
Bolivia	0.4658	0.4280	106	98
Guyana	0.4549	0.4140	109	106
Suriname	0.4344	0.3283	116	127
Promedio subregional	0.5507	0.4869		
Promedio Mundial	0.4882	0.4406		

Fuente. Imagen tomada Estudio de las Naciones Unidas sobre el Gobierno Electrónico (2012)

Del año 2012 al año 2014 el país latinoamericano con más avances en cuanto a la estrategia Gobierno Digital fue Uruguay quien realizo grandes avances pasando a la posición 24 creando la Agencia de Gobierno Electrónico y la Sociedad de la Información y del Conocimiento (AGESIC) en el 2007, lanzando en el año 2011 la Agenda Digital 2011-2015 en la cual se incluye líneas estratégicas y objetivos a realizar en tal período, como se puede observar en la tabla número 5.

Tabla N° 5. Composición y Ranking 2012-2014 de Índice de Gobiernos Electrónicos

2012	2014	Países	Servicios on line	Infraestructura de telecomunicaciones	Capital Humano	Índice Global
1	1	Corea del Sur	0,98	0,94	0,93	0,95
12	2	Australia	0,93	0,80	1,00	0,91
10	3	Singapur	0,99	0,88	0,85	0,91
6	4	Francia	1,00	0,80	0,88	0,89
2	5	Holanda	0,93	0,82	0,92	0,89
18	6	Japón	0,94	0,86	0,86	0,89
5	7	EEUU	0,94	0,74	0,94	0,87
3	8	Reino Unido	0,90	0,85	0,86	0,87
13	9	Nueva	0,84	0,75	1,00	0,86
9	10	Finlandia	0,77	0,86	0,90	0,84
50	26	Uruguay	0,85	0,56	0,81	0,74
39	33	Chile	0,82	0,49	0,82	0,71
56	46	Argentina	0,55	0,48	0,86	0,63

Fuente. Imagen tomada Informe de Naciones Unidas sobre Gobierno Electrónico (2014)

Uruguay ha alcanzado esta posición con respecto a los demás países latinoamericanos debido a los servicios online (Online Service Index – 85.0%) y el capital humano (Human Capital Index – 81.5%) – teniendo en cuenta que no es un país desarrollado. Igualmente, es notorio el desafío que se debe enfrentar respecto a la infraestructura de las telecomunicaciones, la cual, en Uruguay, posee un índice de 56.1% impidiéndole ubicarse por encima de un EGDI de 75%. Esta problemática es recurrente en muchas economías emergentes, tal como se puede apreciar en Chile, quien podría estar en el mismo nivel que Uruguay pues en términos de Servicios Online y Capital Humano tiene mínima diferencia, y Argentina, quien igualmente está más alejado. (Naciones Unidas, 2014)

Como se puede observar los países latinoamericanos han dado grandes avances en la prestación de servicios en línea. Para lograr esto se han generado muchas iniciativas de gobierno electrónico, así como varias aplicaciones para los ciudadanos mejorando la eficiencia del sector público impulsando el desarrollo sostenible.

El Estudio de las Naciones Unidas sobre el gobierno electrónico, 2012, concluye que muchos países han puesto en marcha iniciativas de gobierno electrónico, así como aplicaciones de las tecnologías de la información y las comunicaciones para el pueblo, con el fin de mejorar la eficiencia del sector público y simplificar aún más los sistemas de

gobernanza a favor del desarrollo sostenible. Las soluciones tecnológicas innovadoras han logrado un reconocimiento especial entre los líderes del gobierno electrónico, como medio para revitalizar los rezagados sectores económico y social.

5.1.6. Estrategia de gobierno en línea en Colombia

Gobierno en línea es el nombre que recibe la estrategia de gobierno electrónico (e-government) en Colombia, que busca construir un Estado más eficiente, más transparente y más participativo gracias a las TIC. (http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.htm)

Esto significa que el Gobierno:

- Prestará los mejores servicios en línea al ciudadano
- Logrará la excelencia en la gestión
- Empoderará y generará confianza en los ciudadanos
- Impulsará y facilitará las acciones requeridas para avanzar en los Objetivos de Desarrollo Sostenible -ODS, facilitando el goce efectivo de derechos a través del uso de TIC

La estrategia gobierno en línea para el estado colombiano permite proveer a las entidades públicas a nivel nacional y territorial de servicios logrando proporcionar tramites a la ciudadanía a través de los distintos medios electrónicos, mejorando la participación de la ciudadanía y la calidad que debe brindar la información que suministran las entidades del estado. Ahora los ciudadanos colombianos pueden solicitar un duplicado de cedula en línea, pagar electrónicamente para realizar concursos de méritos en la comisión nacional de servicio civil, escuchar por medio del internet sesiones en vivo de Congreso y Concejos del país.

5.1.6.1. Ejes temáticos de la estrategia

El Ministerio de las tecnologías de la Información de Colombia ha construido la estrategia gobierno en línea a partir de cuatro ejes así:

- **TIC para el Gobierno Abierto**: Busca construir un estado más transparente y colaborativo, donde los ciudadanos participan activamente en la toma de decisiones gracias a TIC.
- **TIC para Servicios**: Busca crear los mejores trámites y servicios en línea para responder a las necesidades más apremiantes de los ciudadanos.
- **TIC para la Gestión**: Busca darle un uso estratégico a la tecnología para hacer más eficaz la gestión administrativa
- **Seguridad y privacidad de la información**: Busca guardar los datos de los ciudadanos como un tesoro, garantizando la seguridad de la información.

Imagen N° 4. Ejes Temáticos de la Estrategia Gobierno en Línea – Ministerio de las Tecnologías de la información

Fuente. Imagen recuperada de https://es.slideshare.net/vivegobiernoenlinea/estrategia-de-acompaamiento-2015.

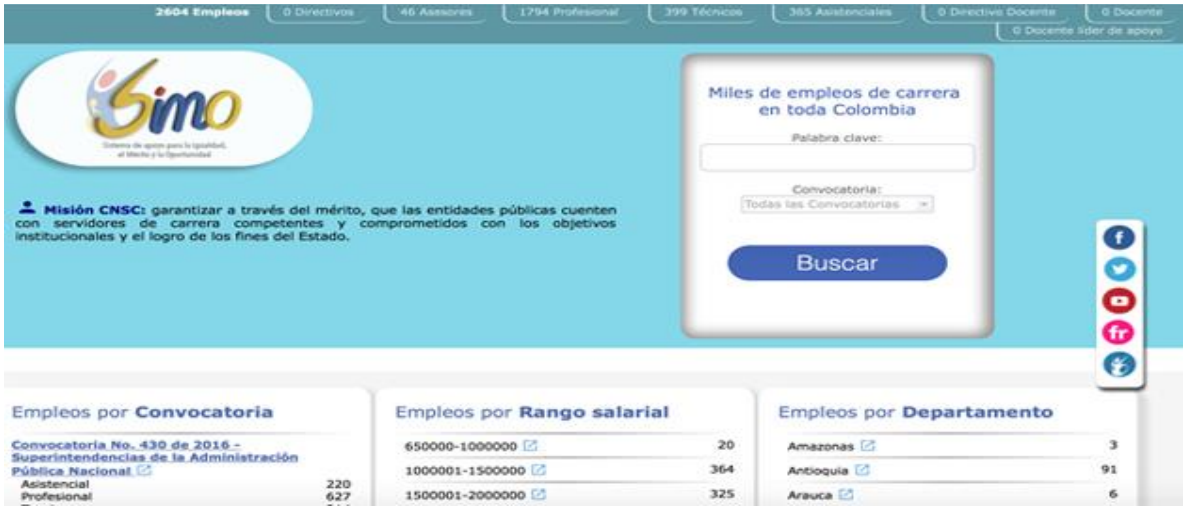
A través del Decreto 1151 de 2008 del Ministerio de Comunicaciones se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, el cual busca como objetivo principal contribuir con la construcción de un estado más eficiente, más transparente y participativo, que preste mejores servicios a

los ciudadanos y a las empresas, a través del aprovechamiento de las Tecnologías de la Información y la Comunicación.

Los principios aplicables a la Estrategia de Gobierno en Línea de acuerdo al artículo 3 son:

- Gobierno centrado en el ciudadano.
- Visión unificada del Estado.
- Acceso equitativo y multicanal.
- Protección de la información del individuo.
- Credibilidad y confianza en el Gobierno en Línea

Imagen N° 5. Estrategia de Gobierno en Línea para acceso al empleo



Fuente. http://www.mintic.gov.co/portal/604/w3-propertyvalue-7616.html

5.2. Manual Para la Implementación de Gobierno en Línea

El manual para la implementación de la estrategia de gobierno en línea determina los lineamientos para cumplir con lo establecido en el Decreto 1151 del 14 de abril de 2008 e incorpora recomendaciones del documento de "Políticas y Estándares para publicar información del Estado colombiano en Internet" del año 2000, las cuales dejan de tener vigencia a partir de la publicación del Manual. (Mintic, 2008)

El Manual para la implementación de la Estrategia de Gobierno En Línea es el Qué y el Cómo para publicar información y proveer trámites y servicios del Estado por medios electrónicos. Surge para garantizar la calidad, oportunidad, accesibilidad, uniformidad y confianza en la información y servicios institucionales ofrecidos por medios electrónicos, ya que hay que asegurar y facilitar el acceso y ubicación a información, trámites y servicios útiles y de interés ciudadano.

El Gobierno colombiano ha aunado esfuerzos desde el año 2000 con el propósito de que La política pública de Gobierno en línea sea extendida y que las entidades puedan evolucionar en forma permanente para brindar al ciudadano un mayor acceso a la ciudadanía. Convirtiéndose en una herramienta por excelencia para mejorar la gestión de lo público y la relación Estado-ciudadano.

En el año 2012 fue lanzado el nuevo manual de implementación de la estrategia gobierno en línea donde se establecen los nuevos lineamientos para la implementación de la estrategia en las entidades públicas del orden nacional y territorial donde se ha realizado un nuevo modelo que exige a las entidades esfuerzos cada vez mayores que permitan, no solo aumentar el número y uso de servicios en línea, sino también mejorar la calidad y el acceso a los mismos, así como el acceso a mayor información y datos, y que permita el involucramiento de forma directa de los demás actores de la sociedad en su construcción, todo lo anterior a través del uso eficiente de las TIC para el cumplimiento de los objetivos del Gobierno Nacional de: disminuir pobreza, aumentar seguridad y aumentar empleo.

Con el nuevo modelo se espera la alineación de actividades con otros temas esenciales de la gestión pública en Colombia, como lo son: la Política Anti trámites, la Política Nacional del Servicio al Ciudadano, la Política de Rendición de Cuentas a la

Ciudadanía, la Política Nacional Anticorrupción, la Política Nacional de Archivo y Gestión Documental, entre otras. (Mintic, 2012).

El estado con la implementación de la estrategia busca que la ciudadanía pueda acceder en forma oportuna a la información de las entidades generando un mejor proceso para la toma de decisiones y mejor ejercicio del control social.

Los ciudadanos ya no tendrán que hacer largas colas para sus trámites lo que permitiría una mejor relación ciudadanía- estado, menos costos y mayor confianza y satisfacción, dado que las entidades serán digitales porque abran incorporado las TIC de forma transversal en su operación tradicional, transformando su funcionamiento interno y la relación con sus usuarios.

Para esto las entidades contarán con sedes electrónicas, en donde se dispondrá de acceso multicanal a toda la información, así como a la gestión en línea de trámites y servicios, observando permanentemente las condiciones de accesibilidad, usabilidad, calidad, seguridad, reserva y privacidad. Igualmente, se habrá creado una cultura de colaboración y participación. (Mintic, 2012)

5.3. Normatividad

La implementación de la Estrategia de Gobierno En Línea ha sido impulsada por normas como:

- **Constitución Política de Colombia:**

A través de los siguientes artículos de la Constitución de Colombia (Asamblea Nacional Constituyente, 1991) se fundamentaron las bases para la estrategia de Gobierno en línea:

- **Artículo 23**. Toda persona tiene derecho a presentar peticiones respetuosas a las autoridades por motivos de interés general o particular y a obtener pronta resolución. El legislador podrá reglamentar su ejercicio ante organizaciones privadas. Por medio de este artículo se reglamenta uno de los más importantes derechos fundamentales para los ciudadanos para el cumplimiento de los fines

del estado como es el Derecho de Petición. Se observa que este opera eficazmente en Gobierno en línea debido a que es un servicio que se ha implementado en diferentes páginas web estatales.

- **Artículo 74**. Todas las personas tienen derecho a acceder a los documentos públicos, salvo los casos que establezca. Este artículo establece claramente el derecho a la información, el cual a través de gobierno en línea se facilitará el acceso a la ciudadanía.
- **La Directiva Presidencial No. 2 de 2000**

  En el año 2000 se aprobó el programa "Agenda de Conectividad" con el Documento CONPES 3072 del mismo año, mediante este documento se establecieron los lineamientos para el desarrollo de la Estrategia Gobierno en línea en base a estos objetivos:

Imagen N° 6. Objetivos de la Agenda de Conectividad

Fuente. Documento Conpes 3072 (ministerio de comunicaciones, 2000)

De acuerdo a esta agenda el Gobierno expidió la Directiva presidencial 02 de 2000 en el cual se establecen los lineamientos que permitirán implementar las tecnologías de información y comunicaciones las distintas entidades del estado, estableciendo 3 fases para el cumplimiento de Gobierno en línea (Presidencia de la república, 2000):

Fase 1: Proveer información en línea a los ciudadanos,

Fase 2: Ofrecer servicios y trámites en línea a los ciudadanos

Fase 3: Contratación en línea.

- La Directiva Presidencial No. 10 de 2002, la Ley 790 de 2002 y el Documento CONPES 3248 de 2003.

En la directiva presidencial 010 de 2002 se establecen metas y compromisos a cumplir por parte de los Ministros y Directores de Departamentos Administrativos y se contempla el fortalecimiento de las TIC en la gestión pública, como un abrebocas para el establecimiento del Programa Gobierno en Línea. (Presidencia de la Republica, 2002).

En concordancia con la Directiva presidencial 010 y con el fin de darle cumplimiento a esta el gobierno nacional expide la ley 790 de 2002 “"Por la cual se expiden disposiciones para adelantar el programa de renovación de la administración pública y se otorgan unas facultades Extraordinarias al Presidente de la República". En así que en su artículo 14 determina:

“**Gobierno en línea**”: El Gobierno Nacional promoverá el desarrollo de tecnologías y procedimientos denominados gobierno electrónico o en línea en las entidades de la rama ejecutiva del orden nacional y, en consecuencia, impulsará y realizará los cambios administrativos, tecnológicos e institucionales relacionados con los siguientes aspectos:

a) Desarrollo de la contratación pública con soporte electrónico;

b) Desarrollo de portales de información, prestación de servicios, y

c) Participación ciudadana y desarrollo de sistemas intergubernamentales de flujo de información.

El Gobierno Nacional desarrollará y adoptará los adelantos científicos, técnicos y administrativos del gobierno electrónico deberá realizarse bajo criterios de transparencia, de eficiencia y eficacia de la gestión pública, y de promoción del desarrollo social, económica y territorialmente equilibrado. (Congreso de la Republica, 2002).

Continuando los lineamientos generales, el alcance y los mecanismos de evaluación del Programa de Renovación de la Administración Pública (PRAP), en desarrollo de la directiva presidencial No 10 de 2002, se elabora el Documento Conpes 3248 de 2002 con el fin de lograr Estado participativo (que estimule la participación y que tenga en cuenta las demandas ciudadanas), un Estado gerencial (que administre lo público con eficiencia, honestidad, austeridad y por resultados) y un Estado descentralizado (que

tenga en cuenta las necesidades locales sin perjuicio del interés nacional y de la solidaridad regional).(Departamento nacional de planeación, 2003).

Incorporando a través del documento el Gobierno electrónico como herramienta para simplificar trámites, difundir información, reducir tiempos en los procesos, fomentar la transparencia, mejorar la coordinación interinstitucional pública y privada, facilitar las relaciones entre el ciudadano y el Estado e incrementar el control ciudadano además de introducir la estrategia anti tramites buscando establecer un marco institucional para permita simplificar, integrar y racionalizar los trámites de la administración pública

- Ley 812 de 2003, el documento Visión 2019, la Ley 1151 de 2007 y el Decreto 1151 de 2008.

La ley 812 de 2003 establece el plan de desarrollo 2003-2006 hacia un estado comunitario el cual fortalece el Programa Gobierno en Línea y los sistemas de información unificados (Congreso de la Republica, 2003). Las leyes 1151 de 2007 y el decreto 1151 de 2008 fortalecen la estrategia Gobierno en línea que dirige el Ministerio de Tecnologías de la Información y las Telecomunicaciones como entidad responsable de liderar y coordinar el desarrollo e implementación del “Programa de Gobierno en Línea”

- El Documento CONPES 3292 de 2004 y la Ley 962 de 2005.

El documento CONPES 3292 de 2004 establece el proyecto de racionalización y automatización de trámites con el fin de lograr que las relaciones entre el Estado y los ciudadanos sean simples, directas, eficientes y oportunas y que la administración pública se oriente bajo criterios gerenciales garantizando una mayor transparencia, buscando el fortalecimiento de la eficiencia y eficacia de la administración Pública a través de tres estrategias (DNP, 2004):

- Coordinación institucional y adecuación normativa
- Análisis funcional para la racionalización y
- Fortalecimiento Tecnológico, a fin de posibilitar una mayor permanencia de las políticas en materia de racionalización de trámites y automatización de los trámites, procesos y procedimientos.

Con la ley 962 de 2005 “Ley Anti tramites” la ley tiene por objeto facilitar las relaciones de los particulares con la Administración Pública, de tal forma que las actuaciones que deban surtirse ante ella para el ejercicio de actividades, derechos o cumplimiento de obligaciones se desarrollen de conformidad con los principios establecidos en los artículos 83, 84, 209 y 333 de la Carta Política. Optimizando la atención al ciudadano mediante el uso de herramientas tecnologías y sistemas de información.

Y por último las leyes y decretos que fortalecieron la transparencia y eficiencia en la contratación pública como el Decreto 2170 del 2002, el Documento CONPES 3249 de 2003, el Decreto 2434 de 2006 y la Ley 1150 de 2007.

- Decreto 1151 de 2008, ley 1341 de 2009

Por medio del decreto 1151 de 2008 se marcan los lineamientos de la estrategia gobierno en línea del MINTIC, estableciendo los objetivos y principios de la estrategia (Mintic, 2008) y mediante la ley 1341 de 2009 se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones así:

- Prioridad al acceso y uso de las TIC.
- Libre competencia,
- Uso eficiente de la infraestructura y de los recursos escasos,
- Protección de los derechos de los usuarios,
- Promoción de la Inversión.
- Neutralidad Tecnológica,
- El Derecho a la comunicación, la información y la educación y los servicios básicos de las TIC.
- Masificación del gobierno en línea.
-

Con estos ocho principios el gobierno busca promocionar en todos los sectores el uso de los TIC con el fin de aumentar la competitividad, la productividad, el respeto a los derechos humanos inherentes y la inclusión social. (Congreso de Colombia, 2009).

5.4. Avances de la Estrategia En Colombia

De acuerdo a la rendición de cuentas del Ministerio de las tecnologías de Información y comunicaciones 2014-2015 publicado en su página web, el eje que más ha realizado avances es el país en Gobierno Digital es TIC Servicios, ya se tienen más de 400 trámites completamente en línea: Se lanzó el Portal SI Virtual, que ha tenido un promedio de 668.000 visitas mensuales desde su lanzamiento en junio. A octubre de 2015 los colombianos habían accedido a 14.390 transacciones de servicios y trámites del estado a través de este servicio en la red.

Los trámites más visitados son el "pasaporte electrónico" seguido de la "copia de la inscripción en el registro civil de nacimiento, matrimonio o defunción" y el "certificado de ingresos y retenciones".

Durante el año 2015 arrancó la Ruta de la Excelencia, una carrera convocada por Mintic con el objeto de que los colombianos puedan acceder en línea a los trámites y servicios del Estado que más solicitan y que en aun no están en internet, en áreas como salud, empleo, identificación, educación, impuestos, servicios. Esto demuestra la capacidad del estado en superarse y en el aprendizaje constante para avanzar en Gobierno electrónico. (Mintic, 2016).

Los siguientes indicadores corresponden a la vigencia 2012-2016 en los ejes temáticos de gobierno en línea:

5.4.1. Tic Servicios:

Con la implementación de diversos proyectos Tic los avances han sido a pasos gigantescos, por ejemplo, en el año 2012, el porcentaje de ciudadanos que realizaban trámites o accedían a servicios por medios electrónicos era del 25%. Esta cifra creció al 30% en 2013, 38% en 2014 y en 2015 llegó al 62%. Esto demuestra que los ciudadanos colombianos cada vez prefieren los medios electrónicos para la realización de sus trámites.

5.4.1.1. Ruta de Excelencia

La ruta de la excelencia hace parte del eje temático Tic Servicios buscando dar respuesta a aquellas necesidades más imperiosas e importantes de los ciudadanos y empresarios frente al acceso a los servicios provistos por las entidades públicas y al aprovechamiento de la información pública para la generación de valor, a través de los siguientes proyectos:

Trámites y servicios en línea: Solicitud de citas médicas y autorización de servicios médicos y medicamentos, historia clínica electrónica, Afiliación única a la Seguridad Social, Inscripción y actualización en el SISBEN, Historia Laboral, Pasaporte, Registro civil (nacimiento, matrimonio y defunción), Cédula de ciudadanía, Tarjeta Militar, Convalidación de título, Facturas electrónicas, Impuesto Industria y Comercio, Impuesto Predial, Creación de empresa , Registro Sanitario, Atención de conflictos familiares en línea.

Temas para la apertura de Datos: Servicio de Salud Pública, prestación salud pública y gestión de riesgo en salud, Ordenamiento Territorial, Cadena productiva del agro, Movilidad, Seguridad Ciudadana, Calidad y cobertura educativa.

Sistemas de Información: Sistema Nacional de Atención y Reparación Integral de Víctimas, Sistema Nacional de Gestión del proceso de restitución de tierras, Sistema integrado de seguridad y emergencias a nivel territorial y nacional.

La Ruta de la Excelencia se convierte en un mecanismo nacional para impulsar tres políticas que propenden por la modernización del Estado se espera que en el 2018 los 25 proyectos que lo conforman estén dispuestos en línea y que logren transformar la relación de los ciudadanos con el Estado, agregando valor en la vida de los colombianos. (Mintic, 2016).

Además de la ruta de la excelencia este eje temático contiene:

- SI Virtual
- Carpeta Ciudadana
- Autenticación electrónica
- Sello de la excelencia

5.4.2. TIC Para Gobierno Abierto

Como se puede observar en la imagen número 5 Colombia ocupa el primer lugar en Latinoamérica y el cuarto lugar en el mundo en Datos abiertos. Es así como la estrategia de Gobierno en línea dentro del componente de TIC para Gobierno abierto que comprende el aprovechamiento de los canales digitales para lograr mayor colaboración, participación y transparencia, ha promovido que esta transformación se de en cada entidad pública, tanto a nivel nacional como territorial.

Imagen N° 7. Tic para Gobierno Abierto

Fuente. Informe de Gestión Estrategia TI 2013-2016. (Mintic, 2016).

Para el año 2015 se logró llegar a más de 600 entidades públicas del orden nacional y territorial publicando datos abiertos en el Catálogo de Colombia y a junio de 2016 el Catálogo contaba con más de 2.000 conjuntos de datos abiertos disponibles para su reutilización.

5.4.3. TIC Para La Gestión

Imagen N° 8. Tic Para Gestión

Fuente. Informe de Gestión Estrategia TI 2013-2016. (Mintic, 2016).

En la imagen número 8 se puede observar que se han realizado 93 lineamientos de obligatorio cumplimiento que mejoran la calidad de la tecnología de la información, ocho

sectores han adoptado el marco de referencia de arquitectura Ti y el nuevo modelo de interoperabilidad. Se pretende incorporar 40 nuevas entidades en el uso del marco de interoperabilidad que soporten las necesidades de los tramites priorizados en la ruta de la excelencia.

5.4.4. Seguridad y Privacidad de la Información

En el área de seguridad y privacidad de la información se han realizado sensibilización y acompañamiento al interior de las entidades que están obligadas por el decreto 1078 de 2015 y a los entes de control, los cuales deben conocer el esquema de implementación. Los sectores con los que se ha trabajado de forma especial con procesos de acompañamiento en aspectos de seguridad y privacidad, son: Entidades del Distrito Capital, Sector Defensa, Sector Hacienda y Crédito Público, Sector Planeación, Sector Inclusión social y reconciliación, Sector Presidencia de la República, Sector Minas y Energía, Sector Salud y Protección Social, Sector Comercio, Sector Vivienda.

Para el final del año 2015 se acompañó a 214 Entidades en el componente de Seguridad y Privacidad de la información, las cuales requirieron en su mayoría fortalecer las temáticas de: Diagnóstico de Seguridad y Privacidad, Plan de Seguridad y Privacidad de la Información e Implementación del Plan de seguridad y privacidad de la información. (Mintic, 2016).

Implementación de la estrategia en las diferentes entidades territoriales de Colombia.

El Ministerio de las Tecnologías de información y comunicación cada año realiza una medición de los resultados de la estrategia gobierno en línea a través de la página establecida para ello, la última evaluación realizada corresponde al año 2016, de esta evaluación se desprenden los resultados del índice de Gobierno en línea, en donde se encuentra el reporte de las Alcaldías y Gobernaciones que reportaron a la Dirección de Gobierno en línea información de su avance en la implementación de la Estrategia, en esta se puede observar los avances que han realizados las diferentes entidades territoriales que reportaron la información así:

Imagen N° 9. Índice territorial Gobierno en Línea

Departamento	Nombre Institución	TIC para servicios	Seguridad y Privacidad de la Información	ÍNDICE GEL
Huila	Alcaldía de Aipe	6	1	3
Bolívar	Alcaldía de Barranco de Loba	0	0	2
Chocó	Alcaldía de Litoral del San Juan	97	85	94
Boyacá	Alcaldía de Sativanorte	6	0	5
Cesar	Alcaldía de La Jagua de Ibirico	87	94	93
Bolívar	Alcaldía de Clemencia	0	0	1
Chocó	Alcaldía de Bajo Baudó	97	84	94
Valle del Cauca	Alcaldía de Trujillo	6	0	3
Huila	Alcaldía de Guadalupe	0	0	2
Cauca	Alcaldía de San Sebastián	6	0	4
Cauca	Alcaldía de Rosas	17	1	5
Cundinamarca	Alcaldía de Pulí	6	5	5
Córdoba	Alcaldía de Tuchín	11	0	4
Sucre	Alcaldía de Colosó	0	0	1
Nariño	Alcaldía de Barbacoas	0	0	5
Putumayo	Alcaldía de Villagarzón	7	0	4
Córdoba	Alcaldía de San José de Uré	6	0	2
Bolívar	Alcaldía de Soplaviento	97	92	93
Tolima	Alcaldía de San Luis	11	4	5
Nariño	Alcaldía de Los Andes Sotomayor	17	0	5
Huila	Alcaldía de Tello	91	87	93
Arauca	Alcaldía de Cravo Norte	11	0	4
Norte de Santander	Alcaldía de Sardinata	0	3	2
Santander	Alcaldía de Landázuri	0	1	4
Caquetá	Alcaldía de Cartagena del Chairá	0	0	1
Bolívar	Alcaldía de Montecristo	0	5	2
Bolívar	Alcaldía de Pinillos	0	1	4
Antioquia	Alcaldía de Valparaíso	11	0	5
Santander	Alcaldía de Puerto Wilches	0	0	2

Fuente. Información recuperada de Índice territorial pagina http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-14714.html

En total reportaron 1123 entidades territoriales, en la Imagen N°9 se tomó una muestra de las entidades que tenían un índice superior a 90 y las que tenían un índice menor que 10.

Las entidades con un índice superior a 90 han diseñado estrategias concernientes a cumplir con los lineamientos establecidos por Gobierno en línea en este reporte se puede concluir que las entidades con mayor índice de Gobierno en línea en Colombia son:

- Alcaldía del Litoral de san Juan
- Alcaldía de bajo baudo

Ambas ubicadas en el departamento del Choco (94), seguidas de la alcaldía de la jagua de ibirico, alcaldía de Soplaviento, alcaldía de Tello (93) en ese orden.

Y las entidades con menor índice de gobierno en línea debido a que no han realizado las acciones necesarias para la implementación de las estrategias son:

- Alcaldía de Coloso- Sucre (1)
- Alcaldía de Clemencia – Bolívar (1)
- Alcaldía de Cartagena del Chaira (1)

Seguidas de muchas otras entidades con un nivel muy bajo de implementación del gobierno en línea. Este índice territorial muestra que muy pocas entidades territoriales han diseñado proyectos para el cumplimiento de la estrategia gobierno en línea debido a que ninguna alcanza un porcentaje del 100% en este índice territorial.

5.5. Dificultades en la Implementación de la Estrategia en Colombia

Quizás las mayores barreras son la cultura de las organizaciones y la falta de apoyo a la estrategia por parte de los Directivos de las Entidades. (Mintic, 2016).

Encontramos múltiples dificultades en la implementación de la estrategia, dificultades como (Pulido Daza y Tibaduiza Ávila, 2013):

Técnicas: Las dificultades de carácter técnico generan que el proceso de incorporación por las entidades y los usuarios sea lento, complejo y tenga resistencias en algunos grupos sociales y, más aún, cuando esta no se le aplica a una sola entidad, sino por el contrario pretende abarcar a todas las entidades de un país en sus diferentes niveles y a sus ciudadanos.

Tecnológicas: La estrategia enfrenta dificultades en cuanto a conectividad a internet, el Mintic ha identificado las siguientes:

Imagen N° 10. Barreras que impiden la masificación de internet

Ciudadanos y microempresas no ven utilidad	Insuficientes aplicaciones
Bajo poder adquisitivo del ciudadano	Terminales Servicio
Alto costo para desplegar infraestructura	Dispersión y complejidad geográfica Alrededor de 200 municipios conectados con fibra óptica Complejidad administrativa última milla
Recursos	Presupuestos de inversión del gobierno limitados

Fuente. Imagen de Dificultades técnicas para la implementación de la nueva normativa en el desarrollo de la estrategia de gobierno en línea y la gestión documental en Colombia

Existen dificultades para llegar a todos los municipios, los recursos son escasos para adquirir infraestructura tecnológica, los ciudadanos no consideran importante el uso de internet sobre todo en sectores alejados y los recursos el gobierno no es suficiente a la hora de atender las necesidades.

Organizacionales: Dentro de las organizaciones aun encontramos gran resistencia al cambio sobre todo en las entidades públicas, donde no se han organizado adecuadamente en sistemas por procesos. Entre las dificultades que más se marcan en el aspecto organizacional podemos encontrar los procesos, el recurso humano y el presupuesto.

5.6. Componentes Implementación de la Estrategia

El manual de implementación establece seis componentes para el desarrollo de la estrategia así (Mintic, 2012):

Tabla N° 6. Componentes Implementación de la Estrategia Gobierno en Línea.

Componente	Objetivo
Elementos transversales	Identificar las necesidades de los usuarios e investigar permanentemente sobre los cambios en las tendencias de comportamiento, para aplicar este conocimiento a sus diferentes momentos de interacción, con la información definir e implementar procesos de mejoramiento permanente en la gestión de tecnología y en la aplicación de un Sistema de Gestión de Seguridad para la protección de los activos de información.
Interacción en línea	Habilitar la comunicación de dos vías de entidades con ciudadanos y empresas. Se ofrecen mecanismos que acercan al ciudadano con la administración, le posibilitan contactarla y hacer uso de la información que proveen las entidades en sus sitios Web.
Información en línea	Garantizar que los diferentes tipos de usuarios tengan acceso electrónico a toda la información relativa a la misión, planeación estratégica, trámites y servicios, espacios de interacción, ejecución presupuestal, funcionamiento, inversión, estructura organizacional, datos de contacto, normatividad relacionada, novedades y contratación, observando las reservas constitucionales y de Ley, cumpliendo todos los requisitos de

Componente	Objetivo
	calidad, disponibilidad, accesibilidad, estándares de seguridad y dispuesta de forma tal que sea fácil de ubicar, utilizar y reutilizar.
Transacción en línea	Brindar a los distintos tipos de usuarios trámites y servicios cuales podrán gestionarse por diversos canales electrónicos, permitiéndoles realizar desde la solicitud hasta la obtención del producto sin la necesidad de aportar documentos que reposen en cualquier otra entidad pública o privada que cumpla funciones públicas
Transformación	Mejorar la eficacia en la ejecución de los procesos eliminando trámites y estableciendo las pautas para que la entidad automatice sus procesos y procedimientos internos.
Democracia en línea	Empoderar a los ciudadanos e involucrarlos en el proceso de toma de decisiones. Promover que las entidades públicas incentiven a la ciudadanía a contribuir en la construcción y seguimiento de políticas, planes, programas, proyectos, la toma de decisiones, el control social y la solución de problemas que involucren a la sociedad en un diálogo abierto de doble vía.

Fuente: MINTIC Estrategia Gobierno en línea: 2012 – 2015 para el orden nacional, 2012 – 2017 para el orden territorial. Manual 3.1. 2012.

5.7. Componente TIC Para Servicios

5.7.1. Logro Servicios Centrados En El Usuario

A través de este componente el gobierno coloca al servicio de los ciudadanos una oferta de servicios que le permitirán tener una mayor interacción con ellos, es así que estos (ciudadanos) podrán contar con una oferta de trámites, servicios y espacios de comunicación a través de canales electrónicos usables y accesibles que responden a sus necesidades y expectativas. (Mintic, 2015).

Con el fin de lograr el cumplimiento de este elemento de tic servicios la estrategia gobierno en línea estableció los siguientes criterios:

- **Caracterización de los usuarios**: A través de este elemento se podrá conocer las necesidades y características de los usuarios, ciudadanos y grupos de interés con el fin de que los trámites y servicios respondan a estas necesidades.

- **Accesibilidad**: Busca que los trámites y servicios disponibles por medios electrónicos cuenten con las características necesarias para que toda la población pueda acceder a ellos, incluso aquella que se encuentra en situación de discapacidad.
- **Usabilidad**: Busca que los trámites y servicios disponibles por medios electrónicos sean de fácil uso, y proporcionen una mejor experiencia a los usuarios, ciudadanos y grupos de interés.
- **Promoción**: Busca aumentar el conocimiento, uso y preferencia de trámites y servicios electrónicos por parte de los usuarios internos y externos.
- **Evaluación de Satisfacción del Usuario:** Busca conocer el grado de satisfacción de los distintos usuarios respecto a la oferta de trámites y servicios electrónicos habilitados por la entidad.
- **Mejoramiento continuo**: Busca aumentar los niveles de satisfacción de los usuarios a través de acciones permanentes de mejoramiento de los trámites y servicios electrónicos.

5.7.2. Logro Sistema Integrado Peticiones, Quejas, Reclamos y Denuncias (PQRD)

A través de este componente se busca que la entidad cuente con múltiples canales que operan de forma integrada, para la atención de peticiones, quejas, reclamos y denuncias para ofrecer a la ciudadanía (Mintic, 2015):

- **Sistema web de contacto, peticiones, quejas, reclamos y denuncias (PQRD)**: A través de este elemento los usuarios podrán contar con un canal de atención y comunicación con la entidad. Con este sistema se realiza seguimiento a las PQRD y se establecen directrices para el mejoramiento continuo.
- **Sistema móvil de contacto, peticiones, quejas, reclamos y denuncias**: Canales de comunicación a través de las tecnologías móviles, facilitando el seguimiento permanente y desarrollando acciones de mejoramiento continuo a partir de la evaluación de la satisfacción del usuario.

- **Sistema integrado de peticiones, quejas, reclamos y denuncias (PQRD):** Integración y centralización de las peticiones, quejas, reclamos y denuncias recibidas a través de los diferentes canales habilitados para tal fin.

5.7.3. Logro Trámites y Servicios en Línea

Los usuarios cuentan con múltiples canales que operan de forma integrada, para la atención de peticiones, quejas, reclamos y denuncias. (Mintic, 2015).

Los criterios para este logro son:

- **Formularios descargables, diligénciales y transaccionales**: Buscan facilitar a los usuarios, ciudadanos y grupos de interés la disposición, diligenciamiento y/o envío de formularios requeridos para la realiza.

- **Certificaciones y constancias en línea**: Busca que los usuarios internos y externos puedan gestionar completamente en línea sus certificaciones y constancias.
- **Trámites y servicios en línea**: Busca que los usuarios puedan gestionar los trámites y servicios ofrecidos por las entidades completamente en línea.
- **Ventanilla Única**: Busca que el usuario gestione de manera integrada los trámites y servicios agrupados por temáticas, intereses o poblaciones, que están en cabeza de una o varias entidades. De esta manera se provee una solución completa al usuario presentando una cara unificada del Estado.

5.8. Componente Seguridad y Privacidad de la Información

El componente Tic seguridad y privacidad de la información busca acciones tendientes a la protección de la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada. Mintic (2015).

Este componente tiene tres logros así:

- Definición del marco de seguridad y privacidad de la información y de los sistemas de información.
- Implementación del plan de seguridad y privacidad de la información y de los sistemas de información.
- Monitoreo y mejoramiento continuo.

5.8.1. Logro Definición del Marco de Seguridad y Privacidad de la Información y de los Sistemas de Información.

A través de este logro se busca determinar el estado actual del nivel de seguridad y privacidad de la información y de los sistemas de información. Mintic (2015).

Los criterios para este logro:

- **Diagnóstico de seguridad y privacidad de la información**: Busca determinar el estado actual del nivel de seguridad y privacidad de la información y de los sistemas de información.
- **Plan de Seguridad y Privacidad de la Información**: Busca generar un plan de seguridad y privacidad alineado con el propósito misional.

5.8.1. Logro Implementación del Plan de Seguridad y Privacidad de la Información y de los Sistemas de Información

A través de la implementación del plan de seguridad y privacidad de los sistemas de información se busca desarrollar las acciones definidas en el plan de seguridad y privacidad. (Mintic, 2015).

Los criterios para este logro son:

- **Gestión de riesgos de seguridad y privacidad de la información**: Busca proteger los derechos de los usuarios de la entidad y mejorar los niveles de confianza en los mismos a través de la identificación, valoración, tratamiento y mitigación de los riesgos de los sistemas de información.

5.8.2. Logro Monitoreo y Mejoramiento Continuo

El logro monitoreo y mejoramiento continuo pretenden que se desarrollen actividades para la evaluación y mejora de los niveles de seguridad y privacidad de la información y los sistemas de información. (Mintic, 2015).

Criterio para este logro:

- **Evaluación de desempeño**: Busca hacer las mediciones necesarias para calificar la operación y efectividad de los controles, estableciendo niveles de cumplimiento y de protección de los principios de seguridad y privacidad de la información.

5.9. Modelo de Seguridad y Privacidad de la Información

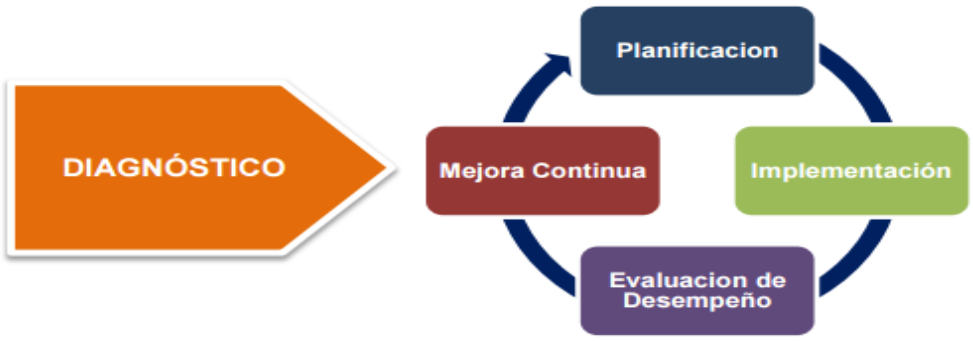
El modelo de seguridad y privacidad de la información comprende el proceso de construcción de una política de privacidad por parte de la entidad, que permita fijar los criterios que seguirán para proteger la privacidad de la información y los datos, así como de los procesos y las personas vinculadas con dicha información. (Mintic, 2015).

A través del modelo de seguridad y privacidad de la información y con el uso de los TIC las entidades estatales buscaran garantizar la protección de la información y privacidad de los datos de acuerdo a las normas colombianas.

El modelo establece 5 fases que permiten gestionar adecuadamente la seguridad y privacidad de sus activos de información. Seguridad que debe gestionarse debido a las amenazas que se ciernen sobre los sistemas de información, amenazas que cada día se tornan más avanzadas y complejas de ahí que la regulación normativa este exigiendo mayor protección a los datos sensibles, personales, comerciales y financieros (Congreso de Colombia, 2012-2013).

El Modelo de seguridad y privacidad de la Información basado en el estándar NTC-ISO-IEC 27001: 2013, brinda la protección necesaria para establecer y mantener un gobierno de seguridad acorde a los objetivos institucionales, demarcando la estructura organizacional con roles y responsabilidades y un conjunto coherente de políticas, procesos y procedimientos que le permitan gestionar los riesgos que atentan contra la confidencialidad, integridad, disponibilidad de la información y de los bienes que la contienen o la procesan. (Tarazona, 2007).

Imagen N° 11. Modelo de Seguridad y Privacidad de la Información



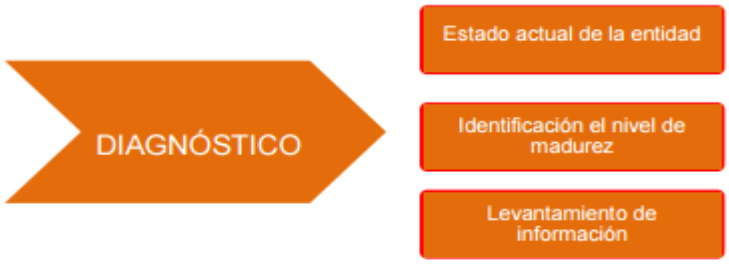
Fuente. Modelos de seguridad y privacidad de a información. Mintic (2015).

5.9.1. Fases del Modelo de Seguridad y Privacidad de la Información.

5.9.1.1. Fase de Diagnóstico

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información. (Mintic, 2015).

Imagen N° 12. Etapas Previas a la Implementación



Fuente. Modelos de seguridad y privacidad de a información. Mintic (2015).

En la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- Determinar el nivel de madurez de los controles de seguridad de la información.

- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en ciberseguridad.

5.9.1.2. Fase de Planificación

En esta fase se deben utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineada con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

El alcance del MSPI permite a la Entidad definir los límites sobre los cuales se implementará la seguridad y privacidad en la Entidad. Este enfoque es por procesos y debe extenderse a toda la Entidad. En el desarrollo del alcance y los límites del Modelo se deben tener en cuenta:

Procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos.

Imagen N° 13. Fase de Planificación

Fuente. Modelos de seguridad y privacidad de a información. Mintic (2015).

La fase de planificación del Modelo de Seguridad y Privacidad de la Información comprende:

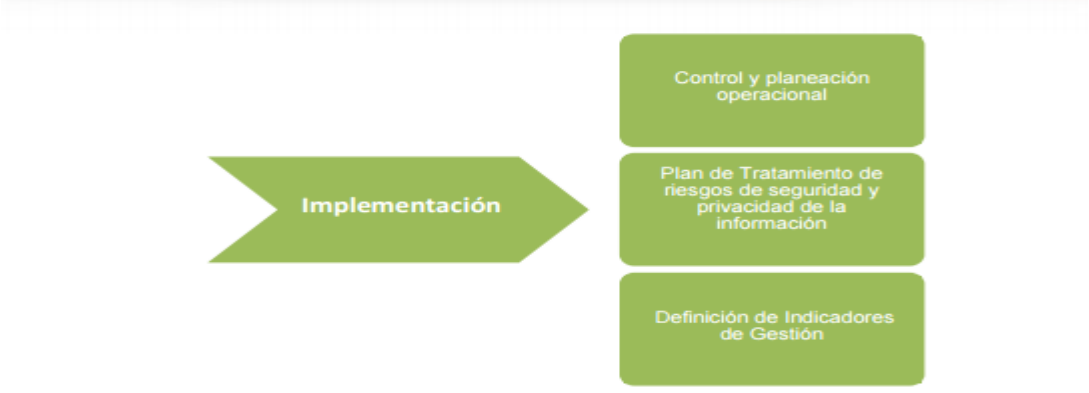
- **Política de seguridad y privacidad de la información**: Documento de alto nivel que incluye la voluntad de la Alta de la Entidad para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información. La política debe contener una declaración general por parte de la administración, donde se especifique sus objetivos, alcance, nivel de cumplimiento. La política debe ser aprobada y divulgada al interior de la entidad.
- **Políticas de Seguridad y Privacidad de la Información**. Manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información.
- **Procedimientos de Seguridad de la Información**: En este Ítem se debe desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos definidos en la entidad.
- **Roles y Responsabilidades de Seguridad y Privacidad de la Información**: La entidad debe definir mediante un acto administrativo (Resolución, circular, decreto, entre otros) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de la Entidad.
- **Inventario de activos de información**: La entidad debe desarrollar una metodología de gestión de activos que le permita generar un inventario de activos de información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios.
- **Integración del MSPI con el Sistema de Gestión documental**: La entidad deberá alinear la documentación relacionada con seguridad de la información con el sistema de gestión documental generado o emitido conforme a los parámetros emitidos por el archivo general de la nación.

- **Identificación, Valoración Y Tratamiento de Riesgos**: La entidad debe definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, así como la declaración de aplicabilidad.
- **Plan de Comunicaciones**: La Entidad debe definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) de la entidad. Este plan será ejecutado, con el aval de la Alta, a todas las áreas de la Entidad.
- **Plan de transición de IPv4 a IPv6**: Para llevar a cabo el proceso de transición de IPv4 a IPv6 en las entidades, se debe cumplir con la fase de planeación establecida en la Guía No 20 - Transición de IPv4 a IPv6 para Colombia que indica las actividades específicas a desarrollar.

5.9.1.3. Fase de implementación

Esta fase le permitirá a la Entidad, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI. (Mintic, 2015).

Imagen N° 14. Fase de Implementación



Fuente. Modelos de seguridad y privacidad de a información. Mintic (2015).

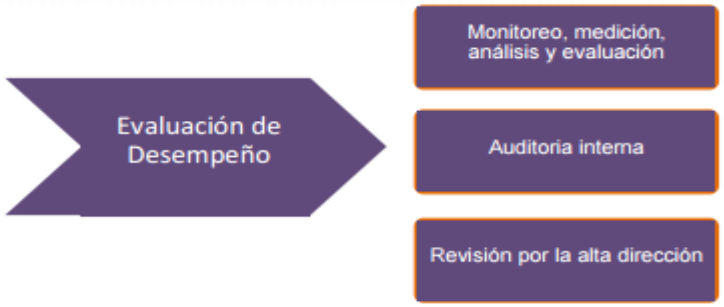
Con base a los resultados de la fase de planeación, en la fase de implementación deberá ejecutarse las siguientes actividades:

- **Planificación y Control Operacional**: La entidad debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos. La entidad debe tener información documentada en la medida necesaria para tener la confianza en que los procesos se han llevado a cabo según lo planificado, adicionalmente, deberá llevarse un control de cambios que le permitan tomar acciones para mitigar efectos adversos cuando sea necesario.
- **Implementación del plan de tratamiento de riesgos**: Se debe implementar el plan de tratamiento de riesgos de seguridad de la información, en el cual se identifica el control a aplicar para llevar cada uno de los riesgos a un nivel aceptable para la entidad, en donde la base para ejecutar esta actividad es la Guía No 8 - de controles de seguridad y privacidad del MSPI. Es preciso tener en cuenta que la aplicación del control sobre los riesgos detectados debe estar aprobados por el dueño de cada proceso.
- **Indicadores De Gestión**: La entidad deberá definir indicadores que le permitan medir la efectividad, la eficiencia y la eficacia en la gestión y las acciones implementadas en seguridad de la información. Los indicadores buscan medir:
- Efectividad en los controles.
- Eficiencia del MSPI al interior de la entidad.
- Proveer estados de seguridad que sirvan de guía en las revisiones y la mejora continua.
- Comunicar valores de seguridad al interior de la entidad.
- Servir como insumo al plan de control operacional.
- Plan de Transición de IPv4 a IPv6: Se deberá generar el documento detallado con el plan de transición e implementación del protocolo IPv6 en la entidad.

5.9.1.4. Fase de Evaluación de Desempeño

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas. (Mintic, 2015).

Imagen N° 15. Fase Evaluación de Desempeño



Fuente. Modelos de seguridad y privacidad de a información. Mintic (2015).

Esta fase comprende:

- Plan de revisión y seguimiento a la implementación del MSPI, en esta actividad la entidad debe crear un plan que contemple las siguientes actividades:
  - Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
  - Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
  - Seguimiento a la programación y ejecución de las actividades de autorías internas y externas del MSPI.
  - Seguimiento al alcance y a la implementación del MSPI.
  - Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
  - Medición de los indicadores de gestión del MSPI
  - Revisiones de acciones o planes de mejora (solo aplica en la segunda revisión del MSPI)

A través del desarrollo de este plan se consolidarán los indicadores en forma periódica y se realizara la evaluación a las metas esperadas.

- Plan de ejecución de las auditorias.

Se generará un plan de auditorías para el MSPI con el fin de verificar si el modelo esta con conforme con los requisitos de la organización, está implementado adecuadamente y se mantiene de forma eficaz; así mismo es necesario difundir a las partes interesadas, los resultados de la ejecución de las auditorías.

5.9.1.5. Fase Mejoramiento Continuo

En esta fase se consolidan los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas. (Mintic, 2015).

En esta fase es importante que la entidad defina y ejecute el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño.

Imagen N° 16. Fase Mejoramiento Continuo

Fuente. Modelos de seguridad y privacidad de a información. Mintic (2015).

Este plan incluye:

- Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.

- Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.

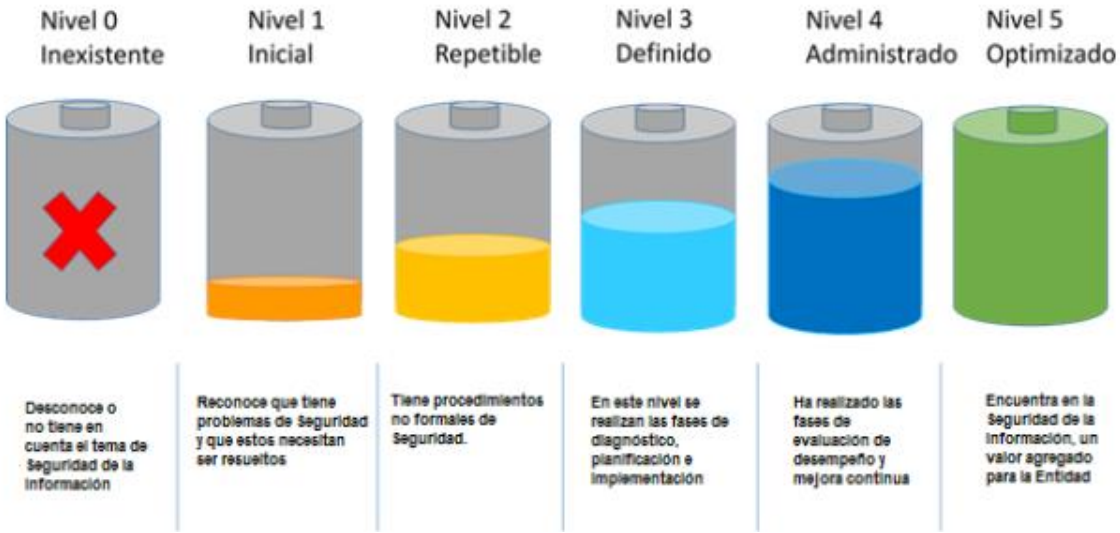
Con los anteriores insumos, la entidad puede efectuar los ajustes a los entregables, controles y procedimientos dentro del MSPI. Estos insumos tendrán como resultado un plan de mejoramiento y un plan de comunicaciones de mejora continua, revisados y aprobados por la Alta de la entidad.

La revisión por la Alta hace referencia a las decisiones, cambios, prioridades etc. tomadas en sus comités y que impacten el MSPI.

5.9.1.6. Modelo de Madurez

Este esquema permite identificar el nivel de madurez del MSPI en el que se encuentran las entidades, midiendo la brecha entre el nivel actual de la entidad y el nivel optimizado. A continuación, la figura 8, muestra los diferentes niveles que hacen parte del modelo de madurez. (Mintic, 2015).

Imagen N° 17. Niveles de Madurez



Fuente. Modelos de seguridad y privacidad de a información. Mintic (2015).

El esquema que muestra los niveles de madurez del MSPI, busca establecer unos criterios de valoración a través de los cuales se determina el estado actual de la seguridad de la información en una entidad del Estado.

En la siguiente tabla se muestran las características del nivel de madurez:

Tabla N° 7. Características de los Niveles de Madurez

NIVEL	DESCRIPCIÓN
Inexistente	Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo, no están alineados a un Modelo de Seguridad. No se reconoce la información como un activo importante para su misión y objetivos estratégicos. No se tiene conciencia de la importancia de la seguridad de la información en la entidad.
Inicial	Se han identificado las debilidades en la seguridad de la información. Los incidentes de seguridad de la información se tratan de forma reactiva. Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.
Repetible	Se identifican en forma general los activos de información. Se clasifican los activos de información. Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información. Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión. La entidad cuenta con un plan de diagnóstico para IPv6.
Definido	La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información. La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información. La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas. La Entidad tiene procedimientos formales de seguridad de la Información La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información. La Entidad ha realizado un inventario de activos de información aplicando una metodología.

NIVEL	DESCRIPCIÓN
	La Entidad trata riesgos de seguridad de la información a través de una metodología. Se implementa el plan de tratamiento de riesgos. La entidad cuenta con un plan de transición de IPv4 a IPv6. Administrado
Administrado	Se revisa y monitorea periódicamente los activos de información de la Entidad. Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información. Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro. La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6. Optimizado
Optimizado	En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización. Se utilizan indicadores de efectividad para establecer si la entidad encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales. La entidad genera tráfico en IPv6.

Fuente. Modelos de seguridad y privacidad de a información. Mintic (2015).

5.9.1.7. Otros Modelos De Madurez

Tabla N° 8. Modelo de Madurez de Seguridad de la Información Existentes y Publicados.

MODELO	DESCRIPCIÓN	COMENTARIOS
Modelo de Madurez de Seguridad TI de NIST CSEAT	Cinco niveles de madurez progresiva: Política Procedimiento Implantación Prueba Integración	Centrado en niveles de documentación
Modelo de Evaluación de la Seguridad de la Información de Citigroup (CITI-ISEM)	Cinco niveles de madurez progresiva: Autocomplacencia Reconocimiento Integración Prácticas comunes Mejora continua	Centrado en concienciación y adopción por parte de la organización
Modelo de madurez de COBIT®	Cinco niveles de madurez progresiva: Inicial / ad hoc Repetible pero intuitivo Proceso definido Gestionado y medible Optimizado	Centrado en procedimientos específicos de auditoría
Modelo SSE-CMM	Cinco niveles de madurez progresiva: Realizado informalmente Planificado y perseguido Bien definido	Centrado en ingeniería de seguridad y diseño de software

MODELO	DESCRIPCIÓN	COMENTARIOS
	Controlado cuantitativamente Continuamente mejorado	
Evaluación de la Capacidad de Seguridad de CERT/CSO	Cinco niveles de madurez progresiva: Existente Repetible Persona designada Documentado Revisado y actualizado Mide usando cuatro niveles: Inicial En desarrollo Establecido Gestionado	Centrado en la medición de la calidad relativa a niveles de documentación

Fuente. Imagen tomada de Cómo puede medirse la seguridad David A. Chapin -CISA, CISM, CISSP, IAM- y Steven Akridge -JD, CSM, CM, CISSP, IAM (2005)

Los modelos de madurez se convierten en una medida importante para comparar una organización con otra, con la definición del nivel de madurez la entidad comprenderá mejor su programa de seguridad con respecto a otra, evaluando así el grado de confianza de los sistemas interconectados. En una implantación de elementos. En un programa maduro, los elementos son ejecutados basándose en el resultado de las etapas de implantación previas. Así la gerencia tendrá claro cuándo puede o debe comprar seguridad. (David A. Chapin -CISA, CISM, CISSP, IAM- y Steven Akridge -JD, CSM, CM, CISSP, IAM 2005).

Con los niveles de madurez definidos la entidad no diseñara medidas de seguridad incorrectas siendo una herramienta que permite tener claridad acerca de las medidas de seguridad que debe tomar la empresa para sus sistemas de información y la información.

Esto no quiere decir que utilizando los niveles de madurez ya la organización está segura e implanto las medidas correctas a estos niveles de madurez hay que añadirle calidad y eficiencia lo que permitirá así a la entidad los logros que en materia de seguridad desean alcanzar.

5.10. Marcos de Referencia para la Implementación de Gobierno TI

Un marco de referencia es una herramienta que permite desarrollar sobre bases sólidas que los recursos de TI estén alineados con los objetivos de la entidad.

Un Marco de referencia de Gobierno TI para el estado colombiano es el punto de partida para que las instituciones del Estado direccionen la forma como entienden,

planean, adquieren y usan las TI. Siguiendo las buenas prácticas que hacen parte del Marco, las entidades pueden optimizar la gestión TI para desarrollar con mayor efectividad su estrategia y el modelo operacional desde una visión integral del Estado. (Mintic, 2017).

Las mejores prácticas de TI posibilitan y soportan (Cruz y Martínez, 2011):

- Una mejor gestión de TI, lo que es crítico para el éxito de la estrategia de la empresa.
- Un gobierno eficaz de las actividades de TI.
- Un marco de referencia eficaz para la gestión de políticas, controles internos y prácticas definidas, lo que es necesario para que todos sepan lo que hay que hacer.
- Muchos otros beneficios, incluyendo ganancia de eficiencias, menor dependencia de expertos, menos errores, mejora de la confianza de los socios de negocios y de regulador.
- El Marco de Referencia para el estado colombiano adopta las mejores prácticas del mercado, por ejemplo, ITIL, COBIT, PMI, ISO. (Mintic 2017).

Entre los marcos de referencia más representativos para desarrollar el gobierno TI encontramos:

Tabla N° 9. Cuadro comparativo de normas y estándares TI

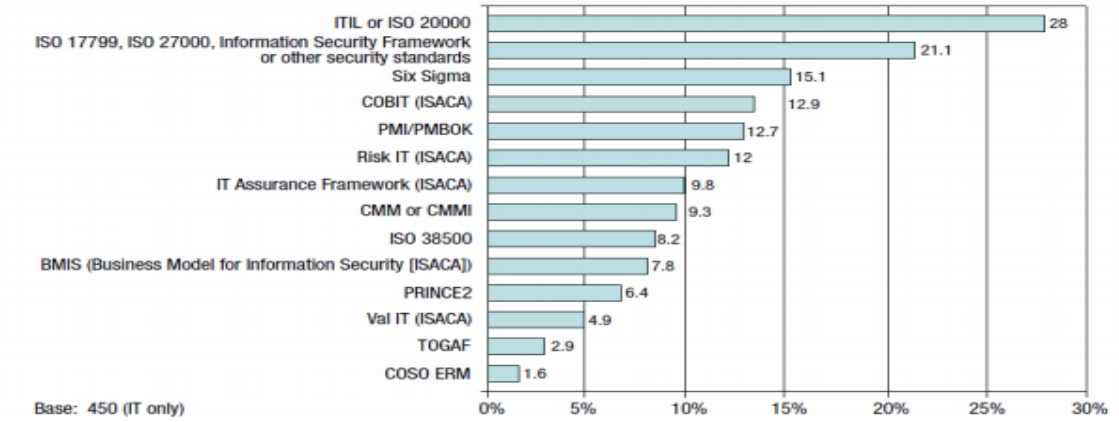
NORMA TI	DESCRIPCIÓN
COBIT	Ayuda a las Organizaciones a crear un valor óptimo a partir de la TI, al mantener un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos. Permite que la información y tecnologías relacionadas se gobiernen y administren de una manera holística en toda la Organización, incluyendo el alcance completo de todas las áreas de responsabilidad funcionales y de negocios, considerando los intereses relacionados con la TI de las partes interesadas internas y externas.
Valit	Definir la relación entre TI y el negocio y las funciones de la organización con responsabilidades de gobierno; Manejar el portafolio de una organización de las inversiones de negocio que permiten TI; y Maximizar la calidad de los casos de negocio

NORMA TI	DESCRIPCIÓN
	para las inversiones de negocio que permiten la TI con especial énfasis en la definición de los principales indicadores financieros
ITIL	ITIL son unas recomendaciones para la correcta gestión de los departamentos IT y se especifican los procesos y procedimientos para ello. No se habla de software ni hardware ni nada por el estilo, es más como una manera de trabajar más ordenada y realmente dirigida a servir a negocio
CMMI	Es un modelo para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de sistemas de software.
ISO/IEC 38500	Es un estándar internacional que provee directrices para el gobierno corporativo de TI y ayuda a los miembros de altos niveles de una organización a entender y cumplir cabalmente sus obligaciones legales, regulatorias y éticas respecto del uso de TI en las organizaciones. Esta norma define el buen gobierno de las TI como el sistema usado por la alta dirección de la organización para controlar el uso presente y futuro de las TI en la organización, de manera que se consigan los planes y objetivos de la misma.
ISO/IEC 90003	Como objetivo tiene el definir requisitos para un sistema de gestión de la seguridad de la información (SGSI), con el fin de garantizar la selección de controles de seguridad adecuados y proporcionales, protegiendo así la información.
Risk IT	Es un marco de referencia normativo basado en un conjunto de principios rectores para una gestión efectiva de riesgos de TI
Coso	Dedicada a proporcionar orientación a la gestión ejecutiva y las entidades de gobierno sobre los aspectos fundamentales de organización de este, la ética empresarial, control interno, gestión del riesgo empresarial, el fraude, y la presentación de informes financieros

Fuente. Información tomada de cuadro comparativo de normas y estándares TI (Zaid Agustín ,2014)

En la imagen número 18 se presentan los marcos y estándares más utilizados según el informe sobre la Gobernabilidad de TI en las empresas realizado por ISACA y el IT Gobernance institute.

Imagen N° 18. Marcos y estándares más utilizados para la gobernabilidad de TI



Fuente. Global Status Report on the Governance of Enterprise it (Gelt) -2011

5.11. Comparación de los Marcos Para Gobierno de TI

Para la comparación de los marcos de referencia de los diferentes modelos de TI se han considerado algunos de los modelos de TI observados y se han tomado los factores más importantes para la realización de la comparación integración de los modelos.

Estos factores son:

- INFORMACIÓN
- ESTRATEGIA TI
- GOBIERNO DE TI
- SISTEMAS DE INFORMACIÓN
- SERVICIOS TECNOLÓGICOS
- USO Y APROPIACIÓN

De acuerdo al estudio realizado por MINTIC en el año 2015 donde se hizo una consultoría con el fin de revisar los referentes internacionales y hacer comparación de dominios y marcos de referencia internacional para la creación del marco de Gobierno Colombiano:

Imagen N° 19. Marcos de Arquitecturas por países Referentes internacionales

Corea	USA	Canadá	España	Australia	Brasil	UK	Colombia
TOGAF TRIZZ	GEA (Government EA Capability Dimension) Integra : TOGAF-FEAF	MAGENTA TOGAF FEAF BSC SOA BPM BSM	FEAF ZACHMANN TOGAF BPM	AGA Magenta FEAF PEAF ITIL SOA	TOGAF ITIL BPM	xGEA	Propuesta: GEA.co

Fuente. Mintic, 2015

De este análisis se tomaron los dominios para el modelo colombiano así:

Imagen N° 20. Cuadro comparativo de los diferentes Marcos Internacionales con el Marco de Referencia de Arquitectura Empresarial para la Gestión de Tecnologías de la Información- Colombia

	Dominios de arquitectura	Corea	USA	Canadá	España	Australia	Brasil	UK	Colombia (*)
	Innovación	x							
INFORMACIÓN	Gestión del Conocimiento	x							x
	Datos		x	x	x				
ESTRATEGIA DE TI	Negocio	x	x	x	x	x	x		
	Estrategia		x	x		x		x	x
	Seguridad		x	x				x	
GOBIERNO DE TI	Gobierno	x	x	x		x			x
SISTEMAS DE INFORMACIÓN	Sistemas de Información	x					x	x	x
	Aplicaciones		x	x	x				
SERVICIOS TECNOLÓGICOS	Tecnología	x	x	x	x	x	x	x	x
	Gestión del Servicio							x	
USO Y APROPIACIÓN	Uso y Apropiación								x

Fuente. Mintic, 2015

Como se puede observar el marco de gobierno de TI tomo elementos de los diferentes marcos de gobierno, tales como Información (Gestión del Conocimiento), estrategia TI (estrategia) Gobierno TI(Gobierno), Sistemas de información (Sistema de información y aplicaciones) servicios tecnológicos (tecnología) y uso apropiación.

Retomando el Marco de Referencia de AE para el Estado Colombiano Mintic, SF, p. 06) se definieron los dominios así:

- **Dominio de Información**: Consiste en el establecimiento de patrones que guiarán la gobernabilidad de la Información, de manera segura y confiable. Entre estos, se tienen: el aseguramiento de la calidad de las TI, la gestión de su ciclo de vida, el análisis de la información y el uso estratégico de ésta, a partir del desarrollo de habilidades y competencias entre el personal empleado con este fin.
- **Dominio de Sistemas de Información**: Estructura los lineamientos para el manejo de aplicaciones y procesos de TI.
- **Dominio de Servicios Tecnológicos**: Trata todos los modelos que se requieren para la implementación de la infraestructura tecnológica, los sistemas, servicios de TIC, operaciones y servicios.
- **Dominio de Estrategia de TI**: Consiste en el diseño de estrategias que se mantendrán alineadas con las estrategias del Estado.
- **Dominio de Gobierno de TI**: Son las guías que serán empleadas para el diseño de proyectos de gobernabilidad, relacionadas con tecnologías de la información, así como políticas, procesos, estructuras y proveedores de TI.
- **Dominio de Uso y Apropiación**: Define los lineamientos para la gestión de cambio y grupos de interés.

5.12. Privacidad de la Información

El principal objetivo del modelo de seguridad y privacidad de la Información es garantizar el manejo adecuado de la información pública en poder de las entidades destinatarias, la cual es uno de los activos más valiosos para la toma de decisiones, el modelo propende por un doble enfoque a saber: a nivel de seguridad marcando un

derrotero para que las entidades destinatarias construyan unas políticas de seguridad sobre la información a fin de salvaguardar la misma a nivel físico y lógico, de manera que se pueda en todo momento garantizar su integridad, disponibilidad y autenticidad.

En esa línea el aseguramiento de los procesos relacionados con los sistemas de información debe complementarse con un enfoque de privacidad para garantizar tanto la protección de los derechos a la intimidad y el buen nombre o la salvaguarda de secretos profesionales, industriales o de información privilegiada de particulares en poder de la administración como el acceso a la información pública cuando esta no se encuentre sometida a reserva. Para ello se requiere dotar al modelo de seguridad de la información de un componente específico relacionado con la privacidad. (Mintic, 2015).

Para que exista claridad sobre la privacidad es necesario tener claro los procesos relacionados con la recolección y uso de información son susceptibles de ser objeto de implementación de medidas de privacidad, como puede ser (Mintic, 2015):

- La Implementación de un sistema de información que tenga la posibilidad de recolectar datos personales, tal como un sistema de seguridad a través de video vigilancia que capture imágenes, datos biométricos, etc.
- El Diseño y ejecución de un sistema de gestión documental
- El Desarrollo de políticas que impliquen la necesidad de recolectar y usar información personal, como por ejemplo políticas de atención de PQRS.
- La Transferencia de información a terceros (otras entidades o países)

Para lograr esto es necesario:

- **Contar con una herramienta de análisis sobre impacto en la privacidad**: Herramienta como MSPI
- **Descripción de los flujos de información**: La cual permite saber qué información está siendo recolectada, con qué propósito, cómo, en qué cantidad y si la misma es objeto de divulgación.
- **Identificar los riesgos de privacidad Los riesgos en relación con la privacidad pueden ser de varios tipos**:
  - En relación con la información personal de los individuos
  - En relación con la información de usuarios institucionales

5.13. Seguridad de la Información

Para tener claridad acerca de los conceptos y modelos que se utilizara en el diseño del eje temático Seguridad y Privacidad de la información se analizaran los distintos conceptos, marco legal y teorías inherentes al Sistema de Gestión en Seguridad de la Información que enmarca el Modelo de seguridad y privacidad de la información.

Para la Asociación Española de la Calidad la Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada. La seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Podemos entender como seguridad un estado de cualquier sistema o tipo de información (informático o no) que nos indica que ese sistema o información está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar a su funcionamiento directo o a los resultados que se obtienen. (AEC ,2017).

En la Norma ISO 27000: 2014, se encuentra la definición de Seguridad de la información definida como como la preservación de la confidencialidad, integridad y disponibilidad de la información.

La información es el principal activo de muchas organizaciones por lo que es necesario protegerla adecuadamente frente a amenazas que puedan poner en peligro la continuidad del negocio. En la actualidad, la mayor parte de la información reside en equipos informáticos, soportes de almacenamiento y redes de datos, encuadrados dentro de lo que se conoce como sistemas de información. Estos sistemas de información están sujetos a riesgos e inseguridades internos y externos a la organización.

El objetivo de las organizaciones es disminuir los riesgos sin necesidad de realizar fuertes inversiones en software y sin contar con una gran estructura de personal. Para ello es necesario conocer y afrontar los riesgos a los que se somete la información, contemplar procedimientos adecuados y planificar e implantar controles de seguridad. (AEC ,2012).

5.13.1. Sistema de Gestión en Seguridad de la Información.

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (López Neira y Ruiz Spohr, 2012).

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- **Confidencialidad**: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad**: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. •
- **Disponibilidad**: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI. (López Neira y Ruiz Spohr, 2017).

5.13.2. Que Incluye un Sistema de Gestión en Seguridad de la Información

En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles.

Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 de la siguiente forma (López Neira y Ruiz Spohr, 2017).

Imagen N° 21. Documentación del Sistema de Seguridad de La información por niveles piramidales

Fuente. López Neira y Ruiz Spohr (2012) Sistema de Gestión en Seguridad de la información

- Documentos de Nivel 1

Manual de seguridad: Por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI. (López Neira y Ruiz Spohr, 2012).

- Documentos de Nivel 2

Procedimientos: Documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información. (López Neira y Ruiz Spohr, 2012):

- Documentos de Nivel 3

Instrucciones, checklists y formularios: Documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información. (López Neira y Ruiz Spohr, 2012).

- Documentos de Nivel 4

- **Registros**: Documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos. De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio) (López Neira y Ruiz Spohr, 2012):
- **Alcance del SGSI**: ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).
- **Política y objetivos de seguridad**: Documento de contenido genérico que establece el compromiso de la y el enfoque de la organización en la gestión de la seguridad de la información.
- **Procedimientos y mecanismos de control que soportan al SGSI**: Aquellos procedimientos que regulan el propio funcionamiento del SGSI.
- **Enfoque de evaluación de riesgos**: Descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.
- **Informe de evaluación de riesgos**: Estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.
- **Plan de tratamiento de riesgos**: Documento que identifica las acciones los recursos, las responsabilidades y las prioridades para gestionar los riesgos de

seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

- **Procedimientos documentados**: Todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.

  Registros: Documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.
- **Declaración de aplicabilidad**: (SOA -Statement of Applicability-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.
- Control de la documentación para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para López Neira y Ruiz Spohr, 2012):
- Aprobar documentos apropiados antes de su emisión.
- Revisar y actualizar documentos cuando sea necesario y renovar su validez.
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
- Garantizar que los documentos procedentes del exterior están identificados.
- Garantizar que la distribución de documentos está controlada.
- Prevenir la utilización de documentos obsoletos.

- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

5.14. Requisitos de la Norma ISO 27001: 2013

Los requisitos generales se encuentran en el numeral 4 de la norma ISO 27001: 2013 así:

La organización debe establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado, en el contexto de las actividades globales del negocio de la organización y de los riesgos que enfrenta.

5.14.1. Establecimiento y Gestión del SGSI:

Establecimiento del SGSI La organización debe:

- Definir el alcance y límites del SGSI en términos de las características del negocio, la organización, su ubicación, sus activos, tecnología, e incluir los detalles y justificación de cualquier exclusión del alcance.

Definir una política de SGSI en términos de las características del negocio, la organización, su ubicación, sus activos y tecnología, que:

1) Incluya un marco de referencia para fijar objetivos y establezca un sentido general y principios para la acción con relación a la seguridad de la información;

2) Tenga en cuenta los requisitos del negocio, los legales o reglamentarios, y las obligaciones de seguridad contractuales;

3) Esté alineada con el contexto organizacional estratégico de gestión del riesgo en el cual tendrá lugar el establecimiento y mantenimiento del SGSI;

4) Establezca los criterios contra los cuales se evaluará el riesgo[1].

5) Haya sido aprobada por la organización

6) Identificar una metodología de valoración del riesgo que sea adecuada al SGSI y a los requisitos reglamentarios, legales y de seguridad de la información del negocio, identificados.

[1] (Véase el numeral 4.2.1, literal c) y; NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001

7) Desarrollar criterios para la aceptación de riesgos, e identificar los niveles de riesgo aceptables. (Véase el numeral 5.1, literal f). La metodología seleccionada para valoración de riesgos debe asegurar que dichas valoraciones producen resultados comparables y reproducibles.

a. Identificar los riesgos

b. Identificar los activos dentro del alcance del SGSI y los propietarios de estos activos.

c. Identificar las amenazas a estos activos.

d. Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas.

e. Identificar los impactos que la pérdida de confidencialidad, integridad y disponibilidad puede tener sobre estos activos.

f. Analizar y evaluar los riesgos.

8). Valorar el impacto de negocios que podría causar una falla en la seguridad, sobre la organización, teniendo en cuenta las consecuencias de la pérdida de confidencialidad, integridad o disponibilidad de los activos.

9). Valorar la posibilidad realista de que ocurra una falla en la seguridad, considerando las amenazas, las vulnerabilidades, los impactos asociados con estos activos, y los controles implementados actualmente.

10). Estimar los niveles de los riesgos.

11). Determinar la aceptación del riesgo o la necesidad de su tratamiento a partir de los criterios establecidos en el numeral 4.2.1, literal c).

12). Identificar y evaluar las opciones para el tratamiento de los riesgos

Las posibles acciones incluyen:

- El término “propietario” identifica a un individuo o entidad que tiene la responsabilidad, designada por la gerencia, de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos.
- El término “propietario” no quiere decir que la persona realmente tenga algún derecho de propiedad sobre el activo. NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001.

13). Aplicar los controles apropiados.

14). Aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la organización para la aceptación de riesgos (véase el numeral 4.2.1, literal c));

15). Evitar riesgos, y

16) Transferir a otras partes los riesgos asociados con el negocio, por ejemplo: aseguradoras, proveedores, etc.

17) Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.

Los objetivos de control y los controles se deben seleccionar e implementar de manera que cumplan los requisitos identificados en el proceso de valoración y tratamiento de riesgos.

Esta selección debe tener en cuenta los criterios para la aceptación de riesgos (véase el numeral 4.2.1. literal c)), al igual que los requisitos legales, reglamentarios y contractuales.

Los objetivos de control y los controles del Anexo A se deben seleccionar como parte de este proceso, en tanto sean adecuados para cubrir estos requisitos. Los objetivos de control y los controles presentados en el Anexo A no son exhaustivos, por lo que puede ser necesario seleccionar objetivos de control y controles adicionales.

Obtener la aprobación de la sobre los riesgos residuales propuestos.

Obtener autorización de la para implementar y operar el SGSI.

18) Elaborar una declaración de aplicabilidad. Se debe elaborar una declaración de aplicabilidad que incluya:

19) Los objetivos de control y los controles, seleccionados en el numeral 4.2.1, literal g. y las razones para su selección.

20) Los objetivos de control y los controles implementados actualmente (véase el numeral 4.2.1., literal e) 2)), y

21) La exclusión de cualquier objetivo de control y controles enumerados en el Anexo A y la justificación para su exclusión.

22) Implementación y operación del SGSI.

La organización debe:

a) Formular un plan para el tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información (véase el numeral 5);

b) Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que incluye considerar la financiación y la asignación de funciones y responsabilidades;

c) Implementar los controles seleccionados en el numeral 4.2.1, literal g) para cumplir los objetivos de control;

d) Definir cómo medir la eficacia de los controles o grupos de controles seleccionados, y especificar cómo se van a usar estas mediciones con el fin de valorar la eficacia de los controles para producir resultados comparables y reproducibles (véase el numeral 4.2.3 literal c));

e) Implementar programas de formación y de toma de conciencia, (véase el numeral 5.2.2);

f) Gestionar la operación del SGSI; g) gestionar los recursos del SGSI (véase el numeral 5.2);

h) Implementar procedimientos y otros controles para detectar y dar respuesta oportuna a los incidentes de seguridad (véase el numeral 4.2.3)

23) Seguimiento y revisión del SGSI

La organización debe:

a) Ejecutar procedimientos de seguimiento y revisión y otros controles para:

1) Detectar rápidamente errores en los resultados del procesamiento;

2) Identificar con prontitud los incidentes e intentos de violación a la seguridad, tanto los que tuvieron éxito como los que fracasaron;

3) Posibilitar si las actividades de seguridades delegadas a las personas o implementadas mediante tecnología de la información se están ejecutando en la forma esperada;

4) Ayudar a detectar eventos de seguridad, y de esta manera impedir incidentes de seguridad mediante el uso de indicadores, y

5) Determinar si las acciones tomadas para solucionar un problema de violación a la seguridad fueron eficaces.

b) Emprender revisiones regulares de la eficacia del SGSI (que incluyen el cumplimiento de la política y objetivos del SGSI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorias de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.

c) Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.

d) Revisar las valoraciones de los riesgos a intervalos planificados, y revisar el nivel de riesgo residual y riesgo aceptable identificado, teniendo en cuenta los cambios en:

1) La Organización,

2) La Tecnología,

3) Los Objetivos Y Procesos Del Negocio,

4) Las Amenazas Identificadas,

5) La eficacia de los controles implementados, y

6) Eventos externos, tales como cambios en el entorno legal o reglamentario, en las obligaciones contractuales, y en el clima social.

7) Realizar auditorías internas del SGSI a intervalos planificados (véase el numeral 6).

8) Emprender una revisión del SGSI, en forma regular para asegurar que el alcance siga siendo suficiente y que se identifiquen mejoras al proceso de SGSI (véase el numeral 7.1).

9) Actualizar los planes de seguridad para tener en cuenta las conclusiones de las actividades de seguimiento y revisión.

10) Registrar acciones y eventos que podrían tener impacto en la eficacia o el desempeño del SGSI (véase el numeral 4.3.3).

Mantenimiento y mejora del SGSI

La organización debe, regularmente:

a) Implementar las mejoras identificadas en el SGSI;

b) Emprender las acciones correctivas y preventivas adecuadas de acuerdo con los numerales 8.2 y 8.3. Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y las de la propia organización;

c) Comunicar las acciones y mejoras a todas las partes interesadas, con un nivel de detalle apropiado a las circunstancias, y en donde sea pertinente, llegar a acuerdos sobre cómo proceder;

d) Asegurar que las mejoras logran los objetivos previstos.

5.15. Requisitos De Documentación

- Generalidades

La documentación del SGSI debe incluir registros de las decisiones, asegurar que las acciones sean trazables a las decisiones y políticas de la gerencia, y que los resultados registrados sean reproducibles.

Es importante estar en capacidad de demostrar la relación entre los controles seleccionados y los resultados del proceso de valoración y tratamiento de riesgos, y seguidamente, con la política y objetivos del SGSI.

La documentación del SGSI debe incluir:

a) Declaraciones documentadas de la política y objetivos del SGSI (véase el numeral 4.2.1, literal b));
b) El alcance del SGSI (véase el numeral 4.2.1, literal a)) c) los procedimientos y controles que apoyan el SGSI;
c) Una descripción de la metodología de valoración de riesgos (véase el numeral 4.2.1, literal c));

   El informe de valoración de riesgos (véase el numeral 4.2.1, literales c) a g));
d) El plan de tratamiento de riesgos (véase el numeral 4.2.2, literal b));
e) Los procedimientos documentados que necesita la organización para asegurar la eficacia de la planificación, operación y control de sus procesos de seguridad de la información, y para describir cómo medir la eficacia de los controles (véase el numeral 4.2.3, literal c));
f) Los registros exigidos por esta norma (véase el numeral 4.3.3), y
g) La declaración de aplicabilidad. NOTA 1 En esta norma, el término “procedimiento documentado” significa que el procedimiento está establecido, documentado, implementado y mantenido.

NOTA 2: El alcance de la documentación del SGSI puede ser diferente de una organización a otra debido a: - El tamaño de la organización y el tipo de sus actividades, y - El alcance y complejidad de los requisitos de seguridad y del sistema que se está gestionando.

NOTA 3: Los documentos y registros pueden tener cualquier forma o estar en cualquier tipo de medio.

- Control de documentos

Los Documentos Exigidos Por El SGSI Se Deben Proteger Y Controlar. Se Debe Establecer Un Procedimiento Documentado Para Definir Las Acciones De Gestión Necesarias Para:

A) Aprobar los documentos en cuanto a su suficiencia antes de su publicación;

B) Revisar y actualizar los documentos según sea necesario y reprobarlos;

C) Asegurar que los cambios y el estado de actualización de los documentos estén identificados;

D) Asegurar que las versiones más recientes de los documentos pertinentes están disponibles en los puntos de uso;

E) Asegurar que los documentos permanezcan legibles y fácilmente identificables;

F) Asegurar que los documentos estén disponibles para quienes los necesiten, y que se apliquen los procedimientos pertinentes, de acuerdo con su clasificación, para su transferencia, almacenamiento y disposición final.

G) Asegurar que los documentos de origen externo estén identificados;

H) Asegurar que la distribución de documentos esté controlada;

I) Impedir el uso no previsto de los documentos obsoletos, y

J) Aplicar la identificación adecuada a los documentos obsoletos, si se retienen para cualquier propósito.

- Control de registros

Se deben establecer y mantener registros para brindar evidencia de la conformidad con los requisitos y la operación eficaz del SGSI. Los registros deben estar protegidos y controlados.

El SGSI debe tener en cuenta cualquier requisito legal o reglamentario y las obligaciones contractuales pertinentes. Los registros deben permanecer legibles, fácilmente identificables y recuperables. Los controles necesarios para la identificación, almacenamiento, protección, recuperación, tiempo de retención y disposición de registros se deben documentar e implementar. Se deben llevar registros del desempeño del proceso, como se esboza en el numeral 4.2, y de todos los casos de incidentes de seguridad significativos relacionados con el SGSI.

5.16. Norma ISO 27001: 2013

En la página web de Wikipedia encontramos la siguiente definición ISO/IEC 27001 es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

5.16.1. Estructura de la Norma ISO 27001:2013

La versión actual de la norma (NTC-ISO-IEC 27001:2013), se encuentra normalizada por el Instituto Colombiano de Normas y Técnicas y Certificación. Dicha norma es una adopción idéntica (IDT) por traducción de la norma ISO/IEC 27001:2013.

Esta norma se encuentra dividida en dos partes; la primera se compone de 10 puntos entre los cuales se encuentran:

- Objeto y campo de aplicación: Especifica la finalidad de la norma y su uso dentro de una organización.

- Referencias normativas

- **Término y definiciones**: Los términos y definiciones usados se basan en la norma ISO/IEC 27000.

- Contexto de la organización: Se busca determinar las necesidades y expectativas dentro y fuera de la organización que afecten directa o indirectamente al sistema de gestión de la seguridad de la información. Adicional a esto, se debe determinar el alcance.

- **Liderazgo**: Habla sobre la importancia de la alta gerencia y su compromiso con el sistema de gestión, estableciendo políticas, asegurando la integración de los requisitos del sistema de seguridad en los procesos de la organización, así como los recursos necesarios para su implementación y operabilidad.

- Planificación: Se deben valorar, analizar y evaluar los riesgos de seguridad de acuerdo a los criterios de aceptación de riesgos, adicional mente se debe dar un tratamiento a los riesgos de la seguridad de la información. Los objetivos y los planes para logar dichos objetivos también se deben definir en este punto.

- Soporte: Se trata sobre los recursos destinados por la organización, la competencia de personal, la toma de conciencia por parte de las partes interesadas, la importancia sobre la comunicación en la organización. La importancia de la información documentada, también se trata en este punto.

- **Operación**: El cómo se debe planificar y controlar la operación, así como la valoración de los riesgos y su tratamiento.

- **Evaluación de desempeño**: Debido a la importancia del ciclo PHVA (Planificar, Hacer, Verificar, Actuar), se debe realizar un seguimiento, medición, análisis y evaluación del sistema de gestión de la información.

- **Mejora**: Habla sobre el tratamiento de las no conformidades, las acciones correctivas y a mejora continua.

La segunda parte, está conformada por el anexo A, el cual establece los objetivos de control y los controles de referencia.

5.17. Documentos Obligatorios Para el Estándar ISO/IEC 27001:2013.

El siguiente listado son los documentos que se requiere elaborar si se quiere cumplir con la norma ISO 27001: (es importante tener en cuenta que los documentos del anexo A son obligatorios sólo si existen riesgos que impliquen su implantación) Kosutic, D, (2013):

- El alcance del sistema de gestión de seguridad de la información (cláusula 4.3)
- Política de seguridad de la información y objetivos (cláusulas 5.2 y 6.2)
- Metodología de evaluación y tratamiento de riesgos (cláusula 6.1.2)
- Declaración de aplicabilidad (cláusula 6.1.3 d)
- Plan de tratamiento de riesgo (cláusula 6.1.3 e y 6.2)
- Informe sobre evaluación de riesgos (cláusula 8.2)
- Definición de roles y responsabilidades de seguridad (cláusulas A.7.1.2 y A.13.2.4)
- Inventario de activos (cláusula A.8.1.1)
- Uso aceptable de los activos (cláusula A.8.1.3)
- Política de control de acceso (cláusula A.9.1.1)
- Procedimientos de operación para gestión de TI (cláusula A.12.1.1)
- Principios de ingeniería de sistemas seguros (cláusula A.14.2.5)
- Política de seguridad para proveedores (cláusula A.15.1.1)
- Procedimiento para gestión de incidentes (cláusula A.16.1.5)
- Procedimientos de Continuidad de negocio (cláusula A.17.1.2)
- Requerimientos legales, regulatorios y contractuales (cláusula A.18.1.1)

5.17.1. Registros obligatorios Norma ISO 27001:2013

Los registros obligatorios para la Norma ISO 27001: 2013 son:

- Registros de formación, habilidades, experiencia y calificaciones (cláusula 7.2)
- Seguimiento y resultados de medición (cláusula 9.1)
- Programa de auditoria interna (cláusula 9.2)
- Resultados de auditorías internas (cláusula 9.2)
- Resultados de la Revisión por (cláusula 9.3)
- Resultados de acciones correctivas (cláusula 10.1)

- Registros de las actividades de usuario, excepciones y eventos de seguridad (cláusulas A.12.4.1 y A.12.4.3).

5.17.2. Metodología de análisis y valoración de los riesgos

Para la valoración, análisis e identificación de riesgos en los procesos informáticos existen diferentes metodologías que buscan realizar una adecuada identificación y prevención de los riesgos que pueden afectar los sistemas de información de la entidad como:

La ISO 31000 es una norma internacional que ofrece las directrices y principios para gestionar el riesgo de las organizaciones.

Esta norma fue publicada en noviembre del 2009 por la Organización Internacional de Normalización (ISO) en colaboración con IEC, y tiene por objetivo que organizaciones de todos los tipos y tamaños puedan gestionar los riesgos en la empresa de forma efectiva, por lo que recomienda que las organizaciones desarrollen, implanten y mejoren continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

5.17.3. Estructura de la norma ISO 31000

La variedad y complejidad de los riesgos es muy diversa por lo que éste estándar internacional desarrollado por la ISO (International Organization for Standardization), no está pensado para un sistema particular de gestión, más bien es una guía de buenas prácticas para las actividades relacionadas con la gestión de riesgos.

El diseño y la implantación de la gestión de riesgos dependerán de las diversas necesidades de cada organización, de sus objetivos concretos, contexto, estructura, operaciones, procesos actividades, servicios, etc.

5.17.4. Principios para la gestión de riesgos

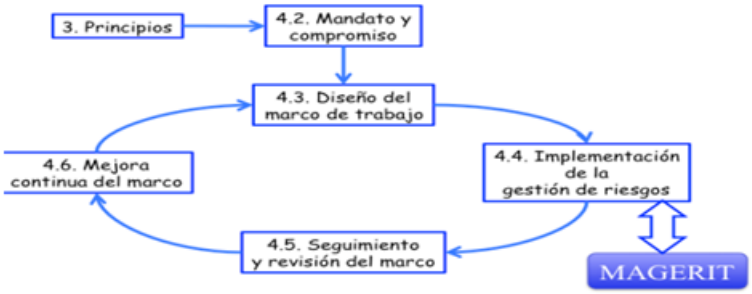
- Crear y proteger el valor. Contribuye a la consecución de objetivos, así como la mejora de ciertos aspectos tales como la seguridad y salud laboral, cumplimiento de los requisitos legales, protección ambiental, etc.

- Estar integrada en los procesos de una organización. No debe ser entendida como una actividad aislada sino como parte de las actividades y procesos principales de una organización.
- Formar parte de la toma de decisiones. La gestión del riesgo ayuda a la toma de decisiones evaluando la información sobre las distintas alternativas.
- Tratar explícitamente la incertidumbre. La gestión del riesgo trata aquellos aspectos de la toma de decisiones que son inciertos, la naturaleza de esa incertidumbre y como puede tratarse.
- Ser sistemática, estructurada y adecuada. Contribuye a la eficiencia y, consecuentemente, a la obtención de resultados fiables.
- Basarse en la mejor información disponible. Los inputs del proceso de gestión del riesgo están basados en fuentes de información como la propia experiencia, la observación y la opinión de expertos.
- Estar hecha a medida. La gestión del riesgo está alineada con el contexto externo e interno de la organización y con su perfil de riesgo.
- Tener en cuenta factores humanos y culturales. Reconoce la capacidad y percepción de los empleados y personas interesadas, esto puede facilitar o dificultar la consecución de los objetivos de la organización.
- Ser transparente e inclusiva. La apropiada y oportuna participación de los grupos de interés (stakeholders) y, en particular, de los responsables a todos los niveles, asegura que la gestión del riesgo permanece relevante y actualizada.
- Ser dinámica, iterativa y sensible al cambio. La organización debe velar para que la gestión del riesgo detecte y responda a los cambios de la empresa y de su entorno.
- Facilitar la mejora continua de la organización. Las organizaciones deberían desarrollar e implementar estrategias para mejorar continuamente, tanto en la gestión del riesgo como en cualquier otro aspecto de la organización

5.17.5. Margerit

La metodología MAGERIT desarrolla el Proceso de Gestión de Riesgos de las tecnologías de la información dentro de la Norma ISO 31000, Sección 4.4 “Implementación de la Gestión de los Riesgos” esta metodología trabaja dentro de un marco para que las entidades de gobierno tomen decisiones teniendo en cuenta los riesgos del uso de tecnologías de la información. (Gobierno de España, 2012).

Imagen N° 22 . Marco de Trabajo para la Gestión del Riesgo ISO 31000



Fuente. Metodología Margerit V3 libro I

Margerit persigue los siguientes objetivos:

Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

- También se ha buscado la uniformidad de los informes que recogen los hallazgos y las conclusiones de las actividades de análisis y gestión de riesgos:
- Modelo de valor: Caracterización del valor que representan los activos para la Organización, así como de las dependencias entre los diferentes activos.
- **Mapa de riesgos**: Relación de las amenazas a que están expuestos los activos.
- **Declaración de aplicabilidad**: Para un conjunto de salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.
- **Evaluación de salvaguardas**: Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.
- **Estado de riesgo**: Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.
- **Informe de insuficiencias**: Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema. Es decir, recoge las vulnerabilidades del sistema, entendidas como puntos débilmente protegidos por los que las amenazas podrían materializarse.
- **Cumplimiento de normativa**: Satisfacción de unos requisitos. Declaración de que se ajusta y es conforme a la normativa correspondiente.
- **Plan de seguridad**: Conjunto de proyectos de seguridad que permiten materializar las decisiones de tratamiento de riesgos.

5.17.6. Metodología OCTAVE

OCTAVE es una técnica de planificación y consultoría estratégica en seguridad basada en el riesgo. (Duque Ochoa, 2010).

El método OCTAVE es un método utilizado para evaluar las necesidades de seguridad de la información de una organización. OCTAVE Allegro es el método más recientemente desarrollado y activamente apoyado. Este método se basa en dos versiones anteriores denominadas OCTAVE Original y OCTAVE-S. (Cert, 2008).

El objetivo de OCTAVE es el riesgo organizacional y el foco son los temas relativos a la estrategia y a la práctica. Cuando se aplica OCTAVE, un pequeño equipo de gente desde los sectores operativos o de negocios hasta los departamentos de tecnología de la información (IT) trabajan juntos dirigidos a las necesidades de seguridad, balanceando tres aspectos: Riesgos Operativos, Prácticas de seguridad Y Tecnología. CERT, (2008).

El método OCTAVE se enfoca en tres fases para examinar los problemas organizacionales y tecnológicos:

- Identificación de la información a nivel gerencial.
- Identificación de la información a nivel operacional.
- Identificación de la información a nivel de usuario final.

Estos tres pasos dan lugar a otros 5 procesos para completar los 8 puntos de los que consta OCTAVE:

- Consolidación de la información y creación de perfiles de amenazas.
- Identificación de componentes claves.
- Evaluación de componentes seleccionados.
- Análisis de riesgos de los recursos críticos.
- Desarrollo de estrategias de protección

5.17.7. Metodología DAFP

El Departamento Administrativo de la Función Pública ha desarrollado la Guía de Administración del riesgo dirigida a las entidades estatales.

Cuando la administración del riesgo se implementa y se mantiene, le permite a la entidad (Dafp, 2011):

- Aumentar la probabilidad de alcanzar los objetivos y proporcionar a la administración un aseguramiento razonable con respecto al logro de los mismos.
- Ser consciente de la necesidad de identificar y tratar los riesgos en todos los niveles de la entidad.

- Involucrar y comprometer a todos los servidores de las entidades de la Administración Pública en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos.
- Cumplir con los requisitos legales y reglamentarios pertinentes.
- Mejorar el Gobierno.
- Proteger los recursos del Estado.
- Establecer una base confiable para la toma de decisiones y la planificación.
- Mejorar la eficacia y eficiencia operativa.
- Mejorar el aprendizaje y la flexibilidad organizacional.

Las entidades de la administración pública deben darle cumplimiento a su misión constitucional y legal, a través de sus objetivos institucionales, los cuales se desarrollan a partir del diseño y ejecución de los diferentes planes, programas y proyectos. (Dafp, 2011).

El cumplimiento de dichos objetivos puede verse afectado por factores tanto internos como externos que crean riesgos frente a todas sus actividades, razón por la cual se hace necesario contar con acciones tendientes a administrarlos. El adecuado manejo de los riesgos favorece el desarrollo y crecimiento de la entidad, con el fin de asegurar dicho manejo es importante que se establezca el entorno y ambiente organizacional de la entidad, la identificación, análisis, valoración y definición de las alternativas de acciones de mitigación de los riesgos, esto en desarrollo de los siguientes elementos:

- Contexto estratégico
- Identificación de riesgos
- Análisis de riesgos
- Valoración de riesgos
- Políticas de administración de riesgos

5.18. Gobierno de Tecnología Informática.

En su definición más básica, el gobierno de TI es el proceso por el cual las decisiones se toman alrededor de inversiones en tecnologías de información. Cómo se toman las decisiones, quién toma las decisiones, quién es responsable y cómo. Los resultados de

las decisiones son medidos y monitoreados son partes del gobierno de TI. (Symons, C, 2005).

Todo el mundo tiene alguna forma de gobierno de TI. Desafortunadamente para muchas empresas, el proceso es ad hoc e informal, no hay coherencia en toda la empresa, la rendición de cuentas es débil - si está presente en absoluto - y no hay mecanismos formales para medir y monitorear los resultados de las decisiones.

Gobierno de TI "es una parte integral de la gobernanza empresarial y consiste en el liderazgo y estructuras organizativas y procesos que aseguren que la TI de la organización sustente y extienda las estrategias y los objetivos de la organización.

Implementar un buen gobierno de TI requiere un marco basado en tres elementos principales:

- Estructura. ¿Quién toma las decisiones? ¿Qué organizaciones estructurales se crearán, quiénes participan en estas organizaciones, y qué responsabilidades asumirán?
- Proceso. ¿Cómo se toman las decisiones de inversión en TI? ¿Cuáles son los procesos de toma de decisiones para proponer inversiones?, ¿Revisar inversiones?, ¿Aprobar y priorizar inversiones?
- Comunicación. ¿Cómo se monitorizarán, medirán los resultados de estos procesos y decisiones, y comunicado? ¿Qué mecanismos se utilizarán para comunicar las decisiones de inversión en TI?

5.18.1. COBIT

La Misión de COBIT: Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento.

Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT, 2005) brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas

de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución.

Estas prácticas ayudarán a optimizar las inversiones habilitadas por TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien. Para que TI tenga éxito en satisfacer los requerimientos del negocio, la debe implementar un sistema de control interno o un marco de trabajo.

El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:

- Estableciendo un vínculo con los requerimientos del negocio
- Organizando las actividades de TI en un modelo de procesos generalmente aceptado
- Identificando los principales recursos de TI a ser utilizados
- Definiendo los objetivos de control gerenciales a ser considerados La orientación al negocio que enfoca COBIT consiste en alinear las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los dueños de los procesos de negocio y de TI.

El enfoque hacia procesos de COBIT se ilustra con un modelo de procesos, el cual subdivide TI en 34 procesos de acuerdo a las áreas de responsabilidad de planear, construir, ejecutar y monitorear, ofreciendo una visión de punta a punta de la TI.

COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados (Stakeholders). COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI.

La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de la misma. Los

beneficios de implementar COBIT como marco de referencia de gobierno sobre TI incluyen:

- Mejor Alineación, Con Base En Su Enfoque De Negocios
- Una Visión, Entendible Para La Gerencia, De Lo Que Hace TI
- Propiedad Y Responsabilidades Claras, Con Base En Su Orientación A Procesos
- Aceptación General De Terceros Y Reguladores
- Entendimiento Compartido Entre Todos Los Interesados, Con Base En Un Lenguaje común
- Cumplimiento de los requerimientos COSO para el ambiente de control de TI El resto de este documento brinda una descripción del marco de trabajo COBIT, así como todos los componentes esenciales organizados por los dominios TI de COBIT y 34 procesos de TI. ISACA. (2007).

5.19. Normatividad Seguridad de la Información

- **Ley 1273 de 2009**. Delitos informáticos. (Congreso de Colombia, 2009): La ley 1273 modifica el Código Penal, creando un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" tratando de preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"
- **Ley Estatutaria 1581 De 2012 Y Decreto Nacional 1377 De 2013:** Principios para el Tratamiento de datos personales. El gobierno de la república de Colombia reglo los principios en materia de tratamiento de datos personales a reglado e Artículo 4° de la Ley Estatutaria 1581 de 2012, la cual fue reglamentada parcialmente por el Decreto Nacional 1377 de 2013. (Congreso de Colombia, 2012-2013).

6. PROBLEMAS IDENTIFICADOS POR NO CONTAR CON LA ESTRATEGIA GOBIERNO EN LÍNEA

La entidad Concejo Distrital de Cartagena al no contar con la Estrategia Gobierno en Línea en los ejes Tic servicios y Tic Seguridad y privacidad de la información, diseñada ni implementada presenta deficiencias en los servicios que ofrece a los ciudadanos además de no proteger la información como su activo más sagrado, entre los problemas identificados tenemos:

- No se ha realizado la caracterización de los usuarios, donde identifique las necesidades de los usuarios con respecto a la información de la entidad. Hasta la fecha el 0% de los usuarios han sido caracterizados.
- el 100% de los trámites deben realizarse en forma manual, la entidad no cuenta con trámites en línea donde los usuarios puedan colocar las quejas, peticiones y reclamos. En el proceso que es manual pueden tardar más de 15 días en contestar una petición, algunas veces la petición, queja o reclamo no llega a la dependencia correcta.
- El 100% de los proyectos debe consultarse dentro de la entidad, la inscripción y la participación en debates debe hacerse directamente en secretaria general.
- No se realiza la evaluación de la satisfacción de los usuarios con respecto a los servicios de la entidad.
- No cuenta con una ventanilla única de trámites para atención al ciudadano.
- No tiene claridad acerca de los riesgos que se presentan al no contar con un diagnóstico ni u con el diseño del sistema de seguridad y privacidad de la información.
- No cuenta con políticas de seguridad de la información
- No cuenta con estrategias de protección de la información de la entidad.
- No posee un plan de riesgos que permita minimizar el impacto de la materialización de estos en la entidad.

7. RESULTADOS ESPERADOS

Se espera definir la Estrategia Gobierno en Línea en el área de tic para servicios y seguridad y privacidad de la información y se desarrollaran las siguientes actividades:

- Realizar el diagnóstico de la situación actual de la Estrategia Gobierno en línea del Concejo Distrital de Cartagena con respecto al eje temático Tic Servicios.
- Identificar las características de los diferentes grupos objetivos del Concejo Distrital de Cartagena
- Definir las directrices de accesibilidad y usabilidad a los trámites y servicios del Concejo Distrital de Cartagena.
- Diseño de estrategias de promoción de los trámites y servicios disponibles por medios electrónicos.
- Definir el procedimiento para realizar la evaluación de la satisfacción del usuario de los servicios y tramites electrónicos
- Realizar el diagnóstico de la situación actual del Eje Temático de la Estrategia Gobierno en línea tic seguridad y privacidad de la Información.
- Definir la política, alcance y objetivos del eje temático seguridad y privacidad de la información para el Concejo Distrital de Cartagena
- Definir los roles y responsabilidades para la seguridad y privacidad de la información.
- Definir el plan de gestión de riesgos para el área de sistemas.
- Definir el proceso de gestión de incidentes de seguridad
- Realización del Diseño de los ejes temáticos de la Estrategia Gobierno en Línea Tic Servicios y Seguridad y Privacidad de la Información para El Concejo Distrital de Cartagena adaptado a sus necesidades.
- Analizar las brechas entre el estado actual y el estado futuro (corto, mediano y largo plazo) definiendo el road map de los proyectos a implementar.

7.1. Plan De Implementación

7.1.1. Contribuciones originales esperadas

Se espera que el presente proyecto contribuya a la entidad Concejo Distrital de Cartagena así:

- Acercarse a la comunidad Cartagenera y colombiana mediante el ofrecimiento de trámites y servicios digitales.
- Capacitación y concientización del personal en una cultura de seguridad de la información
- Cumplir la Misión organizacional y alcanzar la visión.
- Brindar protección a la información y asegurarla en forma adecuada logrando una clara gestión de los procesos de toda la entidad.
- Disminución de costos por pérdida de información.
- Imagen positiva de la entidad frente a las partes interesadas
- Disminución de riesgos por pérdida de información.
- Cumplimiento de los requerimientos de los entes de control.
- Debida protección de los datos e información.

7.1.2. Viabilidad de la investigación

Para determinar la viabilidad de la investigación es necesario tener en cuenta la disponibilidad de recursos financieros, humanos y materiales que determinarán en última instancia los alcances de la investigación (Rojas, 1981).

En la disponibilidad del recurso humano se tendrá en cuenta las personas que participan en el proceso, identificando las actividades que son necesarias para lograr el objetivo propuesto en la investigación, observando si los usuarios del sistema tienen compromiso con el diseño.

En la disponibilidad del recurso financiero se determinará el costo –beneficio de diseñar los ejes temáticos Tic Servicios y Seguridad y Privacidad de la información para el Concejo Distrital de Cartagena.

En la disponibilidad de materiales se observará la tecnología requerida para el rendimiento del proyecto, cual es el riesgo de realizar el diseño y cómo puede afectar el costo del proyecto de investigación.

Al analizar la disponibilidad de recursos financieros, humanos y materiales se determinará la viabilidad del Diseño de los ejes temáticos de los Ejes Temáticos de la Estrategia Gobierno en línea tic servicios y seguridad y privacidad de la Información para El Concejo Distrital de Cartagena de Indias.

7.1.3. Propuesta de Intervención

Tabla N° 10. Plan de Acción para la intervención

ESTRATEGIA	ACTIVIDAD	QUE	COMO	CUANDO	QUIEN
Diseño de los ejes temáticos de la Estrategia Gobierno en Línea Tic servicios y Seguridad y Privacidad de la Información	1. Caracterizar los usuarios de la entidad y Grupos de interés	1.1. Identificar, clasificar y priorizar los grupos de interés involucrados e impactados por los proyectos de TI	1.1.1. Realizar la matriz de caracterización que clasifique y priorice los grupos de interés e impactados por los proyectos TI	Oct/2017	Estudiantes
	1.2. Establecer Directrices de accesibilidad	1.2.1. Establecer los mecanismos que permitan el acceso a los servicios de información por parte de los diferentes grupos de interés, contemplando características de accesibilidad, seguridad y usabilidad.	1.2.1.1. Diseñar una guía que direccione el acceso a los servicios de información por parte de los diferentes grupos de interés, contemplando características de accesibilidad, seguridad y usabilidad.	Oct./2017	Estudiantes
	1.3. Promoción	1.3.1. Diseñar estrategias de promoción de los trámites y servicios disponibles por medios electrónicos	1.3.1.1. Diseña estrategias de promoción de los trámites y servicios disponibles por medios electrónicos, de acuerdo con la caracterización de usuarios	Enero/2017	Estudiantes
	1.4. Evaluación del usuario	1.4.1. Determinar el nivel de avance de la estrategia TIC Servicios	1.4.1.1. Diseño de criterios para la evaluación de los tramites en línea	Febrero/2018	Estudiantes

ESTRATEGIA	ACTIVIDAD	QUE	COMO	CUANDO	QUIEN
	1.5. Sistema Integrado de peticiones quejas y reclamos	1.5.1. Diseñar adecuados canales de comunicación con el ciudadano desde los distintos espacios: Pagina Web, Físico. Donde se le puedan resolver sus inquietudes y peticiones	1.5.1.1. Diseñar un protocolo de Atención Al Ciudadano Y Usuarios De Canales Electrónicos Y Digitales Del Concejo Distrital De Cartagena.	Feb/2017	Estudiantes
Diseño de los ejes temáticos de la Estrategia Gobierno en Línea Tic servicios y Seguridad y Privacidad de la Información	2. Diagnóstico Inicial	Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad	2. Realizar una Lista de chequeo en base a los requisitos de la norma NTC 27001:2013- Modelo de Seguridad y privacidad de la información	Ago.//2017	Estudiantes-Coordinador de Seguridad de la información
	2.1. Diagnóstico del Nivel de Madurez	Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	2.1.2 Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	Oct/2017	Estudiantes-Coordinador de Seguridad de la información
	2.2. Diagnóstico de Vulnerabilidades	Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación	2.2.1 Herramienta de Diagnóstico	Sept/2017	Estudiantes-Coordinador de Seguridad de la información
	3 Mapa de procesos - Identificación de procesos	3.1. Procesos de la organización para la prestación del servicio	3.1.1. Realizar visitas en la zona de estudio con el fin de identificar los procesos para la prestación de servicio	Nov/2017	Estudiantes-Coordinador de Seguridad de la información

ESTRATEGIA	ACTIVIDAD	QUE	COMO	CUANDO	QUIEN
			sensibles a fallas a la seguridad de la información		
	4. Manual de seguridad y privacidad de la información	4.1. Manual de seguridad y privacidad de la información	4.1.1 Realizar el alcance del sistema de gestión, incluyendo los detalles y justificación de cualquier exclusión.	Ene/2018	Estudiantes - Coordinador de seguridad
		4.1.2. Política de Seguridad y Privacidad de la Información	4.1.1.2. Realizar documento con la política de seguridad de la información de acuerdo a la información recolectada y aprobada por el presidente	Ene/2018	Estudiantes - Coordinador de seguridad - Presidente
			4.1.2.1. Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Abril/2018	Coordinador de Seguridad

ESTRATEGIA	ACTIVIDAD	QUE	COMO	CUANDO	QUIEN
	4. Manual de seguridad y privacidad de la información	4.1.3. Roles y responsabilidades de seguridad y privacidad de la información	4.1.3.1. Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces) en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta , deberá designar quien será el encargado de seguridad de la información dentro de la entidad	Abril/2018	Coordinador de seguridad, jefes de área y la Alta
		4.1.4. Inventario de activos de información	4.1.4.1. Documento con la metodología para la identificación, clasificación valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por el alta.	Ene/2018	Coordinador de seguridad
			3.4.1.2. Matriz con la Identificación, valoración y clasificación de activos de información	Ene/2018	Coordinador de seguridad

ESTRATEGIA	ACTIVIDAD	QUE	COMO	CUANDO	QUIEN
			3.4.1.3. Documento con la caracterización de activos de información que contenga datos personales	Ene/2018	Coordinador de seguridad
		4.5. Identificación, valoración y tratamiento de los riesgos	4.5.1. Documento con la metodología de gestión de riesgos	Ene/2018	Coordinador de seguridad
			4.5.2. Documento con el análisis y evaluación de riesgos	Ene/2018	Coordinador de seguridad
Diseño de los ejes temáticos de la Estrategia Gobierno en Línea Tic servicios y Seguridad y Privacidad de la Información	3. Manual de seguridad y privacidad de la información		4..5.3. Documento con el plan de tratamiento de riesgos	ene/2018	Coordinador de seguridad
			4.5.4. Documento con la declaración de aplicabilidad	En/ 2018	Coordinador de seguridad
		4.5. Identificación, valoración y tratamiento de los riesgos	4.5.5. Documentos revisados y aprobados por la alta	May/2018	Coordinador de seguridad
		4.6. Plan de comunicaciones	4.6.1. Documento con el plan de comunicación, sensibilización y capacitación de la entidad	May/2018	Coordinador de seguridad
	5. Implementación del sistema de gestión en	5.1. Implementación	5.1. Cumplimiento de los numerales de la Norma ISO 27001:2013: 5: (Responsabilidad de la, 5.1	May/2018	Coordinador de seguridad, jefes de área y la Alta Dirección

ESTRATEGIA	ACTIVIDAD	QUE	COMO	CUANDO	QUIEN
	seguridad de la información		(Compromiso de la) 7. (Revisión del SGSI por la)		
	6 Auditoria Interna	6.1. Controles de los procesos	6.1. Elaborar programa de auditoria interna	May/2018	Coordinador de seguridad, jefes de área y la Alta Dirección
			6.2. elaborar el procedimiento de auditoria interna	May/2018	Coordinador de seguridad, jefes de área y la Alta Dirección
			6.3. Evaluar el cumplimiento de los requisitos del Modelo de seguridad de la información	May/2018	Coordinador de seguridad, jefes de área y la Alta Dirección
	7. Acciones correctivas	7.1. No conformidades	7.1. Desviación de los procesos	May/2018	Coordinador de seguridad, jefes de área
			7.2. Identificación de las no conformidades de acuerdo al cumplimiento de los requisitos	May/2018	Coordinador de seguridad, jefes de área

Fuente. Los autores de acuerdo a Tic servicios y Modelo de seguridad y privacidad de la información Mintic. (2016).

7.1.4. Índice tentativo

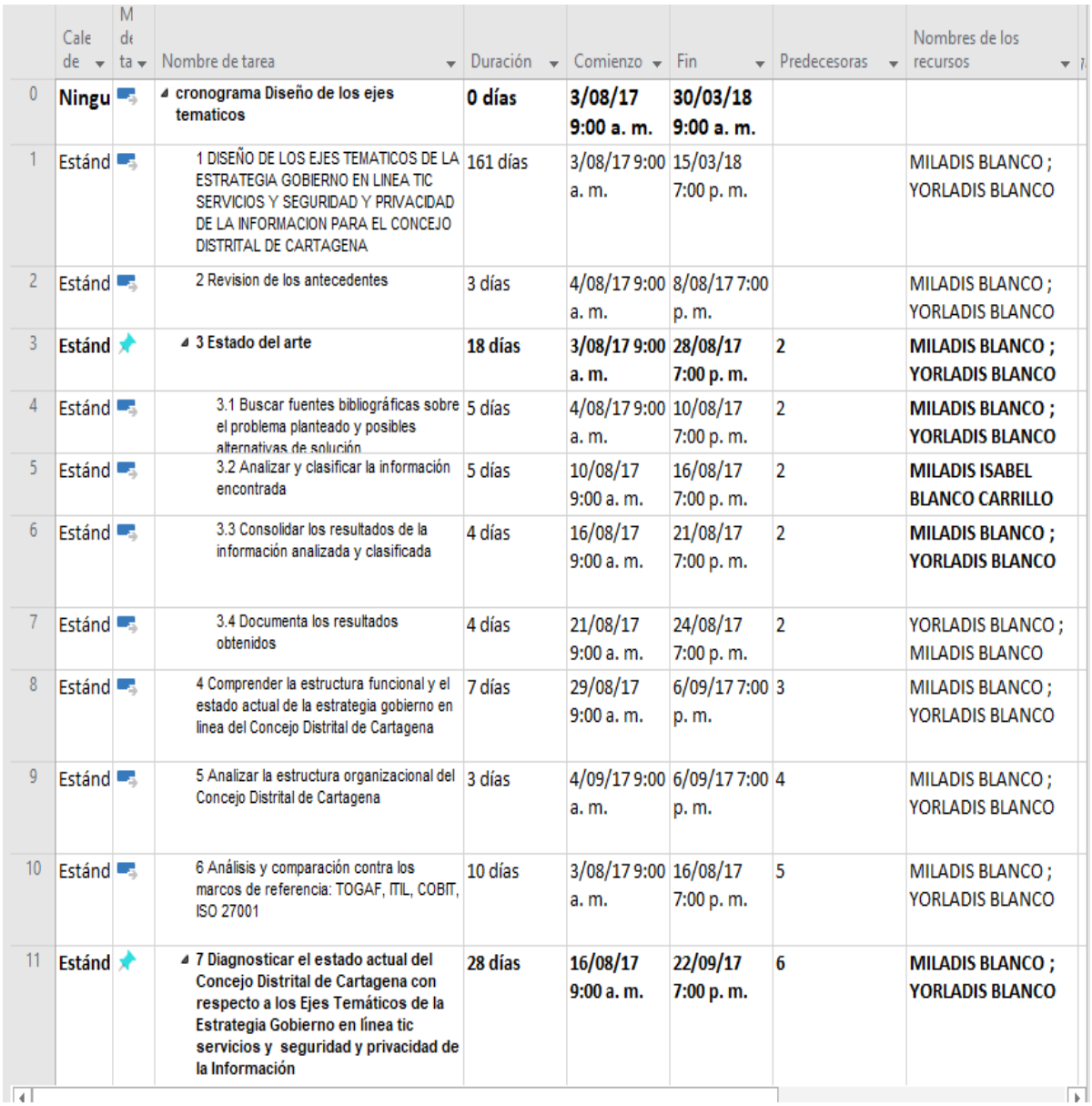
- INTRODUCCIÓN
- PROBLEMA DE INVESTIGACIÓN
- DISEÑO GENERAL
- FUENTES DE INFORMACIÓN ESBOZO MARCO TEÓRICO
- MARCO TEÓRICO
- RESULTADOS ESPERADOS
- PLAN DE IMPLEMENTACIÓN
- ESTRUCTURA FUNCIONAL DEL CONCEJO DISTRITAL DE CARTAGENA
- DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DEL CONCEJO DISTRITAL DE CARTAGENA FRENTE A LA ESTRATEGIA GOBIERNO EN LÍNEA
- DISEÑO DEL EJE TEMÁTICO DE LA ESTRATEGIA GOBIERNO EN LÍNEA TIC SERVICIOS
- ESTADO ACTUAL- DIAGNÓSTICO
- ESTADO FUTURO
- RESULTADOS
- PLAN DE ACCIÓN
- DISEÑO DEL EJE TEMÁTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA EL CONCEJO DISTRITAL DE CARTAGENA
- ESTADO ACTUAL – DIAGNÓSTICO
- ESTADO FUTURO
- RESULTADOS Y ANÁLISIS
- PLAN DE ACCIÓN
- CONCLUSIONES
- RECOMENDACIONES
- BIBLIOGRAFÍA
- ANEXOS

7.2. Cronograma de desarrollo del trabajo de grado

Fecha de Inicio: Julio de 2017

Fecha final: marzo 2018

Imagen N° 23. Cronograma de actividades planeado



	Cale de	M de ta	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
0	**Ningu**		**cronograma Diseño de los ejes tematicos**	**0 días**	**3/08/17 9:00 a. m.**	**30/03/18 9:00 a. m.**		
1	Estánd		1 DISEÑO DE LOS EJES TEMATICOS DE LA ESTRATEGIA GOBIERNO EN LINEA TIC SERVICIOS Y SEGURIDAD Y PRIVACIDAD DE LA INFORMACION PARA EL CONCEJO DISTRITAL DE CARTAGENA	161 días	3/08/17 9:00 a. m.	15/03/18 7:00 p. m.		MILADIS BLANCO ; YORLADIS BLANCO
2	Estánd		2 Revision de los antecedentes	3 días	4/08/17 9:00 a. m.	8/08/17 7:00 p. m.		MILADIS BLANCO ; YORLADIS BLANCO
3	**Estánd**		**3 Estado del arte**	**18 días**	**3/08/17 9:00 a. m.**	**28/08/17 7:00 p. m.**	**2**	**MILADIS BLANCO ; YORLADIS BLANCO**
4	Estánd		3.1 Buscar fuentes bibliográficas sobre el problema planteado y posibles alternativas de solución	5 días	4/08/17 9:00 a. m.	10/08/17 7:00 p. m.	2	**MILADIS BLANCO ; YORLADIS BLANCO**
5	Estánd		3.2 Analizar y clasificar la información encontrada	5 días	10/08/17 9:00 a. m.	16/08/17 7:00 p. m.	2	**MILADIS ISABEL BLANCO CARRILLO**
6	Estánd		3.3 Consolidar los resultados de la información analizada y clasificada	4 días	16/08/17 9:00 a. m.	21/08/17 7:00 p. m.	2	**MILADIS BLANCO ; YORLADIS BLANCO**
7	Estánd		3.4 Documenta los resultados obtenidos	4 días	21/08/17 9:00 a. m.	24/08/17 7:00 p. m.	2	YORLADIS BLANCO ; MILADIS BLANCO
8	Estánd		4 Comprender la estructura funcional y el estado actual de la estrategia gobierno en linea del Concejo Distrital de Cartagena	7 días	29/08/17 9:00 a. m.	6/09/17 7:00 p. m.	3	MILADIS BLANCO ; YORLADIS BLANCO
9	Estánd		5 Analizar la estructura organizacional del Concejo Distrital de Cartagena	3 días	4/09/17 9:00 a. m.	6/09/17 7:00 p. m.	4	MILADIS BLANCO ; YORLADIS BLANCO
10	Estánd		6 Análisis y comparación contra los marcos de referencia: TOGAF, ITIL, COBIT, ISO 27001	10 días	3/08/17 9:00 a. m.	16/08/17 7:00 p. m.	5	MILADIS BLANCO ; YORLADIS BLANCO
11	**Estánd**		**7 Diagnosticar el estado actual del Concejo Distrital de Cartagena con respecto a los Ejes Temáticos de la Estrategia Gobierno en línea tic servicios y seguridad y privacidad de la Información**	**28 días**	**16/08/17 9:00 a. m.**	**22/09/17 7:00 p. m.**	**6**	**MILADIS BLANCO ; YORLADIS BLANCO**

24	Estánd	**12 Eje Tematico seguridad y privacidad de la informacion**	**50 días**	**24/11/17 9:00 a. m.**	**1/02/18 7:00 p. m.**		**MILADIS BLANCO ; YORLADIS BLANCO**
25	Estánd	12.1 aplicar lista de chequeo	4 días	1/12/17 9:00 a. m.	6/12/17 7:00 p. m.	12	MILADIS BLANCO ; YORLADIS BLANCO
26	Estánd	12.2 Verificar el nivel de cumplimiento de la entidad frente a los requisitos del Modelo de Seguridad y Privacidad de la información de la estrategia Gel definiendo las acciones a seguir para su cumplimiento dentro de la entidad	5 días	1/12/17 9:00 a. m.	7/12/17 7:00 p. m.	12	MILADIS BLANCO ; YORLADIS BLANCO
27	Estánd	12.3 Realizar la asignación de los roles y responsabilidades en la estructura organizacional en cuanto a seguridad y privacidad de la información.	9 días	1/12/17 9:00 a. m.	13/12/17 7:00 p. m.	12	MILADIS BLANCO ; YORLADIS BLANCO
28	Estánd	12.4 Definir las políticas de la Seguridad de la Información de la entidad tomando como base Modelo de Seguridad y Privacidad de la información de la estrategia Gel	10 días	27/10/17 9:00 a. m.	9/11/17 7:00 p. m.	12	MILADIS BLANCO ; YORLADIS BLANCO
29	Están	12.5 Definir el alcance y los objetivos del Modelo de Seguridad y Privacidad de la información de la estrategia Gel para el Concejo Distrital de Cartagena	8 días	9/11/17 9:00 a. m.	20/11/17 7:00 p. m.	12	MILADIS BLANCO ; YORLADIS BLANCO
30	Estánd	12.6 Realizar la clasificación de los activos de información del proceso de Dirección Financiera y Dirección Administrativa	10 días	1/12/17 9:00 a. m.	14/12/17 7:00 p. m.	12	MILADIS BLANCO ; YORLADIS BLANCO
31	Estánd	12.7 Valorar los riesgos de seguridad que permita definir planes de tratamiento de riesgos de acuerdo a la metodología señalada.	9 días	4/12/17 9:00 a. m.	14/12/17 7:00 p. m.	12	MILADIS BLANCO ; YORLADIS BLANCO
32	Estánd	12.8 Manual de seguridad y privacidad de la informacion Concejo Distrital de Cartagena	2 días	14/12/17 9:00 a. m.	15/12/17 7:00 p. m.	12	MILADIS BLANCO ; YORLADIS BLANCO
33	Estánd	13 revision final segundo entregable	7 días	15/12/17 9:00 a. m.	25/12/17 7:00 p. m.	12	MILADIS BLANCO ; YORLADIS BLANCO
34	Estánd	14 realizar ajustes del entregable	5 días	25/12/17 9:00 a. m.	29/12/17 7:00 p. m.	13	MILADIS BLANCO ; YORLADIS BLANCO
35	Estánd	15 realizar segunda entrega	0 días	30/12/17 9:00 a. m.	30/12/17 9:00 a. m.	14	MILADIS BLANCO ; YORLADIS BLANCO
36	Estánd	16 Documento aprobado	4 días	17/01/18 9:00 a. m.	22/01/18 7:00 p. m.		MILADIS BLANCO ; YORLADIS BLANCO
37	Estánd	17 Elaborar y presentar el Plan de Acción para la implementacion de la Estrategia Gobierno en Linea Tic Servicios y Seguridad y Privacidad de la Informacion para el Concejo Distrital de Cartagena	23 días	22/01/18 9:00 a. m.	21/02/18 7:00 p. m.		MILADIS BLANCO ; YORLADIS BLANCO
38	Estánd	18 Cierre	6 días	21/02/18 9:00 a. m.	28/02/18 7:00 p. m.	17	MILADIS BLANCO ; YORLADIS BLANCO
39	Estánd	19 Documento final	6 días	28/02/18 9:00 a. m.	7/03/18 7:00 p. m.		MILADIS BLANCO ; YORLADIS BLANCO
40	Estánd	20 Revision al documento final	6 días	19/03/18 9:00 a. m.	26/03/18 7:00 p. m.		MILADIS BLANCO ; YORLADIS BLANCO
41	Estánd	21 Entrega del documento final	0 días	30/03/18 9:00 a. m.	30/03/18 9:00 a. m.		MILADIS BLANCO ; YORLADIS BLANCO

Fuente. Los autores

7.3. Cronograma ejecutado

Imagen N° 24. Cronograma Ejecutado

	Cal de	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Prede	Nombres de los recursos
0	**Ningu**		**cronograma Diseño de los ejes tematicos**	**0 días**	**3/08/17 9:00 a. m.**	**30/03/18 9:00 a. m.**		
1	Están		1 DISEÑO DE LOS EJES TEMATICOS DE LA ESTRATEGIA GOBIERNO EN LINEA TIC SERVICIOS Y SEGURIDAD Y PRIVACIDAD DE LA INFORMACION PARA EL CONCEJO DISTRITAL DE CARTAGENA	161 días	3/08/17 9:00 a. m.	15/03/18 7:00 p. m.		MILADIS BLANCO[50%] YORLADIS BLANCO [50%]
2	**Ningu**		**2 Revision de los antecedentes**	**3 días**	**4/08/17 9:00 a. m.**	**8/08/17 7:00 p. m.**		**MILADIS BLANCO; YORLADIS BLANCO**
3	**Están**		**2.1 Estado del arte**	**18 días**	**3/08/17 9:00 a. m.**	**28/08/17 7:00 p. m.**		**MILADIS BLANCO; YORLADIS BLANCO**
4	Están		2.1.1 Buscar fuentes bibliográficas sobre el problema planteado y posibles alternativas de solución	5 días	4/08/17 9:00 a. m.	10/08/17 7:00 p. m.		**MILADIS BLANCO; YORLADIS BLANCO**
5	Están		2.1.2 Analizar y clasificar la información encontrada	5 días	10/08/17 9:00 a. m.	16/08/17 7:00 p. m.		**MILADIS ISABEL BLANCO CARRILLO**
6	Están		2.1.3 Consolidar los resultados de la información analizada y clasificada	4 días	16/08/17 9:00 a. m.	21/08/17 7:00 p. m.		**MILADIS BLANCO; YORLADIS BLANCO**
7	Están		2.1.4 Documenta los resultados obtenidos	4 días	21/08/17 9:00 a. m.	24/08/17 7:00 p. m.		MILADIS BLANCO; YORLADIS BLANCO
8	Están		3 Comprender la estructura funcional y el estado actual de la estrategia gobierno en linea del Concejo Distrital de Cartagena	7 días	29/08/17 9:00 a. m.	6/09/17 7:00 p. m.	3	MILADIS BLANCO; YORLADIS BLANCO
9	Están		4 Analizar la estructura organizacional del Concejo Distrital de Cartagena	3 días	4/09/17 9:00 a. m.	6/09/17 7:00 p. m.	4	MILADIS BLANCO; YORLADIS BLANCO
10	Ningu		5 Análisis y comparación contra los marcos de referencia: TOGAF, ITIL, COBIT, ISO 27001	10 días	3/08/17 9:00 a. m.	16/08/17 7:00 p. m.	5	MILADIS BLANCO; YORLADIS BLANCO
11	**Están**		**6 Diagnosticar el estado actual del Concejo Distrital de Cartagena con respecto a los Ejes Temáticos de la Estrategia Gobierno en línea tic servicios y seguridad y privacidad de la Información**	**28 días**	**16/08/17 9:00 a. m.**	**22/09/17 7:00 p. m.**	**6**	**MILADIS BLANCO; YORLADIS BLANCO**
12	Están		6.1 Realizar las encuestas, entrevistas y fichas tecnicas para el diagnostico	5 días	16/08/17 9:00 a. m.	22/08/17 7:00 p. m.	6	MILADIS BLANCO; YORLADIS BLANCO
13	Están		6.2 tabular las encuestas para definir el diagnostico	9 días	22/08/17 9:00 a. m.	1/09/17 7:00 p. m.	6	MILADIS ISABEL BLANCO CARRILLO
14	Están		6.3 documento diagnostico	13 días	1/09/17 9:00 a. m.	19/09/17 7:00 p. m.	6	MILADIS BLANCO; YORLADIS BLANCO
15	Están		7 revision final del entregable	3 días	18/09/17 9:00 a. m.	20/09/17 7:00 p. m.	7	MILADIS BLANCO; YORLADIS BLANCO
16	Están		8 realizar ajustes del entregable, conclusiones y recomendaciones	6 días	22/09/17 9:00 a. m.	29/09/17 7:00 p. m.	7	MILADIS BLANCO; YORLADIS BLANCO
17	Están		9 realizar primera entrega	0 días	30/09/17 9:00 a. m.	30/09/17 9:00 a. m.	7	MILADIS ISABEL BLANCO CARRILLO
18	**Están**		**10 Definir las estrategias para el Diseño del eje tematico Tic Servicios**	**15 días**	**2/10/17 9:00 a. m.**	**20/10/17 7:00 p. m.**	**10**	**MILADIS BLANCO; YORLADIS BLANCO**
19	Están		10.1 Identificar las características de los diferentes grupos objetivos del Concejo Distrital de Cartagena	5 días	20/10/17 9:00 a. m.	26/10/17 7:00 p. m.	11	MILADIS BLANCO; YORLADIS BLANCO

20	Están	10.2 Incorporar a los trámites y servicios electrónicos directrices de accesibilidad y usabilidad	6 días	26/10/17 9:00 a. m.	2/11/17 7:00 p. m.	11	MILADIS BLANCO; YORLADIS BLANCO
21	Están	10.3 Diseñar estrategias de promoción de los trámites y servicios disponibles por medios electrónicos.	7 días	2/11/17 9:00 a. m.	10/11/17 7:00 p. m.	11	MILADIS BLANCO; YORLADIS BLANCO
22	Están	10.4 Establecer criterios para la evaluación de la satisfacción del usuario de los servicios y tramites electrónicos	6 días	10/11/17 9:00 a. m.	17/11/17 7:00 p. m.	11	MILADIS BLANCO; YORLADIS BLANCO
23	Están	10.5 Definir las pautas para la elaboración de protocolos de atención en los diferentes canales por los cuales presente servicios a los ciudadanos clientes.	7 días	25/09/17 9:00 a. m.	9/01/18 7:00 p. m.	11	YORLADIS BLANCO ; MILADIS BLANCO
24	**Están**	**11 Eje Tematico seguridad y privacidad de la informacion**	**50 días**	**24/11/17 9:00 a. m.**	**1/02/18 7:00 p. m.**		**MILADIS BLANCO[50%]**
25	Están	11.1 aplicar lista de chequeo	4 días	1/12/17 9:00 a. m.	6/12/17 7:00 p. m.	12	MILADIS BLANCO; YORLADIS BLANCO
26	Están	11.2 Verificar el nivel de cumplimiento de la entidad frente a los requisitos del Modelo de Seguridad y Privacidad de la información de la estrategia Gel definiendo las acciones a seguir para su cumplimiento dentro de la entidad	5 días	1/12/17 9:00 a. m.	7/12/17 7:00 p. m.	12	MILADIS BLANCO; YORLADIS BLANCO
27	Están	11.3 Realizar la asignación de los roles y responsabilidades en la estructura organizacional en cuanto a seguridad y privacidad de la información	9 días	1/12/17 9:00 a. m.	13/12/17 7:00 p. m.	12	MILADIS BLANCO; YORLADIS BLANCO
28	Están	11.4 Definir las políticas de la Seguridad de la Información de la entidad tomando como base Modelo de Seguridad y Privacidad de la información de la estrategia Gel	10 días	27/10/17 9:00 a. m.	9/11/17 7:00 p. m.	12	MILADIS BLANCO; YORLADIS BLANCO
29	Están	11.5 Definir el alcance y los objetivos del Modelo de Seguridad y Privacidad de la información de la estrategia Gel para el Concejo Distrital de Cartagena	8 días	9/11/17 9:00 a. m.	20/11/17 7:00 p. m.	12	MILADIS BLANCO; YORLADIS BLANCO
30	Están	11.6 Realizar la clasificación de los activos de información del proceso de Dirección Financiera y Dirección Administrativa	10 días	1/12/17 9:00 a. m.	14/12/17 7:00 p. m.	12	MILADIS BLANCO; YORLADIS BLANCO
31	Están	11.7 Valorar los riesgos de seguridad que permita definir planes de tratamiento de riesgos de acuerdo a la metodología señalada	9 días	4/12/17 9:00 a. m.	14/12/17 7:00 p. m.	12	MILADIS BLANCO; YORLADIS BLANCO
32	Están	11.8 documento Manual de politicas de seguridad de la informacion	2 días	14/12/17 9:00 a. m.	15/12/17 7:00 p. m.	12	MILADIS BLANCO; YORLADIS BLANCO
33	Están	12 revision final segundo entregable	7 días	15/12/17 9:00 a. m.	25/12/17 7:00 p. m.	12	MILADIS BLANCO; YORLADIS BLANCO
34	Están	13 realizar ajustes del entregable	5 días	25/12/17 9:00 a. m.	29/12/17 7:00 p. m.	13	MILADIS BLANCO; YORLADIS BLANCO
35	Están	14 realizar segunda entrega	0 días	30/12/17 9:00 a. m.	30/12/17 9:00 a. m.	14	MILADIS BLANCO; YORLADIS BLANCO
36	Están	15 Documento aprobado	4 días	17/01/18 9:00 a. m.	22/01/18 7:00 p. m.		MILADIS BLANCO; YORLADIS BLANCO
37	Están	16 Elaborar y presentar el Plan de Acción para la implementacion de la Estrategia Gobierno en Linea Tic Servicios y Seguridad y Privacidad de la Informacion para el Concejo Distrital de Cartagena	23 días	22/01/18 9:00 a. m.	21/02/18 7:00 p. m.		MILADIS BLANCO; YORLADIS BLANCO
38	Están	17 Cierre	6 días	21/02/18 9:00 a. m.	28/02/18 7:00 p. m.	17	MILADIS BLANCO; YORLADIS BLANCO
39	Están	18 Documento final	6 días	28/02/18 9:00 a. m.	7/03/18 7:00 p. m.		MILADIS BLANCO; YORLADIS BLANCO
40	Están	19 Revision al documento final	6 días	19/03/18 9:00 a. m.	26/03/18 7:00 p. m.		MILADIS BLANCO; YORLADIS BLANCO
41	Están	20 Entrega del documento final	0 días	30/03/18 9:00 a. m.	30/03/18 9:00 a. m.		MILADIS BLANCO; YORLADIS BLANCO

Fuente. Los autores

Las diferencias existentes entre el cronograma planeado y el cronograma ejecutado radican en que la construcción y análisis de algunos documentos conllevo más tiempo

del esperado debido a los ajustes del director del proyecto para la mejora del trabajo de grado.

7.4. Diagrama de Gantt

Ver. Anexo 1

7.5. Presupuesto

Imagen N° 25. Presupuesto para el desarrollo del proyecto.

ITEM		DESCRIPCIÓN	VALOR EN PESOS (COP) ACTIVIDAD DEL PROYECTO			
			Recoleccion de Informacion	Iso 27001	Documentación Final	TOTAL
MATERIAL TEXTUAL	Libros	Dcumentos escificos en la bibliografia que no se encuentran en forma gratuita	50.000			50.000
	Impresiones y Fotocopias	Impresiones y Fotocopias	40.000	15.000		55.000
SERVICIOS	Internet	Consumo normal de servicio de internet según el cobro del proveedor el servicio ISP	350.000		140.000	490.000
HADWARE	Computadores	Equipos personales de los ejecutores del proyecto	-			-
	Impresoras	Obtencion de algunos documentos en formato fisico	50.000		291.000	341.000
	Almacenamiento Masivo para almacenar Información como copia de seguridad o transporte	Tecnologias para almacenar informacion como copia de seguridad o transporte	10.000	-	-	10.000
SOFTWARE	Software	Se hará uso preferencial de software gratis y aplicativos web	-			
	Gannt Project		-			
PERSONAL	Honorarios de los ejecutores del proyecto	Al ser un proyecto academico se ofrecio al Concejo Distrital de Cartagena y no se solicitaron honorarios	-	-		-
IMPREVISTOS		3% del total para imprevistos y gastos ocasionales				-
TOTAL DE RUBROS Y/O ACTIVIDADES DEL PROYECTO			500.000	15.000	431.000	946.000

* Los valores son aproximados y seran asumidos en su totalidad por los autores del proyecto.

Fuente. Los autores

8. COMPRENDER LA ESTRUCTURA FUNCIONAL Y EL ESTADO ACTUAL DE LA ESTRATEGIA GOBIERNO EN LÍNEA DEL CONCEJO DISTRITAL DE CARTAGENA

8.1. Analizar la Estructura Organizacional del Concejo Distrital de Cartagena.

8.1.1. Reseña Histórica de los Concejos

Los Concejos Municipales de Colombia tienen sus antecedentes históricos en los Cabildos de España, a raíz de la política de población que emprendieron los reyes católicos cuando Cristóbal Colón empezaba su segundo viaje hacia América. El propósito de la Corona era el de estimular e institucionalizar una especie de autoridad local con el fin de apoyarse en ella en la lucha contra la invasión musulmana y la colonización de los territorios conquistados al Islam. De esta forma se llegó a consolidar un código colonial de población que contenía instrucciones para los descubridores, conquistadores y misioneros, sobre el modo para fundar y organizar pueblos.

Según el autor Augusto Hernández Becerra, en su libro las Instituciones Municipales en Colombia, en la época Colonial “el viejo régimen municipal castellano decaía ya en España cuando se trasplantó al Nuevo Mundo, pero aquí creció con personalidad propia y vigor sorprendente. El órgano básico de administración municipal para la época fue el Cabildo y entre sus miembros principales se encontraban el alférez real, los alcaldes, generalmente en número de dos; el alguacil mayor y los regidores, cuyo número oscilaba según la importancia de la población entre 6 y 12, siendo a veces sólo 4 y en ocasiones hasta 24.

Esta especie de cuerpo colegiado tenía la función de administrar un determinado territorio en todos los aspectos propios de la vida social. Sus sesiones podían ser “cerradas” cuando solo se reunían los miembros del Cabildo y “abiertas” cuando además de los miembros concurrían vecinos y ciudadanos a debatir asuntos de interés general.

En 1810, época de la República, los Cabildos de la Nueva Granada, quienes habían emprendido el proceso de emancipación, se independizaron de España a raíz de las reformas implementadas por Carlos III, quienes, según el autor Luis Villar Borda, en su libro Democracia Municipal, consideraron menguada la autonomía de los Cabildos. Autores como Enrique Tamayo Borrero, sostienen que las reformas de Carlos III

promovieron la apertura democrática para la designación de los miembros del Cabildo, la creación del cargo de personero y la fiscalización de la hacienda municipal.

Lo cierto es que, sin lugar a dudas, la amenaza que sintieron los oligarcas y aristócratas miembros del Cabildo, de perder el poder y la dominación que tenían sobre el pueblo y los recursos, fue razón que dio impulso al proceso de independencia, no por ser inconvenientes las reformas de Carlos III, sino por ir en contra de los intereses personales de los Cabildantes de la época.

Con la Constitución Federalista de 1853 se fortaleció el poder y la autonomía de las provincias al punto de que empezaron a promulgar sus propias constituciones, determinando su organización y administración, sin embargo, fracasó en su propósito por integrar dos formas de Estado completamente opuestos, como es el Centralismo y el Federalismo, por lo que ha su corta duración vino un proceso de organización territorial hasta 1863, año en que se promulgó la Constitución de Rionegro.

El periodo Federalista imperó desde 1843 hasta 1886, año en que se expidió la Constitución Centralista de 1886 como respuesta a lo que se consideró el colapso del Federalismo por los constantes levantamientos contra el Gobierno Central por considerar que estaban violando el principio de la no injerencia, al tratar de inmiscuirse en los asuntos locales.

La Constitución Unitaria y Centralista de 1886 se redactó con fundamento en la tesis del presidente Rafael Núñez quien consideraba que la mejor forma de Estado es el Centralismo Político y la Descentralización Administrativa. El Dr. Augusto Hernández resume las consecuencias de la Constitución de 1886 en las provincias y municipios así:" Los Estados soberanos perdieron sus atributos políticos y su patrimonio público. Las autoridades del poder ejecutivo departamental y municipal serán en adelante nombradas por el gobierno nacional y solo tendrán competencias administrativas reglamentadas por la ley. La capacidad impositiva pasó a ser monopolio del Congreso, que con el tiempo transferirá a las asambleas departamentales y concejos municipales la administración de algunos impuestos para la subsistencia seccional y local."

Es preciso recordar que con la Constitución de 1886 se crearon como tal los concejos municipales y se abrió la posibilidad de que los cabildantes fueran elegidos popularmente

(Acto legislativo 02 de 1908), pero con facultades muy limitadas como la de votar los tributos conforme a la Ley. Disponía el artículo 198 de esta Carta Política que “en cada Distrito municipal habrá una Corporación popular que se designará con el nombre de Consejo municipal.” siendo la primera vez que en la historia Institucional de Colombia se usó la expresión “consejo municipal” pero escrita con “s”.

En el año de 1945, finalizando el segundo gobierno del presidente Alfonso López Pumarejo, se llevó a cabo una reforma que revisó la organización del Estado y modificó el régimen departamental y municipal, en cuanto a la creación de Departamentos, la clasificación de los municipios, la validez y presunción de legalidad de los acuerdos municipales.

Para finalizar con los antecedentes de los Concejos Municipales en este periodo, citaremos al autor Wilson Herrera Llanos y su artículo Régimen Municipal en Colombia, quien resume el proceso de fortalecimiento de los municipios a partir de 1984 así: “debemos reseñar el proceso de fortalecimiento municipal, iniciado con las leyes 14 de 1983, 50 de 1984 y la 55 de 1985, que trataron, respectivamente, sobre fortalecimiento de los fiscos municipales, funcionamiento del presupuesto público y ordenamiento de las finanzas del Estado, proceso que vino a culminar con la expedición del acto legislativo N° 01 de enero 9 de 1986, relativo a la elección popular de alcaldes y consultas populares, ampliamente desarrollado por las leyes 11 de 1986, sobre estatuto básico de la administración municipal, desarrollado por el decreto 1333 de 1986; la ley 12 de ese mismo año, sobre Cesión del Impuesto del Valor Agregado (IVA); la ley 78 de 1986, sobre desarrollo de la elección popular de alcaldes, debidamente complementada por la 49 de 1987 y, finalmente, las leyes 77, 78, 80 y 81 de 1987, que desarrollaron el estatuto de la descentralización según el traslado de los diversos servicios públicos, inspección y vigilancia de la urbanización y construcción, el transporte urbano municipal y funciones especiales conjuntas del Instituto de Bienestar Familiar y los municipios.”

Con las reformas anteriores se pretendió consolidar el principio de la descentralización territorial y la participación de todos los ciudadanos en la conformación del poder político, dando paso al proceso de reforma constitucional que culminó con la expedición de la Constitución Política de 1991, que, aunque mantuvo una estructura unitaria para el

Estado, proclamó al municipio como entidad fundamental de la organización territorial y le traslado mayores funciones y competencias.

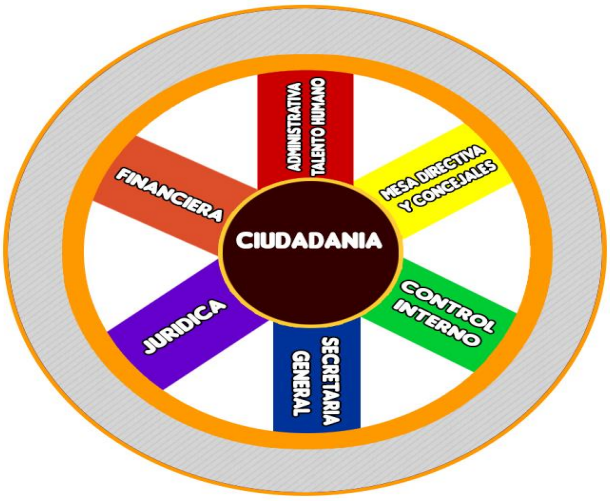
“Es indiscutible que la Constitución de 1991 realizó fundamentales cambios que responden a una concepción más democrática y descentralizada, orientada al perfeccionamiento de la autonomía de las entidades territoriales, a fin de lograr una mayor eficiencia en el funcionamiento del Estado. Sin embargo, el esfuerzo que realizó la constituyente de 1991 por fortalecer la descentralización territorial no fue suficiente, la Constitución de 1991 no reformó al municipio, solo ratificó las transformaciones de la década que le antecedió, dando paso a una relativa descentralización y a una autonomía que ha tenido que irse aclarando y ratificando por la Corte Constitucional, a raíz de las múltiples interpretaciones que se da a las Leyes que desarrollan este principio constitucional.

Se destaca el incremento de las atribuciones dadas a los Concejos Municipales tanto en la Constitución de 1991 como en las reformas que han incrementado y fortalecido el papel de los Concejos Municipales, definiéndolos como una Corporación Político-Administrativa, y encargándole el ejercicio del Control Político sobre la administración municipal. (Fenacon, 2017)

8.2. Concejo Distrital de Cartagena

El Concejo Distrital de Cartagena, es una Corporación Administrativa de elección Popular, creada conforme a lo establecido en la Constitución y la Ley, reglado por la norma (artículo 312 de la Constitución Política, artículo 21 de la Ley 136 de 1994), ubicado en la Calle 24 (Calle del Arsenal) # 10-08 Edificio Galeras de la Marina. -Barrió Getsemaní jurisdicción del distrito de Cartagena de indias D.T. Y C, Bolívar. Su arquitectura organizacional al igual que todos sus procesos tienen como prioridad los ciudadanos. Todas las dependencias trabajan colaborativamente buscando acciones y resultados que permitan el liderazgo de la entidad a nivel de concejos municipales y distritales.

Imagen N° 26. Arquitectura Organizacional Concejo Distrital de Cartagena



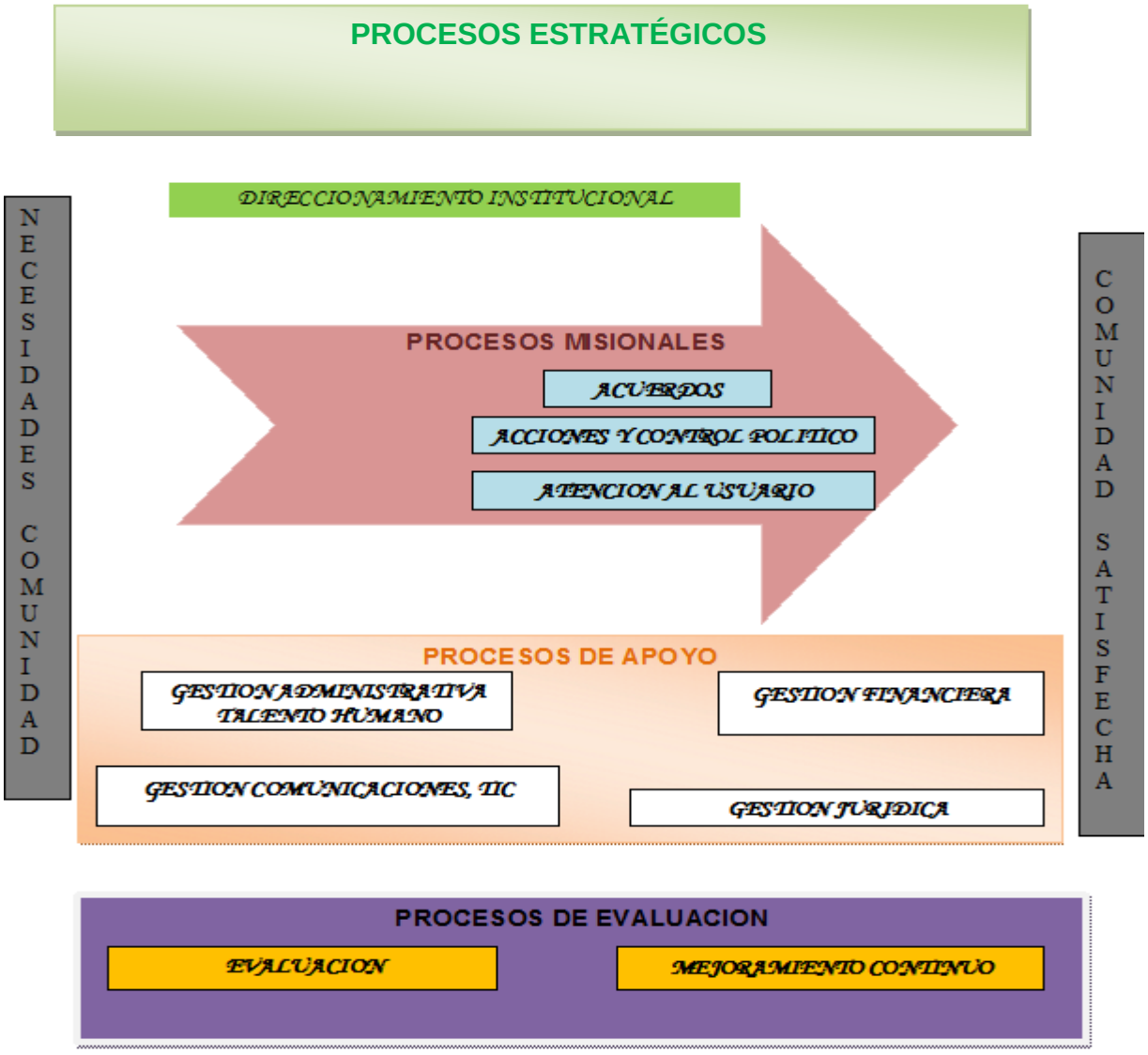
Fuente. Los autores de acuerdo a la información del Concejo Distrital de Cartagena.

8.2.1. Arquitectura de la Entidad

8.2.1.1. Cadena de Valor

La cadena de valor de la organización se ve representada por el mapa de procesos; como se muestra en la siguiente Imagen.

Imagen N° 27. Mapa de procesos Concejo Distrital de Cartagena



Fuente. Concejo Distrital

El Concejo Distrital de Cartagena de Indias dentro de su cadena de valor cuenta con los procesos estratégicos, los procesos misionales los cuales son los procesos más relevantes debido a que contribuyen directamente al cumplimiento de la razón de ser de la corporación, son responsabilidad de todos los Concejales, se ejecutan con su liderazgo, guiados por la Mesa Directiva y teniendo en cuenta las disposiciones legales sobre el actuar, proporcionan el resultado previsto por la corporación en el cumplimiento de su función.

Los procesos de apoyo son aquellos que se implementan para prestar apoyo a los demás procesos, los aprovisionan de recursos tanto técnicos, tecnológicos, financieros y humanos para el cumplimiento de la misión de la corporación y los procesos de evaluación verificación y control que son los procesos necesarios para controlar y medir las actuaciones de la corporación, realizar análisis de desempeño, proponer recomendaciones y sugerencias para la mejora en las operaciones de la entidad, forman parte integral de los otros procesos tanto misionales, de apoyo y estratégico. Permiten medir el desempeño y mejora de la eficacia y la eficiencia.

Dentro de los procesos también encontramos los procesos de evaluación que son los que permiten medir el cumplimiento de los objetivos institucionales.

8.2.2. Planeación Estratégica

MISIÓN DE LA ENTIDAD: “Debatir, estudiar y aprobar con responsabilidad y sindéresis los proyectos de acuerdos y ejercer el correspondiente control político como vocero y representante de la comunidad para el correcto funcionamiento de la Administración Distrital”

VISIÓN DE LA ENTIDAD: "Posicionar al 2020, al Concejo Distrital de Cartagena de Indias, como una corporación moderna y eficiente en su función administrativa, en aras del ejercicio democrático, del control social y político”

8.2.3. Objetivos Estratégicos de la Empresa

Objetivos de la entidad: Se constituyen en objetivos estratégicos de la entidad los siguientes:

- Vigilar la gestión integral del ejecutivo en sus distintos componentes, la gestión de los resultados de la administración y de las entidades que manejan los diferentes programas o bienes del Distrito; fundamentado en la eficacia, la economía y la equidad, conforme a los procedimientos, sistemas y principios que establece la ley.
- Generar en todos los funcionarios conciencia de la planeación, como herramienta fundamental y punto de partida para el desarrollo de las actividades productivas de cada dependencia, que conlleve a la formulación, ejecución y autocontrol de sus planes y proyectos; y que sea un proceso participativo que busque el logro de resultados mediante el uso racional de los recursos.

8.2.4. Plan Integral de Desarrollo

Según la reglamentación de la convocatoria pública para proveer el cargo de secretario (a) general del Concejo Distrital de Cartagena de Indias conforme a lo establecido en el artículo 126 constitucional, (Resolución No 164), se establece un Plan de Acción.

8.2.5. Valores Éticos

Tabla N° 11. Principios y Valores éticos del Concejo Distrital de Cartagena

PRINCIPIOS	VALORES
Responsabilidad	Compromiso
Liderazgo	Creatividad
Respeto	Calidad
Transparencia	Austeridad
Igualdad	Integridad
Justicia	Trabajo en equipo
	Honestidad

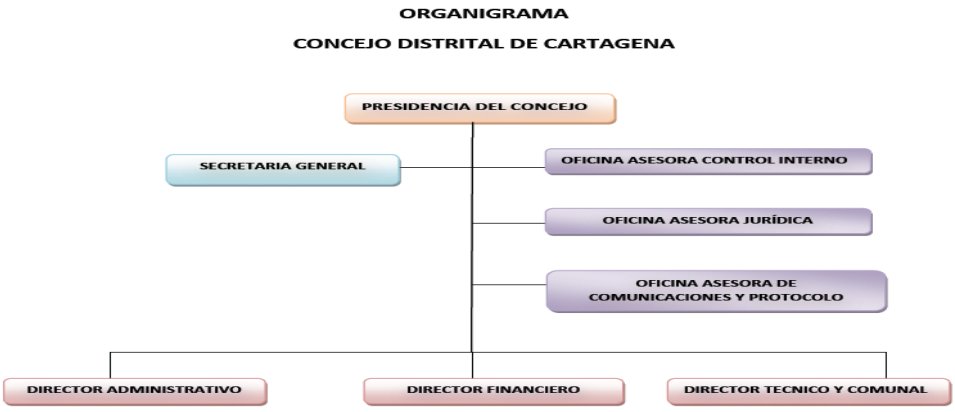
Fuente. Concejo Distrital

8.3. Estructura Organizacional y Funciones

8.3.1. Estructura Organizacional

El Concejo de Cartagena de Indias está organizado de la siguiente manera, como lo indica el organigrama mostrado a continuación:

Imagen N° 28. Organigrama Concejo Distrital de Cartagena



Fuente: tomado de la página web del Concejo Distrital de Cartagena

8.3.2. Funciones

Las siguientes son las funciones del Concejo Distrital de Cartagena de Indias (Funcicar, 2016):

- Reglamentar y garantizar la buena prestación de servicio por parte del Distrito haciendo control político a las dependencias de la Administración Distrital y a los entes que desempeñen funciones públicas.
- Adoptar planes de desarrollo (Económico, social, obras públicas)
- Autorizar los contratos que celebra la Alcaldía.
- Normatizar y expedir el presupuesto de Rentas y Gastos cada año.
- Determinar la estructura, las funciones, y escalas de remuneración de la Administración Distrital y atender las iniciativas del Alcalde.
- Reglamentar, vigilar y controlar las actividades relacionadas con el uso del suelo, construcción y enajenación de inmuebles destinados a vivienda.
- Elegir el Personero y el contralor Distrital cada tres años.
- Cuidar el patrimonio ecológico del distrito.
- Clasificar las áreas del perímetro urbano y darles nomenclatura a las casas, predios, vías etc.
- Establecer, reformar o eliminar tributos, impuestos, contribuciones y sobretasas.
- Defender nuestra cultura y cuidarla.
- Organizar la contraloría y personería.
- Dictar las normas del presupuesto de rentas y gastos.
- Elegir al Secretario General del Concejo.
- Autorizar los viajes internacionales del Alcalde.
- Señalar multas y penas de arrestos a quienes incumplas los acuerdos.
- Pedir informes a empleados del Distrito, para garantizar el buen desempeño de sus deberes.
- Reglamentar el repartimiento y entrega de los terrenos comunales y baldíos del Distrito y expedir normas que reglamenten las actividades recreativas y de entretenimientos en zonas de uso público.

8.3.3. Trámites y Servicios Actuales que Ofrece el Concejo Distrital de Cartagena

El Concejo Distrital de Cartagena en uso de sus facultades administrativas ofrece a la ciudadanía y entes interesados los siguientes servicios:

- Radicado de proyectos de acuerdo de interés a la ciudadanía
- Consulta de proyectos de acuerdo de intereses a los entes interesados y ciudadanía
- Consulta de actas de acuerdo a la ciudadanía y entes interesados
- Realización de control político a los funcionarios del distrito de Cartagena.
- Respuestas a derechos de petición de la ciudadanía.

8.4. Estado Del Arte De Diseño De Los Ejes Temáticos De La Estrategia Gobierno En Línea Tic Servicios Y Seguridad Y Privacidad De La Información

Para el desarrollo del estado del arte se realizó una revisión en línea de tesis que realizaran Diseños de los ejes temáticos de la estrategia gobierno en línea Tic servicios y seguridad y privacidad de la información, no hallándose proyectos específicos en el área, pero encontrándose diferentes bibliografías concernientes a Gobierno electrónico en el cual destacamos:

Ruiz Velasco (2013). En la Ciudad de Bogotá – Colombia desarrollo un trabajo de grado titulado " EL GOBIERNO EN LÍNEA EN COLOMBIA" el desarrollo de esta investigación se centró en analizar la situación actual Cuál es la situación actual del gobierno en línea en Colombia, realizando un rastreo histórico conceptual y legal sobre Tecnologías de Información y Comunicación (TIC), Internet y Gobierno en línea, entre otros, también se realiza una descripción de los antecedentes normativos relativos al desarrollo del gobierno en línea en Colombia y una recopilación sobre las Estrategias del Gobierno en Línea en Colombia para el período comprendido entre 2008 y 2012.

Concluyendo que el Gobierno en Línea ha impulsado el desarrollo económico, político, social y cultural del país, contribuyendo en cierta medida con el mejoramiento de la calidad de vida de todos los colombianos. En este sentido, sugiere una serie de bondades que en términos generales benefician a todos los sectores, comunidades y personas.

Lo expuesto anteriormente se relaciona directamente con la presente investigación, puesto que el autor utiliza la estrategia Gobierno en línea para mostrar la utilidad de su implementación en las entidades del estado.

Zea Hernández (2015) “Estado del arte del Gobierno Electrónico en Colombia para revisar la implementación del Gobierno en Línea.” En el trabajo de investigación se realiza una aproximación a lo que es gobierno electrónico, el estado del arte de gobierno electrónico y la estrategia en Colombia, concluyendo que la estrategia es muy importante para el desarrollo del país por los grandes avances que se han realizado en materia de tecnología, la gestión del conocimiento, y la gran presión de la responsabilidad social en cualquier actividad de la administración pública.

Sandoval y Massal (2010) Gobierno electrónico. ¿Estado, ciudadanía y democracia en internet? Este artículo trata sobre la proliferación de los gobiernos electrónicos en el mundo. Se recogen las perspectivas teóricas que lo perfilaron y se aborda la implementación del Gobierno en Línea en Colombia para así reflexionar en torno al comportamiento del estado y la sociedad en su encuentro con el mundo informático y la llamada era digital. El articulo muestra la importancia del compromiso institucional para lograr la implementación del gobierno electrónico en el país.

Sánchez y Rincón (2015). Gobierno electrónico, en el contexto local de la administración colombiana. En este artículo se muestra como el Gobierno electrónico permite a los países en proceso de tecnificación la opción de ponerse al mismo nivel de los tecnificados, siempre y cuando se aprovechen las nuevas tecnologías, lo que les permite avanzar en el proceso de adecuación de infraestructura; toda vez que las primeras transformaciones efectuadas en las administraciones tecnificadas.

Zapata y Pineda (2014). La Gestión Documental Electrónica en la Estrategia de Gobierno en línea: Análisis del Componente Gobierno –Ciudadano, este proyecto realiza un análisis de la gestión documental electrónica en el desarrollo de la estrategia de gobierno en línea como herramienta de participación ciudadana en las entidades de la rama ejecutiva del orden nacional, once entidades de la rama ejecutiva del poder público la cual tiene como función principal la de gobernar, administrar o ejecutar, que se manifiesta a través de la expedición de unos actos administrativos propiamente dichos

que poseen nivel jerárquico inferior a la ley dentro de la pirámide jurídica colombiana y se dan a conocer mediante su notificación. Se realiza una identificación y descripción los diversos servicios del gobierno en línea que involucran el componente de participación ciudadana y se identifican los principales tipos de documentos electrónicos que se gestionan como resultado de la estrategia de Gobierno en línea en desarrollo del componente Gobierno- Ciudadano.

En esta investigación se concluye que existe una inadecuada gestión documental y un problema de la implementación de nuevas tecnologías para la gestión de documentos electrónicos en la estrategia de Gobierno en Línea, por la gestión del cambio cultural que debe operarse para el cumplimiento de estas políticas. Este documento nos muestra la necesidad de implementar adecuados diseños en las diferentes temáticas de gobierno en línea para lograr el éxito de la estrategia.

Red GEALC, SEDI- OEA y ICA / IDRC (2008) De la teoría a la práctica: Cómo implementar con éxito el gobierno electrónico. Estos documentos exponen las características esenciales del concepto de gobierno electrónico y se describe brevemente su origen, su evolución conceptual y las características de su desarrollo actual en la América Latina y la Región Caribe, mostrando las barreras más comunes a la implementación de proyectos de E-Gobierno y su percepción general por parte de los actores en la región. Esta investigación es importante para el desarrollo del proyecto debido a que muestra las barreras a la implementación de gobierno electrónico.

En investigaciones internacionales encontramos a:

Robayo Valencia (2017) Gobierno electrónico en el Ecuador: análisis de su implementación en el marco del Plan Nacional 2014-2017. En este proyecto investigación, se revisa conceptos generales, que permiten entender las implicaciones que tiene la adopción del gobierno electrónico dentro de la administración pública. Adicionalmente se analiza el grado de desarrollo del Gobierno Electrónico en el Ecuador, a través de 3 aspectos: la medición de los indicadores propuestos en el Plan Nacional de Gobierno Electrónico (PNGE) del año 2014, la revisión de la aplicación de las tecnologías de la información y comunicación en los proyectos operativos y la evaluación los portales web gubernamentales. Los resultados del análisis realizado permitirán obtener en porcentaje el nivel de adopción del Plan Nacional, y consecuentemente ubicar

al Ecuador dentro de un nivel de madurez del gobierno electrónico. Este proyecto de grado muestra el avance de la implementación de a estrategia en Ecuador.

Pedraza Henríquez (2010). Con la tesis doctoral “Propuesta de un modelo gerencial estratégico socialmente responsable basado en el gobierno electrónico para la gestión de los gobiernos locales en el estado Aragua- Venezuela” a través de esta investigación se plantea una ruptura de los paradigmas de la administración pública y los nuevos cambios a los cuales debe someterse con el gobierno electrónico para lograr una nueva gestión pública donde el gobierno electrónico se muestra como una solución para la eficiencia y eficacia de los gobiernos locales y un acercamiento a las comunidades.

8.5. Aplicación del Modelo de Seguridad y Privacidad de la Información de la Estrategia Gel para Garantizar la Protección de los Recursos Tecnológicos en el Concejo Distrital de Cartagena

De acuerdo a la guía Modelo de Seguridad y Privacidad de la Información versión 3.0.1 realizada por Mintic en el año 2016 el MSPI preserva la confidencialidad, integridad, disponibilidad y privacidad de la información, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

Mediante la aplicación de este modelo el Concejo Distrital de Cartagena podrá formular estrategias que le permitan garantizar la protección de su información contribuyendo al logro de sus objetivos estratégicos.

¿Pero cómo se aplicará el modelo para lograr la protección de los recursos tecnológicos en el Concejo Distrital de Cartagena?

Inicialmente es necesario la realización del diagnóstico para lo cual se utilizan encuestas a los funcionarios de la entidad, el diagnostico permite conocer el estado actual con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información., teniendo el diagnostico se procede a identificar el nivel de madurez del MSPI para realizar así un documento con el análisis de vulnerabilidades y de riesgo. (Mintic, 2016).

El desarrollo del procedimiento señalado permitirá desarrollar el MSPI desarrollando para la entidad:

- Política de seguridad y privacidad de la información: La política de seguridad y privacidad de la información da cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno en línea de acuerdo a las Metas, Entregables e Instrumentos de la Fase de Planificación establecidas en la Guía Modelo de Seguridad y Privacidad de la Información versión 3.0.1 realizada por Mintic en el año 2016 donde se establece que es necesario contar con un documento con la política general de

seguridad de la información, debidamente aprobado y socializado al interior de la Entidad, por la alta Dirección.

- Procesos y procedimientos, debidamente definidos, los cuales permitirán la aplicación de controles de seguridad y privacidad de la información.
- Roles y responsabilidades de la seguridad de la información, donde se asignan las responsabilidades en cuanto a la seguridad de la información y
- Valoración de los activos de información y análisis de riesgos, el cual es de gran importancia porque a través de una adecuada valoración de los activos se podrá determinar la importancia de este dentro de la organización.

¿Pero cómo se realiza una adecuada clasificación de los activos de información de los Procesos de Atención al Usuario, Administrativa y Financiera del Concejo Distrital de Cartagena que permita determinar los riesgos en la seguridad de la información y definir los planes de tratamiento de los riesgos?

Los pasos que se deben realizar para una adecuada clasificación de los activos de información que permita determinar los riesgos en la seguridad de la información y definir los planes de tratamiento de riesgos para el Concejo Distrital de Cartagena en los procesos de Atención al usuario, Administrativa y Financiera de acuerdo a la guía para el levantamiento y valoración de activos de seguridad de la información de ministerio de salud y protección social 2017 son:

- Identificar y clasificar los activos informáticos procesos dirección financiera, dirección administrativa y atención al usuario.
- Realizar el Inventario de activos informáticos de los procesos de Dirección Financiera, Dirección Administrativa y Atención al usuario y
- Realiza la valoración de los activos de acuerdo a la metodología escogida.

9. DIAGNÓSTICO EJE TEMÁTICO TIC SERVICIOS

9.1. Estado del Arte Diagnóstico Tic Servicios

Se hizo una revisión en las distintas páginas de las entidades de los Concejos del Gobierno Colombiano y no existe un diagnóstico publicado acerca de la estrategia Gobierno en línea Eje Temático Tic Servicios.

Para el diagnóstico de la estrategia Tic Servicios se encuesto a 17 empleados de la entidad pertenecientes a las áreas de financiera, secretaria general y administrativa, además de los ciudadanos que visitaron la entidad el día 29 de agosto de 2017 para un total de 37 encuestas aplicadas y se realizó la revisión de las diferentes fuentes de información de los trámites que se tienen en el Concejo Distrital de Cartagena, SUIT (Sistema Único de Información y Tramites del Gobierno Colombiano) y Página Web de las entidad.

9.2. Aplicación De La Encuesta y Diagnóstico

9.2.1. Ficha Técnica Encuesta

Objetivo: Realizar el diagnóstico del eje temático Tic Servicios de la estrategia Gobierno en línea del Concejo Distrital de Cartagena.

Nombre: Cedula:

Cargo:

Tipo de Herramienta: Encuesta

Empresa: Concejo Distrital de Cartagena

Muestra: Focalización de empleados del Concejo Distrital, contratista del área de sistemas y ciudadanos de la entidad.

Método de aplicación: Cara a cara

Tipo de preguntas: Cerradas y abiertas basadas en variables cualitativas

Variables: Servicios de la entidad

Tamaño de la muestra: 37 personas

Tabla N° 12. Encuesta Servicios Centrados en el Ciudadano

SERVICIOS CENTRADOS EN EL USUARIO					
PREGUNTAS	si	no	ns/nr	Observaciones	Documento prueba
1. La entidad cuenta con trámites y servicios en línea					
2. Conoce usted los trámites y servicios que presta la entidad a la ciudadanía					
3. sabe si los trámites y servicios en línea están inscritos en el Suit					
4. 8.3.4. Si conoce los trámites y servicios en línea o manuales sabe que tramites cuenta con caracterización de los usuarios					
5. Sabe si la entidad presta lo siguientes servicios y tramites en línea					
Tramites:					
a. Presentación de proyectos de acuerdo mediante iniciativa popular					
b. Propuestas de control político					
c. participación de la comunidad en espacios de discusión (inscripción virtual)					
d. Cabildo Abierto (Inscripción virtual)					
e. Peticiones, quejas, reclamos y sugerencias					
Servicios					
a. Asesorías jurídicas					
b. Consulta de actas y proyectos de acuerdo					
6. De los procedimientos y trámites administrativos existentes cuales se pueden realizar en línea					
Tramites:					
a. Presentación de proyectos de acuerdo mediante iniciativa popular					
b. Propuestas de control político					
c. participación de la comunidad en espacios de discusión (inscripción virtual)					
d. Cabildo Abierto (Inscripción virtual)					
e. Peticiones, quejas, reclamos y sugerencias					
Servicios					
a. Asesorías jurídicas					
b. Consulta de actas y proyectos de acuerdo					

SERVICIOS CENTRADOS EN EL USUARIO					
PREGUNTAS	si	no	ns/nr	Observaciones	Documento prueba
7. La Entidad informa al usuario sobre sus derechos, obligaciones y las condiciones de uso del trámite o servicio en línea.					
8. La Entidad garantiza la protección de los datos personales de los usuarios del trámite o servicio en línea					
Usabilidad					
9. Los objetivos del sitio web de la entidad están bien definidos					
10. Cuenta la entidad con un estudio de Personajes y Escenarios, en donde se consideren por lo menos cinco usuarios de cada grupo representativo, y en el que se identifiquen las características, motivaciones, y escenarios de uso					
11. Cuenta la entidad con un documentos donde especifique las necesidades de los usuarios					
12. El sitio web de la entidad cuenta con una clara política de evaluación, si la respuesta es afirmativa señale cual					
13. Considera la arquitectura de la página web adecuada, es fácil realizar la navegación por el sitio					
14. como es su experiencia de usuario en la página web de la entidad					
a. buena					
b. mala					
c. pésima					
d. ns/nr					
15. La entidad cuenta con un sistema integrado para la gestión de peticiones, quejas, reclamos y denuncias que ingresan por diversos canales					
16. La entidad expide certificados y constancias para la ciudadanía por medios electrónicos					
17. Especifique si conoce otros tramites / procedimientos que tiene la entidad					
18. La entidad cuenta con ventanilla única para los tramites					
19. Que tramites le gustaría que se hicieran por la página web					

SERVICIOS CENTRADOS EN EL USUARIO					
PREGUNTAS	si	no	ns/nr	Observaciones	Documento prueba
1. consulta de pagos de contratistas. 2. Descarga de proyectos de acuerdo 3. Buzón de quejas y sugerencias 4. Descarga de actas 5. Certificación laboral 6. Manuales publicados 7. ejecución presupuestal 8 Mejorar la página web.					

Fuente. Los autores de acuerdo a la Estrategia Gobierno en Línea Tic Servicios

9.3. Análisis e interpretación de resultados

9.3.1. Servicios Centrados En El Usuario- Conocimiento De Trámites De La Entidad.

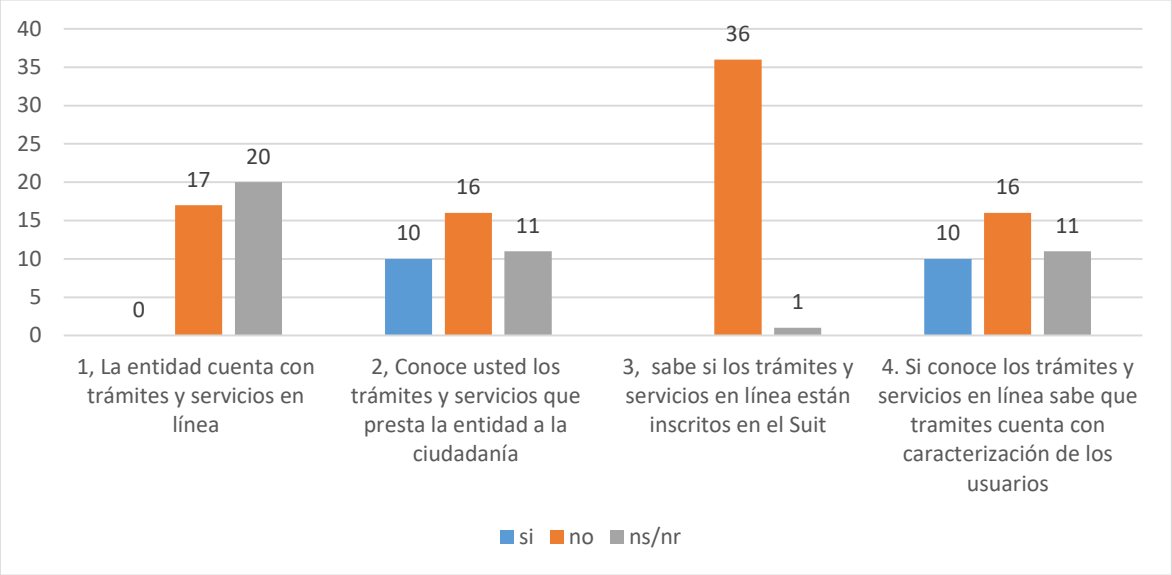
Para el logro servicios centrados en el usuario y poder conocer la percepción de los encuestados en los trámites y servicios de la entidad se formularon 4 preguntas que se relacionan en la tabla número 13.

Tabla N° 13. Resultados Logro Servicios Centrados en el Usuario - Conocimiento de trámites de la entidad

SERVICIOS CENTRADOS EN EL USUARIO	si	%	no	%	ns/nr	%
1, La entidad cuenta con trámites y servicios en línea	0	0%	17	46%	20	54%
2, Conoce usted los trámites y servicios que presta la entidad a la ciudadanía	10	27%	16	43%	11	30%
3, sabe si los trámites y servicios en línea están inscritos en el Suit	0	0%	36	0%	1	3%
4. Si conoce los trámites y servicios en línea sabe que tramites cuenta con caracterización de los usuarios	10	27%	27	73%	0	0%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de financiera, Administrativa, Contratista del área de sistemas y ciudadanos asistentes a las sesiones de la entidad.

Grafico N° 1. Gráfico Logro Servicios Centrados en el Usuario - Conocimiento de trámites de la entidad.



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de financiera, Administrativa, Contratista del área de sistemas y ciudadanos asistentes a las sesiones de la entidad.

De acuerdo a la Tabla número 13 donde se indican los porcentajes y la Grafica número 1 se puede concluir:

A la pregunta número 1: La entidad cuenta con trámites y servicios en línea, de las 37 personas encuestadas, el 54% de los encuestados responden que no sabe o no responde mientras que el 46% respondieron que no.

De acuerdo a las entrevistas realizadas al personal de planta de la entidad correspondiente a 17 personas manifiestan que existen los siguientes trámites:

- Radicado de proyectos de acuerdo de interés a la ciudadanía
- Consulta de proyectos de acuerdo de intereses a los entes interesados y ciudadanía
- Consulta de actas de acuerdo a la ciudadanía y entes interesados
- Realización de control político a los funcionarios del distrito de Cartagena.
- inscripción en proyectos de acuerdo, entrega de actas.

- Respuestas a derechos de petición de la ciudadanía.

Pero estos trámites y servicios no se han implementado en la página web lo que dificulta el acceso de la ciudadanía a los trámites y servicios de la entidad.

Pregunta numero 2: Se les pregunto si conocían los trámites que se prestaba a la ciudadanía a lo que el 43% respondió que no los conocían, un 30 % no sabe o no responde y un 27% que, si los conoce, sobre cuáles son los que conoce respondieron, que a través de la secretaria general se reciben:

Los proyectos de acuerdo: 70% de los encuestados que respondieron que si manifestaron que se tramitan proyectos de acuerdo en la entidad.

Se tramitan las actas de los debates: 60% de los encuestados que respondieron que si manifestaron que se tramitan las actas de los debates en forma manual y se lleva un archivo físico.

Se citan a los invitados: 100% de los encuestados que respondieron que a través de secretaria se citan a los invitados por envió de correspondencia física.

Se reciben propuestas de los debates a realizar: 50% de los encuestados que respondieron que sí, manifestaron que se reciben propuestas de los debates a utilizar, sobre todo proposiciones de la alcaldía de Cartagena.

Para la pregunta numero 3 acerca si conocen los trámites y servicios de la entidad se encuentran en el Suit, e 36 personas de las encuestadas respondieron que no mientras una respondió que no sabe.

A la pregunta número 4 , si conoce los trámites y servicios en línea o manuales sabe que tramites cuenta con caracterización de los usuarios De los 37 de los encuestados, 10 respondieron que si conoce los trámites (punto 8.3.2.), estos encuestados corresponde en su mayoría a los empleados del Concejo Distrital el 73%, responde que los trámites (Radicado de proyectos de acuerdo de interés a la ciudadanía, Consulta de proyectos de acuerdo de intereses a los entes interesados y ciudadanía, Consulta de actas de acuerdo a la ciudadanía y entes interesados, Realización de control político a los funcionarios del Distrito de Cartagena) no cuentan con caracterización de usuario.

Es preciso aclarar que el 100% coinciden en que los trámites son en forma manual aún no se realiza ningún trámite en línea.

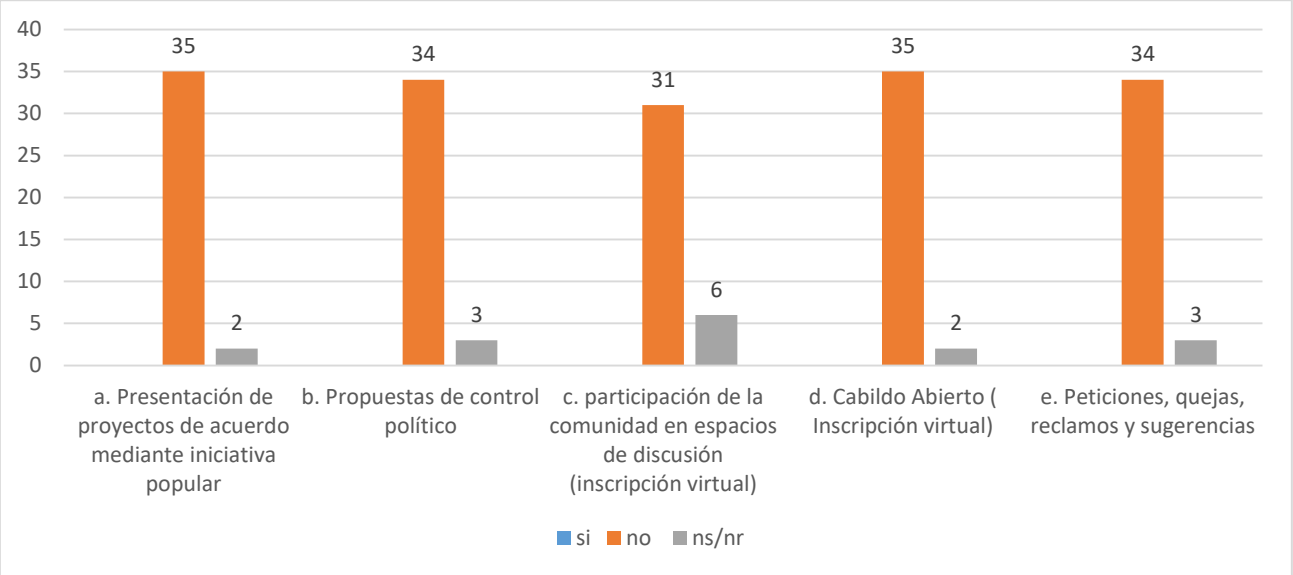
9.3.2. Logro Servicios Centrados en el Usuario - Trámites y servicios que presta la entidad de la entidad.

Tabla N° 14. Resultados Logro Servicios Centrados en el Usuario Trámites que presta la entidad de la entidad.

Tramites	si	%	no	%	ns/nr	%
a. Presentación de proyectos de acuerdo mediante iniciativa popular	0	0%	35	95%	2	5%
b. Propuestas de control político	0	0%	34	92%	3	8%
c. participación de la comunidad en espacios de discusión (inscripción virtual)	0	0%	31	84%	6	16%
d. Cabildo Abierto (Inscripción virtual)	0	0%	35	95%	2	5%
e. Peticiones, quejas, reclamos y sugerencias	0	0%	34	92%	3	8%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de financiera, Administrativa, Contratista del área de sistemas y ciudadanos asistentes a las sesiones de la entidad.

Grafico N° 2. Logro Servicios Centrados en el Usuario Trámites que presta la entidad de la entidad.



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de financiera, Administrativa, Contratista del área de sistemas y ciudadanos asistentes a las sesiones de la entidad.

De acuerdo a la Grafica Numero 2 y la tabla 14 se puede concluir que la entidad actualmente en materia de trámites presenta la siguiente situación:

La entidad no cuenta con el servicio de presentación de proyectos de acuerdo mediante iniciativa popular en línea de acuerdo a lo manifestado por 35 de los 37 encuestados mientras 2 no saben o no responden.

De acuerdo con el 92% de los encuestados la entidad no cuenta con el trámite propuestas de control político en línea.

Como se puede observar en el área de inscripciones virtuales para la participación de la comunidad en espacios de discusión, la entidad no cuenta con este servicio tal como lo manifestaron 31 personas de las 37 que participaron en la encuesta, mientras las 6 personas restantes no saben o no responden.

El 95% de los encuestados manifiesta que la entidad no cuenta con el trámite inscripción de cabildo abierto de manera virtual, el 5% no sabe o no responde.

A la pregunta que si la entidad presta el servicio en línea de peticiones, quejas y reclamos 34 de los 37 participantes respondió que no mientras 3 no saben o no responden. La entidad no posee ni en forma física ni en línea una oficina especial para la recepción de peticiones, quejas y reclamos.

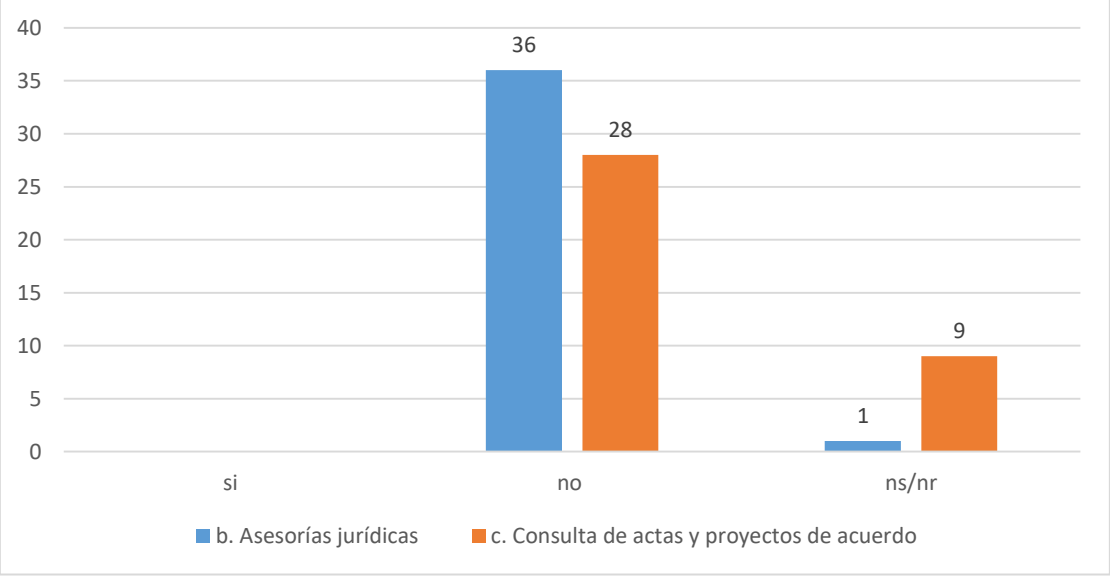
Logro Servicios Centrados en el Usuario - Servicios que presta la entidad de la entidad.

Tabla N° 15. Resultados Logro Servicios Centrados en el Usuario - Servicios que presta la entidad de la entidad

Servicios						
	si	%	no	%	ns/nr	%
b. Asesorías jurídicas	0	0%	36	97%	1	3%
c. Consulta de actas y proyectos de acuerdo	0	0%	28	76%	9	24%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de financiera, Administrativa, Contratista del área de sistemas y ciudadanos asistentes a las sesiones de la entidad.

Grafico N° 3. **Logro Servicios Centrados en el Usuario - Servicios que presta la entidad de la entidad**



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de financiera, Administrativa, Contratista del área de sistemas y ciudadanos asistentes a las sesiones de la entidad.

Para la pregunta si se puede solicitar asesorías jurídicas en línea el 97% manifestó que no mientras el 3% restante no sabe o no responde.

Para la pregunta se puede consultar actas y proyectos de acuerdo en línea los encuestados respondieron que la entidad no posee el servicio de consulta de actas y proyectos de acuerdo en línea, tal como lo manifiesta el 76% de los encuestados, mientras un 24% no sabe o no responde. La manera de consultar un proyecto de acuerdo o acta se hace mediante una petición por escrito la cual debe dirigirse a la Secretaria general de la corporación la cual surte los trámites internos que sean necesarios.

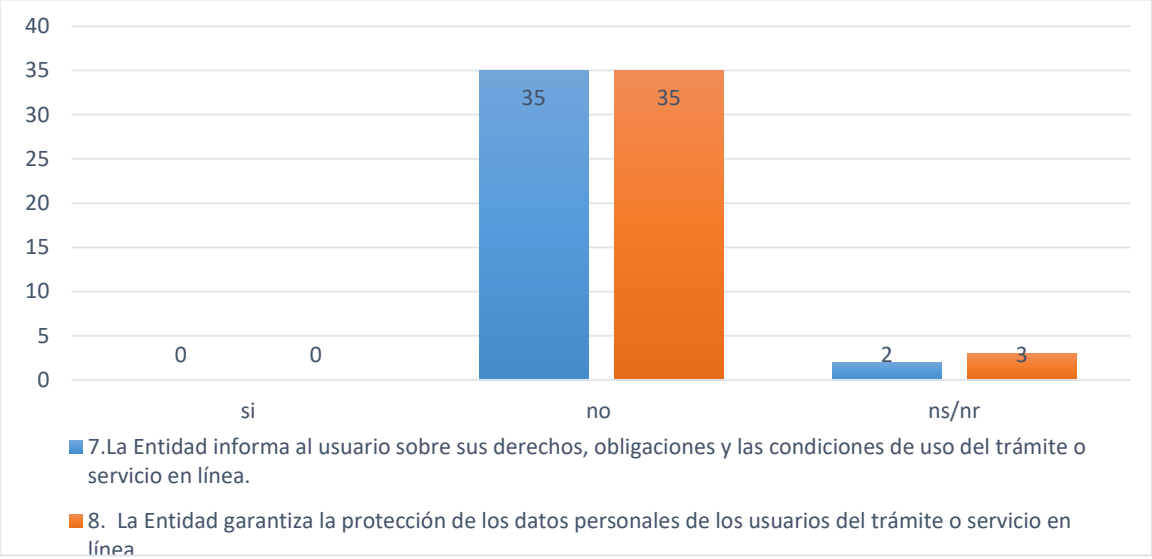
Logro servicios centrados en el usuario – información que suministra la entidad acerca de los trámites y servicios en línea

Tabla N° 16. Resultados Logro servicios centrados en el usuario –Información que suministra la entidad.

Preguntas	si	%	no	%	ns/ nr	%
7. La Entidad informa al usuario sobre sus derechos, obligaciones y las condiciones de uso del trámite o servicio en línea.	0	0%	35	95%	2	5%
8. La Entidad garantiza la protección de los datos personales de los usuarios del trámite o servicio en línea	0	0%	35	95%	3	8%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de financiera, Administrativa, Contratista del área de sistemas y ciudadanos asistentes a las sesiones de la entidad.

Grafico N° 4: Logro servicios centrados en el usuario –Información que suministra la entidad.



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Contratista del área de sistemas y ciudadanos asistentes a las sesiones de la entidad.

El 95% de los encuestados para la pregunta ¿La Entidad informa al usuario sobre sus derechos, obligaciones y las condiciones de uso del trámite o servicio en línea? Infirió que no se les informa sobre sus derechos, obligaciones y las condiciones de uso del trámite o servicio en línea, mientras el 5% no sabe o no responde.

La entidad no garantiza la protección de los datos personales de los usuarios del trámite o servicio en línea de acuerdo al 92% de los encuestados, el 8% restante no sabe o no responde. La respuesta se da debido a que la entidad no posee ningún tipo de servicio o tramite en línea.

USABILIDAD

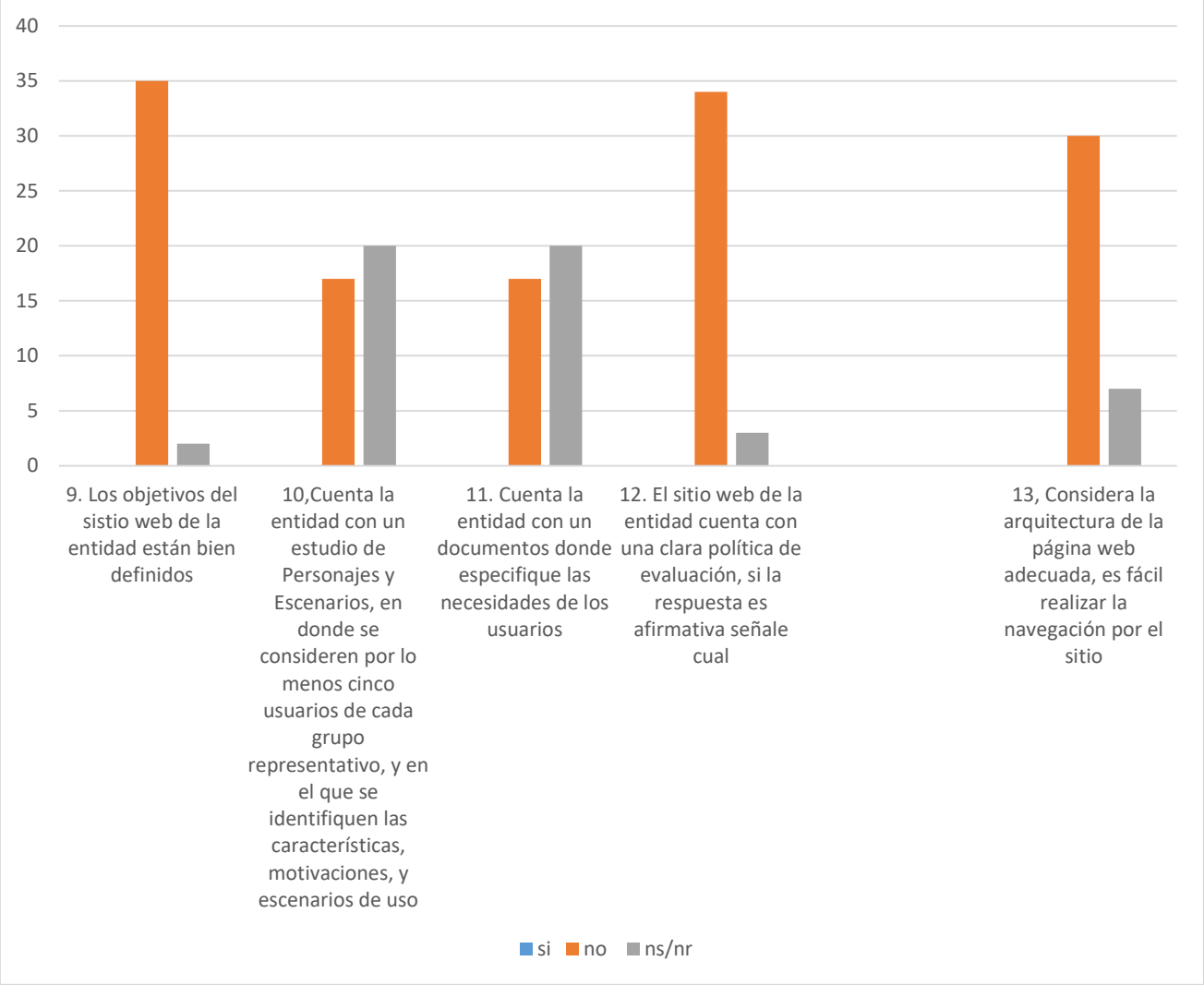
Para usabilidad de los trámites se diseñaron 10 preguntas que nos exponen la situación actual de usabilidad de los trámites y servicios del Concejo Distrital de dieron como resultado los siguientes gráficos y tablas:

Tabla N° 17. Usabilidad – Tramites y pagina Web

Pregunta	si	%	no	%	ns/nr	%
9. Los objetivos del sitio web de la entidad están bien definidos	0	0%	35	95%	2	5%
10 Cuenta la entidad con un estudio de Personajes y Escenarios, en donde se consideren por lo menos cinco usuarios de cada grupo representativo, y en el que se identifiquen las características, motivaciones, y escenarios de uso	0	0%	17	46%	20	54%
11. Cuenta la entidad con un documentos donde especifique las necesidades de los usuarios	0	0%	17	46%	20	54%
12. El sitio web de la entidad cuenta con una clara política de evaluación, si la respuesta es afirmativa señale cual	0	0%	34	92%	3	8%
13, Considera la arquitectura de la página web adecuada, es fácil realizar la navegación por el sitio	0	0%	30	81%	7	19%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de financiera, Administrativa, Contratista del área de sistemas y ciudadanos asistentes a las sesiones de la entidad.

Grafico N° 5. Usabilidad – Tramites y pagina Web



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de financiera, Administrativa, Contratista del área de sistemas y ciudadanos asistentes a las sesiones de la entidad.

De acuerdo a la tabla 17 y el Gráfico número 5, en la pregunta numero 9: El 95% de los encuestados manifiestan que los objetivos no están definidos debido a que nos los conocen, no se ha realizado una socialización a la ciudadanía y constantemente esta no funciona o está en mantenimiento mientras el 5% no sabe no responde.

Pregunta Número 10: La entidad no cuenta con estudios de personajes y escenarios tal como lo establece el 54% de los encuestados, el 46% no sabe o no responde a la pregunta. Esto nos indica que no hay una caracterización de los usuarios de la entidad,

por lo que se hace imposible conocer sus gustos y preferencias siendo muy difícil proponer servicios y tramites que se ajusten a sus necesidades.

Pregunta numero 11: De acuerdo a lo inferido por 17 de los 37 encuestados la entidad no cuenta con documentos para la identificación de las necesidades de los usuarios, lo que es necesario para su satisfacción, 20 de los encuestados no saben o no respondieron la pregunta.

A la pregunta numero 12 acerca de las políticas de evaluación de la entidad el 92% de los encuestados no cuenta con claras políticas de evaluación lo que no permite saber el grado de satisfacción del sitio por parte de los administradores, el 8% no sabe o no responde.

En la pregunta numero 13 el 81% de los encuestados considera que la arquitectura del sitio no es adecuada, el 19% no sabe o no responde, es necesario realizar un estudio de la arquitectura planteada para saber porque los usuarios del sitio consideran que es impropia.

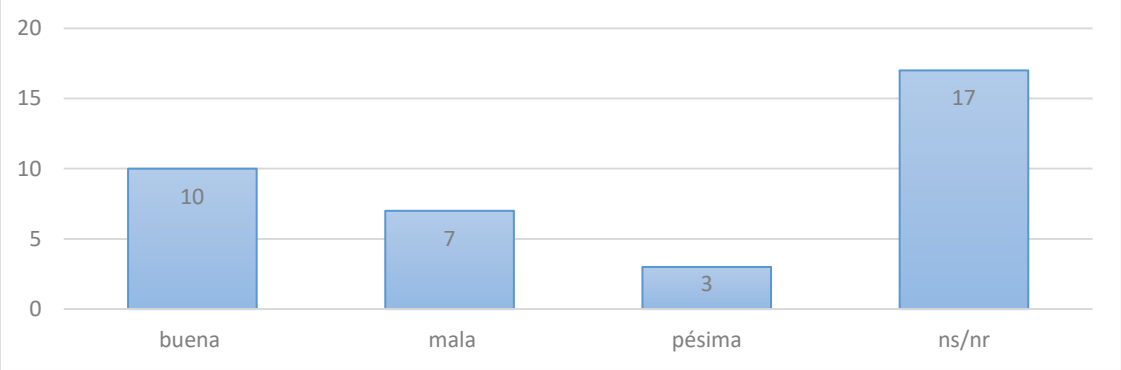
Usabilidad -Como es su experiencia de usuario en la página web de la entidad

Tabla N° 18. Usabilidad- Experiencia de usuario en la página web de la entidad.

14. como es su experiencia de usuario en la página web de la entidad	R	%
buena	10	27%
mala	7	19%
pésima	3	8%
ns/nr	17	46%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de financiera, Administrativa, Contratista del área de sistemas y ciudadanos asistentes a las sesiones de la entidad.

Grafico N° 6. . Usabilidad Experiencia de usuario en la página web de la entidad



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de financiera, Administrativa, Contratista del área de sistemas y ciudadanos asistentes a las sesiones de la entidad.

10 de los 37 encuestados que corresponde al 27% considera que la experiencia con la página web es buena, 7 que es mala y 3 que es pésima mientras que 17 de los encuestados que corresponde al 46% no saben o no responde.

Es necesario realizar una sensibilización hacia la ciudadanía cartagenera con el fin de que conozcan adecuadamente la página web de la entidad teniendo en cuenta que es un medio de comunicación de gran importancia para la ciudadanía.

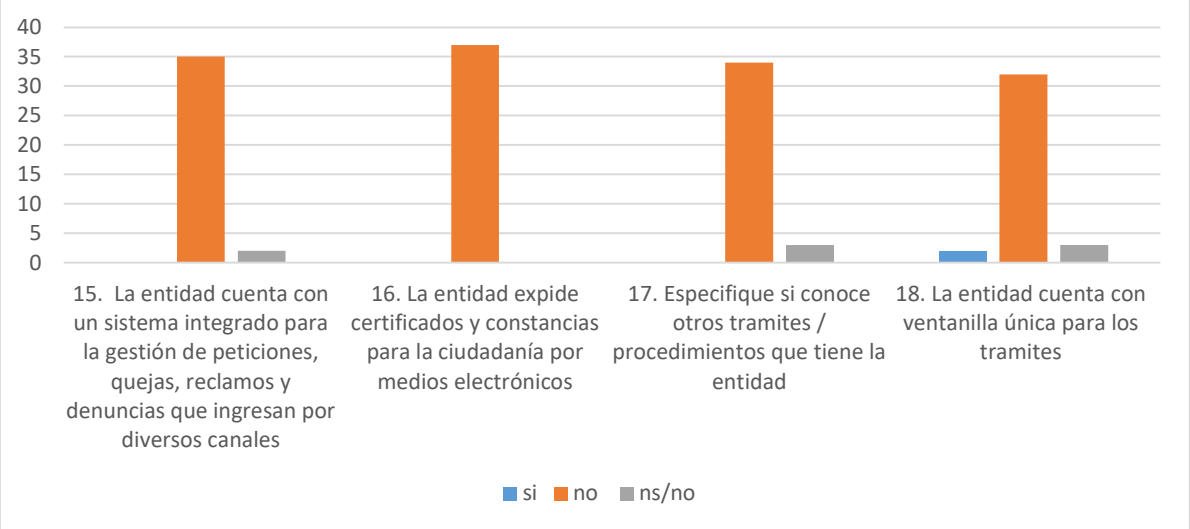
Usabilidad – Sistema PQRD, certificados y otros trámites, Ventanilla única

Tabla N° 19. Usabilidad - Sistema PQRD, certificados y otros trámites, Ventanilla única

Pregunta	si	%	no	%	ns/nr	%
15. La entidad cuenta con un sistema integrado para la gestión de peticiones, quejas, reclamos y denuncias que ingresan por diversos canales	0	0%	35	1%	2	5%
16. La entidad expide certificados y constancias para la ciudadanía por medios electrónicos	0	0%	37	1%	0	0%
17. Especifique si conoce otros tramites / procedimientos que tiene la entidad	0	0%	34	1%	3	8%
18. La entidad cuenta con ventanilla única para los tramites	2	5%	32	1%	3	8%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de financiera, Administrativa, Contratista del área de sistemas y ciudadanos asistentes a las sesiones de la entidad.

Grafico N° 7. Usabilidad - Sistema Pqrd, certificados y otros trámites, Ventanilla única



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de financiera, Administrativa, Contratista del área de sistemas y ciudadanos asistentes a las sesiones de la entidad.

Como se observa en la tabla 19 y el Gráfico número 7 se evalúan las preguntas 15 a las 18 en la primera pregunta si la entidad cuenta con un sistema integrado de peticiones, quejas y reclamos de acuerdo a lo manifestado por el 95% de los encuestados no se cuenta con él, Las peticiones se entregan en la oficina de correspondencia y estas son dirigidas a secretaria general algunas veces se incumplen los plazos por no entregar en la oficina adecuada el oficio. El 5 % de los encuestados no sabe o no responde.

La pregunta número 16, ¿La entidad expide certificados y constancias para la ciudadanía por medios electrónicos?, de acuerdo a los 37 encuestados la entidad no expide certificados y constancia por medios electrónicos, por lo que es necesario que la ciudadanía asista presencialmente ante cualquier solicitud de la entidad.

En relación a la pregunta N° 17 ¿Especifique si conoce otros trámites / procedimientos que tiene la entidad? De acuerdo a lo manifestado por 34 de los encuestados no conocen otro tipo de trámites o procedimientos que realiza la entidad, tres funcionarios no saben o no responden.

Para la pregunta número 18 que corresponde a la ventanilla única, de acuerdo a 32 de los 37 encuestados la entidad no cuenta con una ventanilla única para trámites, 3 no saben no responden y 2 de los encuestados manifiestan que si, al indagar la respuesta afirmativa dice que encuentran una oficina de correspondencia que les recibe los documentos.

Al verificar la página web se observa que está en renovación, al entrevistar al ingeniero contratado informa que a través de la página web no se dispone de ningún trámite y servicio en línea, por lo que en todos los casos el ciudadano debe realizar los procesos personalmente, por lo cual debe desplazarse al Concejo de Cartagena realizando filas en muchas ocasiones con resultados poco eficientes y confiables dado que las dependencias trabajan en forma desarticulada dificultando los tramites que necesitan los ciudadanos.

Que tramites sugeriría implementar en la entidad en línea

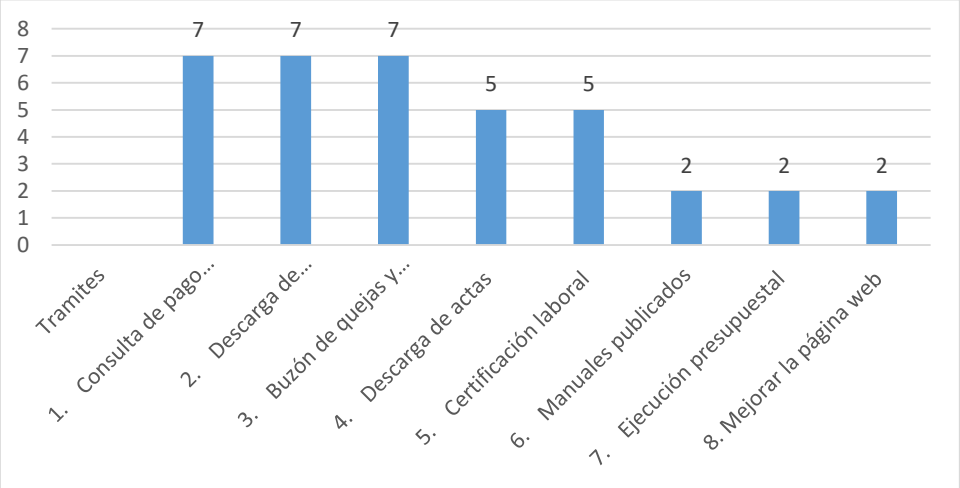
Se realizó una pregunta abierta con el fin de conocer cuales trámites le gustaría al usuario que se implementara en línea a lo que se obtuvo las siguientes respuestas:

Tabla N° 20. Trámites y servicios a implementar en la entidad

Tramites	Respuestas	%
1. Consulta de pago contratistas	7	19%
2. Descarga de proyectos de acuerdo	7	19%
3. Buzón de quejas y sugerencias	7	19%
4. Descarga de actas	5	14%
5. Certificación laboral	5	14%
6. Manuales publicados	2	5%
7. Ejecución presupuestal	2	5%
8. Mejorar la página web	2	5%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de financiera, Administrativa, Contratista del área de sistemas y ciudadanos asistentes a las sesiones de la entidad.

Grafico N° 8. Trámites y servicios a implementar en la entidad



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de financiera, Administrativa, Contratista del área de sistemas y ciudadanos asistentes a las sesiones de la entidad.

De acuerdo a los encuestados los trámites que sugeriría implementar en la entidad en línea serian en este orden:

Consulta de pago contratistas (19%)
Descarga de proyectos de acuerdo (19%)
Buzón de quejas y sugerencias (19%)
Descarga de actas (14%)
Certificación laboral (14%)
Manuales publicados (5%)
Ejecución presupuestal (5%)
Mejorar la página web (5%)

9.4. Diagnóstico Modelo De Seguridad y Privacidad La Información

9.4.1. Estado del Arte Diagnóstico Modelo de Seguridad y Privacidad la Información.

Se hizo una revisión en las distintas páginas de las entidades de los Concejos del Gobierno Colombiano y no existe un DIAGNÓSTICO publicado acerca de la estrategia Gobierno en línea Modelo de Seguridad y privacidad de la información, pero existe referencia bibliográfica relacionada con la seguridad de la información para algunas entidades del estado así:

Gallo Oñate, 2014, Diagnóstico de cumplimiento del modelo gestionado por el sistema de administración de la seguridad de la información de gobierno en línea – sasigel alineado con la norma 27000 para el instituto nacional de formación técnica profesional de la guajira. La tesis busca identificar los parámetros que establece el Sistema de Administración de la Seguridad de la Información de Gobierno en Línea (SASIGEL) y abordar algunos aspectos que servirán como base para lograr la verificación sobre el Nivel de madurez del Instituto Nacional de Formación Técnica Profesional con respecto a la implementación del modelo SASIGEL. El proyecto realiza la verificación del nivel de madurez frente a la norma 27001.

Concluyendo que La implementación del Sistema de Gestión de Seguridad de la información cada día se convierte en un aspecto muy importante dentro de las organizaciones y por medio del SASIGEL les permitirá a dichas organizaciones adoptar un modelo Gubernamental que se adapta tanto para las entidades públicas como las privadas que lo deseen acoger.

Pulido y Mantilla, (2016). Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina TIC de la alcaldía municipal de Fusagasugá, basados en la gestión del riesgo informático, donde se presentan organizadamente los temas objeto de estudio abordado en el desarrollo de un modelo para la implementación de un Sistema de Gestión de Seguridad de la Información y protocolos de seguridad informática en la Alcaldía Municipal de Fusagasugá, con el que se pueda gestionar y controlar los Riesgos Informáticos identificados y a los que se encuentra expuesta la entidad.

Se aplicó la metodología PHVA y la normatividad emitida por el Ministerio de las TIC para Gobierno en Línea 3.0 y el modelo de seguridad y privacidad de la información establecida para las entidades públicas por parte del gobierno nacional. También se presentan herramientas de medición como encuestas y entrevistas, cuyo resultado indica que la entidad debe incluir planes de capacitación en temas de Seguridad, privacidad y confidencialidad de la información e ingeniería social, y emplear estrategias transversales de comunicación para la difusión y apropiación de la seguridad y privacidad de la información en la entidad.

Para el diagnóstico de la estrategia modelo de seguridad y privacidad la información se encuesto a 16 colaboradores de las áreas de financiera, secretaría general y administrativa y el contratista del área de sistemas para un total de 17 encuestas aplicadas.

9.4.2. Aplicación de la Encuesta y Diagnóstico

9.4.2.1. Ficha Técnica Encuesta

Objetivo: realizar el diagnóstico del Modelo de seguridad y privacidad de la información de la estrategia Gobierno en línea del Concejo Distrital de Cartagena.

Nombre: Área:

Cargo:

Tipo de Herramienta: Encuesta

Empresa: Concejo Distrital de Cartagena

Muestra: Focalización de empleados del Concejo Distrital

Método de aplicación: Cara a cara

Tipo de preguntas: Cerradas basadas en variables cualitativas

Variables: Seguridad y privacidad de la información

Tamaño de la muestra: 17 personas (16 Funcionarios de planta y un (1) contratista del área de sistemas.

Tabla N° 21. Encuesta Modelo de Seguridad y privacidad de la información

N	POLÍTICAS DE SEGURIDAD	SI	NO	NS/NR	Explique Su respuesta	Evidencia documental
1	Existen documento(s) de políticas de seguridad de los sistemas de Información					
2	•Existe normativa relativa a la seguridad de los SI					
3	•Existen procedimientos relativos a la seguridad de SI					
4	•Existe un responsable de las políticas, normas y procedimientos					
5	•Existen mecanismos para la comunicación a los usuarios de las normas					
6	•Existen controles regulares para verificar la efectividad de las políticas					
	ORGANIZACIÓN DE LA SEGURIDAD	SI	NO	NS/NR	Explique Su respuesta	Evidencia documental
7	•Existen roles y responsabilidades definidos para las personas implicadas en la seguridad					
8	•Existe un responsable encargado de evaluar la adquisición y cambios de SI					
9	La Dirección y las áreas de la Organización participa en temas de seguridad					
10	•Existen condiciones contractuales de seguridad con terceros y outsourcing					
11	•Existen criterios de seguridad en el manejo de terceras partes					
12	•Existen programas de formación en seguridad para los empleados, clientes y terceros					
13	•Existe un acuerdo de confidencialidad de la información que se accesa.					
14	•Se revisa la organización de la seguridad periódicamente por una empresa externa					

	ADMINISTRACIÓN DE ACTIVOS	SI	NO	NS/NR	Explique Su respuesta	Evidencia docume ntal
15	•Existen un inventario de activos actualizado					
16	•El Inventario contiene activos de datos, software, equipos y servicios					
17	•Se dispone de una clasificación de la información según la criticidad de la misma					
18	• Existe un responsable de los activos					
19	•Existen procedimientos para clasificar la información					
20	•Existen procedimientos de etiquetado de la información					
	SEGURIDAD DE LOS RR.HH.	SI	NO	NS/NR	Explique Su respuesta	Evidencia documental
21	•Se tienen definidas responsabilidades y roles de seguridad					
22	•Se tiene en cuenta la seguridad en la selección y baja del personal					
23	•Se plasman las condiciones de confidencialidad y responsabilidades en los contratos					
	SEGURIDAD DE LOS RR.HH.	SI	NO	NS/NR	Explique Su respuesta	Evidencia documental
24	•Se imparte la formación adecuada de seguridad y tratamiento de activos					
25	•Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad					
26	•Se recogen los datos de los incidentes de forma detallada					
27	•Informan los usuarios de las vulnerabilidades observadas o sospechadas					
28	•Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades					
29	• Existe un proceso disciplinario de la seguridad de la información					
	SEGURIDAD FÍSICA Y DEL AMBIENTE	SI	NO	NS/NR	Explique Su respuesta	Evidencia documental
30	Existe perímetro de seguridad física (una pared, puerta con llave).					

	SEGURIDAD FÍSICA Y DEL AMBIENTE	SI	NO	NS/NR	Explique Su respuesta	Evidencia documental
31	Existen controles de entrada para protegerse frente al acceso de personal no autorizado					
32	Un área segura ha de estar cerrada, aislada y protegida de eventos naturales					
33	En las áreas seguras existen controles adicionales al personal propio y ajeno					
34	Las áreas de carga y expedición están aisladas de las áreas de SI					
35	La ubicación de los equipos está de tal manera para minimizar accesos innecesarios.					
36	Existen protecciones frente a fallos en la alimentación eléctrica					
37	Existe seguridad en el cableado frente a daños e intercepciones					
38	Se asegura la disponibilidad e integridad de todos los equipos					
39	Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente					
40	Se incluye la seguridad en equipos móviles					
	GESTIÓN DE COMUNICACIONES Y OPERACIONES	SI	NO	NS/NR	Explique Su respuesta	Evidencia documental
41	Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados					
	GESTIÓN DE COMUNICACIONES Y OPERACIONES	SI	NO	NS/NR	Explique Su respuesta	Evidencia documental
42	Están establecidas responsabilidades para controlar los cambios en equipos					
43	Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad					
44	Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas					
45	Existe una separación de los entornos de desarrollo y producción					
46	Existen contratistas externos para la gestión de los Sistemas de Información					
47	Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento					

	GESTIÓN DE COMUNICACIONES Y OPERACIONES	SI	NO	NS/NR	Explique Su respuesta	Evidencia documental
48	Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones					
49	Controles contra software maligno					
50	Realizar copias de Backus de la información esencial para el negocio					
51	Existen logs para las actividades realizadas por los operadores y administradores					
52	Existen logs de los fallos detectados					
53	Existen rastro de auditoría					
54	Existe algún control en las redes					
55	Hay establecidos controles para realizar la gestión de los medios informáticos.(cintas, discos, removibles, informes impresos)					
56	Eliminación de los medios informáticos. Pueden disponer de información sensible					
57	Existe seguridad de la documentación de los Sistemas					
58	Existen acuerdos para intercambio de información y software					
59	Existen medidas de seguridad de los medios en el tránsito					
60	Existen medidas de seguridad en el comercio electrónico.					
61	Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada					
	GESTIÓN DE COMUNICACIONES Y OPERACIONES	SI	NO	NS/NR	Explique Su respuesta	Evidencia documental
62	Existen medidas de seguridad en las transacciones en línea					
63	Se monitorean las actividades relacionadas a la seguridad					
	CONTROL DE ACCESOS	SI	NO	NS/NR	Explique Su respuesta	Evidencia documental
64	Existe una política de control de accesos					
65	Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario					
66	Existe una gestión de los password de usuarios					

	CONTROL DE ACCESOS	SI	NO	NS/NR	Explique Su respuesta	Evidencia documental
67	Existe una revisión de los derechos de acceso de los usuarios					
68	Existe el uso del password					
69	Se protege el acceso de los equipos desatendidos					
70	Existen políticas de limpieza en el puesto de trabajo					
71	Existe una política de uso de los servicios de red					
72	Se asegura la ruta (path) desde el terminal al servicio					
73	Existe una autenticación de usuarios en conexiones externas					
74	Existe una autenticación de los nodos					
75	Existe un control de la conexión de redes					
76	Existe un control del routing de las redes					
77	Existe una identificación única de usuario y una automática de terminales					
78	Existen procedimientos de log-on al terminal					
79	Se ha incorporado medidas de seguridad a la computación móvil					
80	Está controlado el teletrabajo por la organización					
	DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	SI	NO	NS/NR	Explique Su respuesta	Evidencia documental
81	Se asegura que la seguridad está implantada en los Sistemas de Información					
82	Existe seguridad en las aplicaciones					
83	Existen controles criptográficos.					
	DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	SI	NO	NS/NR	Explique Su respuesta	Evidencia documental
84	Existe seguridad en los ficheros de los sistemas					
85	Existe seguridad en los procesos de desarrollo, testing y soporte					
86	Existen controles de seguridad para los resultados de los sistemas					
87	Existe la gestión de los cambios en los SO.					

	DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	SI	NO	NS/NR	Explique Su respuesta	Evidencia documental
88	Se controlan las vulnerabilidades de los equipos					
	ADMINISTRACIÓN DE INCIDENTES	SI	NO	NS/NR	Explique Su respuesta	Evidencia documental
89	Se comunican los eventos de seguridad					
90	Se comunican los debilidades de seguridad					
91	Existe definidas las responsabilidades antes un incidente.					
92	Existe un procedimiento formal de respuesta					
93	Existe la gestión de incidentes					
	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	SI	NO	NS /NR	Explique Su respuesta	Evidencia documental
94	Existen procesos para la gestión de la continuidad.					
95	Existe un plan de continuidad del negocio y análisis de impacto					
96	Existe un diseño, redacción e implantación de planes de continuidad					
97	Existe un marco de planificación para la continuidad del negocio					
98	Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio.					
	CUMPLIMIENTO	SI	NO	NS/NR	Explique Su respuesta	Evidencia documental
99	Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas					
100	Existe el resguardo de la propiedad intelectual					
101	Existe el resguardo de los registros de la organización					
102	Existe una revisión de la política de seguridad y de la conformidad técnica					
103	Existen consideraciones sobre las auditorías de los sistemas					

Fuente. Encuesta elaborada por de acuerdo al modelo de seguridad y privacidad de la información Estrategia Gobierno en línea.

9.5. Análisis e Interpretación de los Resultados Modelo de Seguridad de la Información.

Para el diagnóstico del Modelo de seguridad y privacidad de la información es necesario realizar un análisis que permita determinar el estado actual de la entidad esto permite identificar las brechas existentes dentro de la organización para lo cual se aplicó la encuesta de evaluación del Modelo de Seguridad de la información, se realizó la encuesta a los empleados del área de Administrativa, Secretaria General, Financiera y el contratista del área de sistemas.

9.5.1. Dimensión Políticas De Seguridad

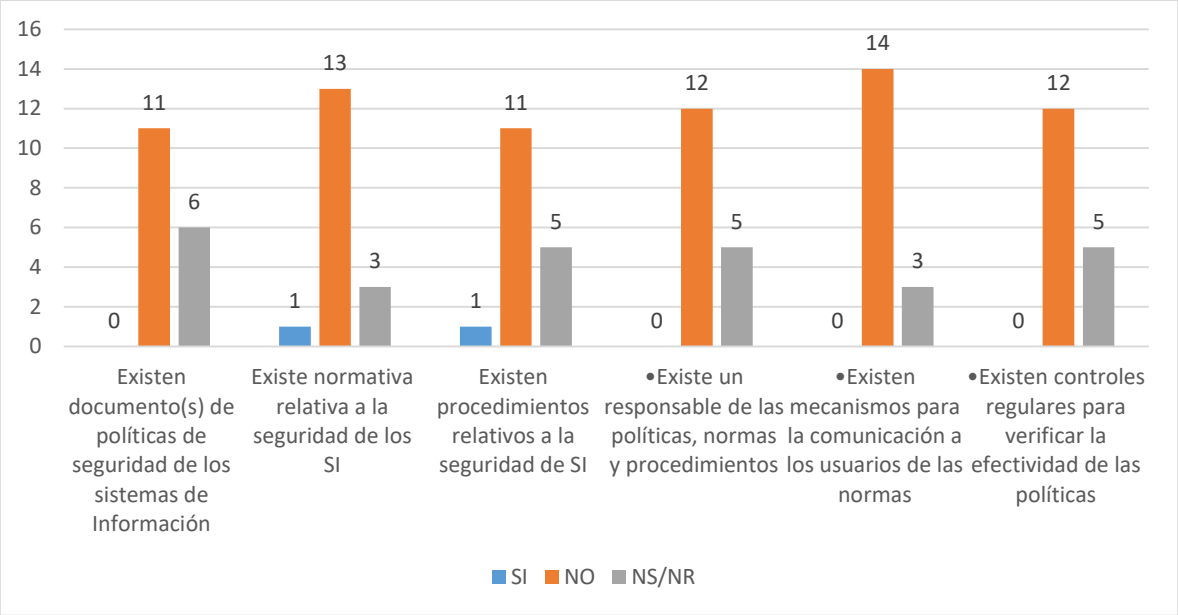
Esta dimensión contiene 6 ítems que muestran si el Concejo Distrital de Cartagena da soporte a la gestión de seguridad de la información de acuerdo al Modelo de seguridad y privacidad de GEL

Tabla N° 22. Resultados Dimensión Políticas de Seguridad

POLÍTICAS DE SEGURIDAD	SI	%	NO	%	NS/NR	%
1, Existen documento(s) de políticas de seguridad de los sistemas de Información	0	0%	11	65%	6	35%
2, Existe normativa relativa a la seguridad de los SI	1	6%	13	76%	3	18%
3, Existen procedimientos relativos a la seguridad de SI	1	6%	11	65%	5	29%
4 Existe un responsable de las políticas, normas y procedimientos	0	0%	12	71%	5	29%
5, Existen mecanismos para la comunicación a los usuarios de las normas	0	0%	14	82%	3	18%
6 Existen controles regulares para verificar la efectividad de las políticas	0	0%	12	71%	5	29%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas.

Grafico N° 9. Dimensión Políticas de Seguridad



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas.

Como se puede observar en el gráfico N°9 y en la tabla N° 22 de acuerdo a las preguntas realizadas se puede inferir:

Pregunta 1: A la pregunta existen documentos de políticas de seguridad de los sistemas de información el 65% de empleados del Concejo Distrital de Cartagena respondió que no existen políticas y el 35% no sabe o no responde. Lo que permite concluir que el Concejo Distrital de Cartagena no tiene documentos relativos a políticas de seguridad de los sistemas de información y que es necesario diseñar las políticas correspondientes a la protección de los sistemas de información que posee.

Pregunta 2: Los empleados del Concejo Distrital de Cartagena respondieron a la pregunta ¿Existe normatividad relativa a la seguridad de los sistemas de información? el 76% respondió que no existe, el 18% no sabe o no responde, el 6% manifiesta que sí.

A los colaboradores que contestaron positivamente, se les requirió expresar cuál es la normatividad, a lo que responden que la entidad no posee normatividad propia, pero existen normas nacionales que lo regulan. Por lo que inferimos que la entidad debe adoptar las normas necesarias para regular lo concerniente a la seguridad de los sistemas de información.

A la pregunta número 3, ¿La entidad no posee procedimientos relativos a la seguridad de la información? como lo manifestaron el 65% de los encuestados, un 29% no sabe o no responde y un 6% dice que existen los procedimientos, se les evalúa acerca de los tipos de procedimiento a lo que ellos responden que algunos han creado sus contraseñas para los equipos, tienen llave de la oficina, pero procedimientos por escrito y sensibilizados por la alta dirección no posee la entidad.

Ante la pregunta N° 4 ¿Si existe un responsable de las políticas, normas y procedimientos? 12 de los encuestados manifestaron que no existe mientras 5 no sabe o no responde.

Pregunta N° 5: ¿La entidad no existen mecanismos para la comunicación a los usuarios de las normas? De acuerdo al 82% de los encuestados el 18% restante no sabe o no responde.

Esto denota la falta de comunicación de las normas por parte de la alta dirección con los usuarios lo que hace difícil tener claridad acerca de que normas que existen en la corporación, como es el manejo de la seguridad y que procedimientos deben seguir para proteger la información. A la pregunta ¿Si existen controles regulares para verificar la efectividad de las políticas? El 71 % de los encuestados manifiesta que en la entidad no existen controles regulares para verificar la efectividad de las políticas de seguridad, se entrevistó al ingeniero de sistemas (contratista) y manifestó que no existe ningún tipo de control que además no ha podido diseñar ni implementar ninguno porque posee contratos temporales que no le permite realizar una labor efectiva en el área.

9.5.2. Organización de la Seguridad

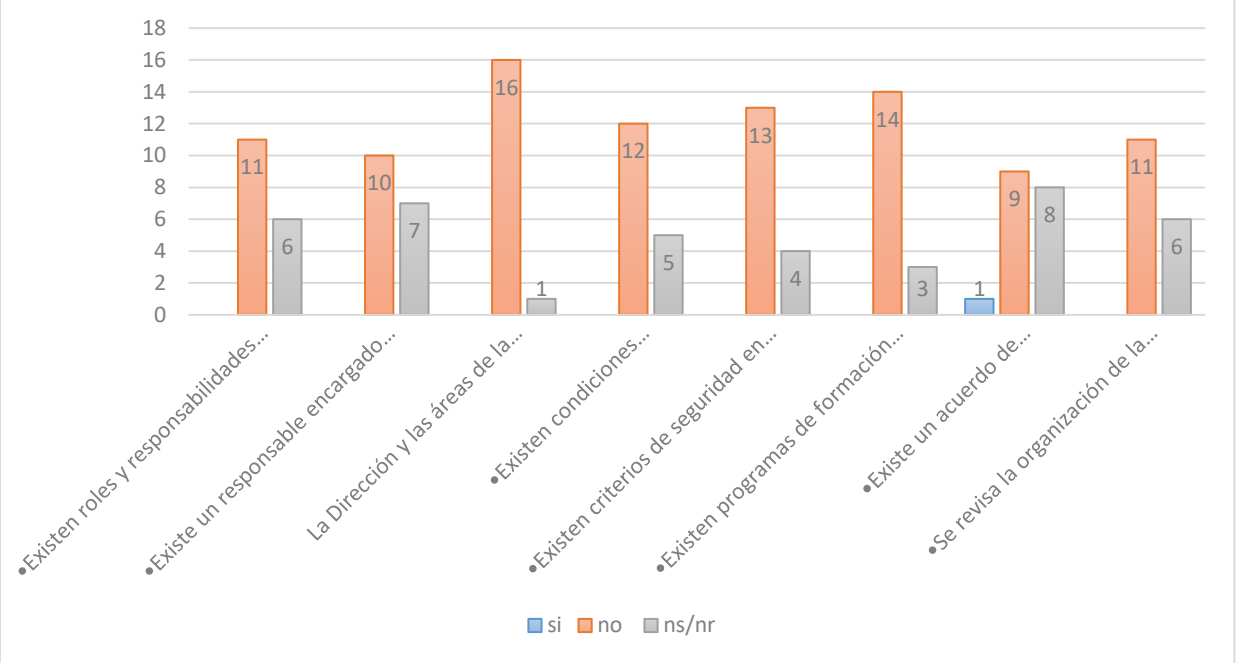
Para la Dimensión organización de la seguridad se formularon 8 preguntas que permitirán conocer las responsabilidades en la seguridad de la información, como se accesa, como se gestiona y se comunica está dentro de la organización

Tabla N° 23. Resultados Dimensión Organización de la Seguridad

Preguntas	si	%	no	%	ns/nr	%
7. Existen roles y responsabilidades definidos para las personas implicadas en la seguridad	0	0%	11	65%	6	35%
8 Existe un responsable encargado de evaluar la adquisición y cambios de SI	0	0%	10	59%	7	41%
9. La Dirección y las áreas de la Organización participa en temas de seguridad	0	0%	16	94%	1	6%
10 Existen condiciones contractuales de seguridad con terceros y outsourcing	0	0%	12	71%	5	29%
11 Existen criterios de seguridad en el manejo de terceras partes	0	0%	13	76%	4	24%
12 Existen programas de formación en seguridad para los empleados,	0	0%	14	82%	3	18%
13. Existe un acuerdo de confidencialidad de la información que se accesa.	1	6%	9	53%	8	47%
14. Se revisa la organización de la seguridad periódicamente por una empresa externa	0	0%	11	65%	6	35%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas.

Grafico N° 10. Dimensión Organización de la Seguridad



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas.

En la tabla N° 23 y el Gráfico número 10 se pueden observar los resultados obtenidos en la dimensión organización, en la pregunta ¿Existen roles y responsabilidades definidos para las personas? En la entidad no existen roles ni responsabilidades definidas para las personas implicadas en la seguridad de los sistemas de información ni de la información. Para la seguridad de la entidad se cuenta con un servicio de vigilancia privada que suministra la Alcaldía de la ciudad y consiste en dos vigilantes uno nocturno y uno diurno, existe un sistema de cámaras en los pasillos que lo administra un funcionario en provisionalidad, hay que recalcar que hay cámaras que no funcionan.

Para la pregunta ¿Existe un responsable encargado de evaluar la adquisición y cambios de SI? En el Concejo Distrital de Cartagena no existe un responsable encargado de evaluar la adquisición y cambios de sistemas de información de acuerdo a los manifestado por el 59% de los encuestados, existen dos sistemas de información llamados SAFE y ZEUS los cuales no están integrados entre si y son llevado por los funcionarios en planta.

A la pregunta ¿La y las áreas de la organización participa en temas de seguridad? En el Concejo Distrital de Cartagena la y las áreas de la organización no participan en temas de seguridad de la información tal como lo manifestaron el 94% de los encuestados el 6% no sabe o no responde. No se han realizado campañas de sensibilización, ni se conocen que medidas aplicar en caso de una violación a la seguridad.

Se les pregunto ¿Si existen condiciones contractuales de seguridad con terceros y outsourcing? Actualmente la entidad no posee ningún tipo de contrato de seguridad con terceros, ni outsourcing de acuerdo a lo manifestado por el 71% de los encuestados, el 29% restante no sabe o no responde.

De acuerdo a lo manifestado por los encuestados, la entidad solo realizo un contrato a un técnico de sistemas una vez finalizado el contrato por prestación de servicios el cual fue por 5 meses, no se realizó ningún tipo de contrato de seguridad para los sistemas de información.

Sobre ¿Si existen criterios de seguridad en el manejo de terceras partes? El 76% de los encuestados infiere que no hay criterios de seguridad en el manejo de terceras partes mientras el 24% no sabe o no responde, esto permite tener claridad acerca de que no existen medidas de protección de la información para terceras personas ajenas a la institución., lo que podía afectar el manejo de la información, y si Existen programas de formación en seguridad para los empleados manifestaron que no existe ningún tipo de programas de formación en seguridad para los empleados de acuerdo a lo manifestado por el 82% de los empleados encuestados en el Concejo Distrital de Cartagena, el 18% restante no sabe o no responde.

Es necesario que la entidad diseñe programas de formación en seguridad de la información para los empleados.

Igualmente, No existe ningún acuerdo de confidencialidad de la información de acuerdo al 50% de los encuestados, el 44% no sabe o no responde, el 6% que corresponde al contratista del área de sistemas afirma que si, el manifiesta que en la cláusula de todos los contratos de prestación de servicios existe una específica de confidencialidad de la información que utilicen los contratistas para el desarrollo de sus servicios.

Es necesario realizar un análisis acerca de los acuerdos de confidencialidad que deben firmar los empleados de planta incluyendo provisionales o de carrera.

La entidad no revisa la organización de la seguridad en forma periódica con una empresa externa de acuerdo a lo expresado por el 65% de los encuestados, el 35% restante no sabe o no responde de acuerdo a lo consultado en la pregunta número 14.

9.5.3. Dimensión Administración de Activos

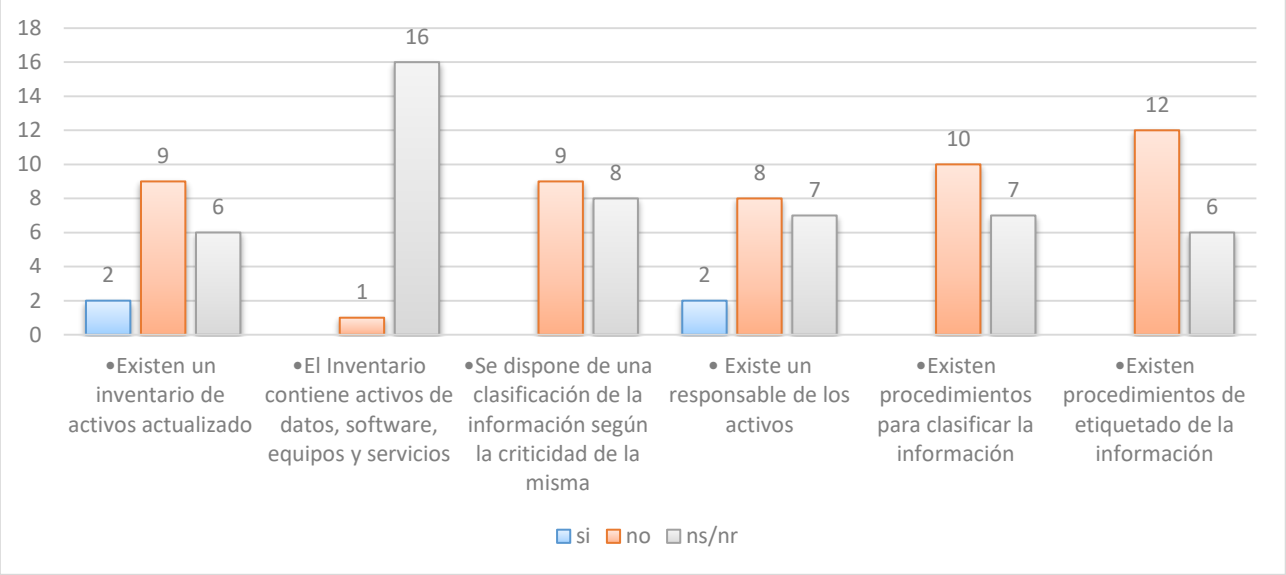
Esta dimensión contiene 6 preguntas que permiten obtener información acerca de la administración de los activos de información del Concejo Distrital de Cartagena.

Tabla N° 24. Resultados Dimensión Administración de Activos

Preguntas	si	%	no	%	ns/nr	%
15 Existen un inventario de activos actualizado	2	12%	9	53%	6	35%
16 El Inventario contiene activos de datos, software, equipos y servicios	0	0%	1	6%	16	94%
17. Se dispone de una clasificación de la información según la criticidad de la misma	0	0%	9	53%	8	47%
18. Existe un responsable de los activos	2	12%	8	47%	7	41%
19 Existen procedimientos para clasificar la información	0	0%	10	59%	7	41%
20. Existen procedimientos de etiquetado de la información	0	0%	11	65%	6	35%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas.

Grafico N° 11. Dimensión Administración de Activos



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas.

Los resultados que se obtienen en esta dimensión son:

De acuerdo a lo expresado por el 53% de los encuestados la entidad no cuenta con un inventario de activos actualizado, el 35% no sabe o no responde la encuesta, mientras el 12% manifiesta que sí.

La funcionaria del área de almacén manifiesta que existe un inventario físico donde se detalla todos los activos de la entidad, el cual se verifica y se constata que existe, pero no está integrado con el área de contabilidad lo que no refleja una adecuada información de los activos existentes dentro de la entidad. La funcionaria entrega el inventario correspondiente a elementos tecnológicos de la entidad. La cual se muestra en la tabla número 24.

Tabla N° 25. Inventario Infraestructura Tecnológica Concejo Distrital De Cartagena

Marca Y Modelo Del Equipo	Ubicación	Año De Compra	Uso	Licencia De Software
IMPRESORA HILARSE JET 1005P	Tercer Piso	2013	Institucional	
TELÉFONO PANASONIC	Primer piso	2010	Institucional	
IMPRESORA EPSON LX 300	Primer piso	2008	Institucional	
IMPRESORA EPSON LX 300	Primer piso	2008	Institucional	
Equipo de cómputo HP COMPAQ L1710	Primer piso	2010	Institucional	Sin Licencia
TELÉFONO MARCA GRAN TREANS COM CABLES	Primer piso	2010	Institucional	
Equipo de cómputo COMPAQ	Segundo piso	2013	Institucional	Sin Licencia
IMPRESORA HP LASER JET P1102W V	Segundo piso	2012	Institucional	
Equipo de Computo MARCA QBEX MOD. 77242971	Segundo piso	2011	Institucional	Sin Licencia
IMPRESORA HP LASER JET P1102W	Segundo piso	2012	Institucional	
IMPRESORA MULTIFUNCIONAL MARCA HP DESK JET F2480	Segundo Piso	2013	Institucional	
IMPRESORA LASER 1102W	Segundo piso	2013	Institucional	
Equipo de Computo MARCA DELL CNOHP889-73731-83Q16WS	Segundo piso	2009	Institucional	Sin Licencia
IMPRESORA HP LASER JET P1005W VND3X24959	Segundo piso	2013	Institucional	
Equipo de Computo MARCA COMPAQ CNC037RDHF	Segundo piso	2013	Institucional	Sin Licencia
Pc Equipo de cómputo HP CNT9356926	Segundo piso	2013	Institucional	Sin Licencia
IMPRESORA LASSER P1102VNB4900322	Segundo piso	2013	Institucional	
TELÉFONO PANASONIC MOD. KX-TS500LX	Segundo piso	2013	Institucional	
Pc equipo de Computo MARCA QBEX MILANO S/FACTU85012514U	Segundo piso	2013	Institucional	Sin Licencia
Pc equipo de Computo MARCA COMPAQ Mxx0280f40	Segundo piso	2013	Institucional	Sin Licencia
Pc Equipo de Computo MARCA COMPAQ CNC037RDH9	Segundo piso	2015	Institucional	Sin Licencia
IMPRESORA LASER HP 1102P VNB4D44855	Segundo piso	2012	Institucional	

Marca Y Modelo Del Equipo	Ubicación	Año De Compra	Uso	Licencia De Software
Equipo de cómputo HP MOD. WB971LTKABM	Segundo piso	2012	Institucional	Sin Licencia
equipo de cómputo marca accer mod.s181 etlrfod001320esebb526	segundo piso	2012	institucional	sin licencia
IMPRESORA MARCA HP LASERRJETP 1102W VNB4D44876	Segundo piso	2012	Institucional	
Equipo de Cómputo MARCA QBEX MILANO 77242971 LCD 19´´SERIE NACRU85002504U	Segundo piso	2013	Institucional	Sin Licencia
IMPRESORA HPLASE JETP P1005 SERIE UND3520646	Segundo piso	2012	Institucional	
Equipo de EQUIPO DE COMPUTO MARCA ACCER MOD SNID RE. 13205891885	Segundo piso	2010	Institucional	Sin Licencia
Equipo de Computo Equipo de Computo MARCA COMPAQ SERIE CNC037RTGY	Segundo piso	2010	Institucional	Sin Licencia
IMPRESORA HP LASERJET DOD. 1102W SERIE VNB4G03868	Segundo piso	2012	Institucional	
TELÉFONO MARCA PANASONIC SERIE 3HBK1442599	Segundo piso	2011	Institucional	
Equipo de Computo MARCA COMPAQ SERIE CNT12VCL4	Segundo piso	2013	Institucional	Sin Licencia
IMPRESORA MARCA HP JET P1102W SERIE VNMU4D44854	Segundo piso	2010	Institucional	
Equipo de Computo MARCA HP V181ES SERIE CNT935691D	Primer piso	2011	Institucional	Sin Licencia
IMPRESORA HP LASER JET P1102W SERIE SERIAL VNB4L69629	Primer piso	2012	Institucional	
EXTENSIÓN 32B VARIOS CONECTORES	Primer piso	2013	Institucional	
IMPRESORA HP F2280 SERIE RB683-64001	Primer piso	2011	Institucional	
EQUIPO DE COMPUTO HACER MOD.5181HL SERIAL ETLRFOD00L	Primer piso	2012	Institucional	Sin Licencia
IMPRESORA HP.1005 SERIE VNB 3322665	Primer piso	2012	Institucional	
TEL. MARCA PANASONIC	Primer piso	2008	Institucional	

Marca Y Modelo Del Equipo	Ubicación	Año De Compra	Uso	Licencia De Software
EQUIPO DE COMPUTO MARCA COMPAQ SERIE CNT012VKO	Segundo piso	2011	Institucional	Sin Licencia
IMPRESORA MARCA HP LASER JET P1102W SERIE VNB4G03870	Segundo piso	2011	Institucional	
EQUIPO DE COMPUTO MARCA COMPAQ SERIE CNT012VCL2	Segundo piso	2011	Institucional	Sin Licencia
IMPRESORA MARCA HP LASERJET P1102W SERIE VND3H20323	Segundo piso	2011	Institucional	
TELÉFONO MARCA PANASONIC SERIE 3GVK1368852	Segundo piso	2008	Institucional	
EQUIPO DE COMPUTO MARCA HACER SERIE SND13303329785	Segundo piso	2011	Institucional	Sin Licencia
IMPRESORA MARCA LASSER JET P1102W. SERIE NV4K67754	Segundo piso	2011	Institucional	
EQUIPO DE COMPUTO MARCA HP S1931A SERIE 3CQ1132GRP	Tercer piso	2012	Institucional	Sin Licencia
IMPRESORA MARCA HP LASERJET 1102W SERIE VNB4L69629	Tercer piso	2011	Institucional	
EQUIPO DE COMPUTO MARCA HP SERIE PUAV0944002577 SERIAL ENT9366917	Tercer piso	2012	Institucional	Sin Licencia
TELÉFONO MARCA GRAN TREAM	Tercer piso	2009	Institucional	
EQUIPO DE COMPUTO MARCA DELL SERIE COD. BARRA SERIAL-CN00N4927317BG6NRS	Tercer piso	2011	Institucional	Sin Licencia
DISCO DURO PD MARCA SIGALE EXTERNO SERIE NAOCP3LF	Tercer piso	2014	Institucional	Sin Licencia
EQUIPO DE COMPUTO SAMSUNG LCD 15" APROX.	Segundo piso	2013	Institucional	Sin Licencia
EQUIPO DE COMPUTO MARCA HP SERIE ELITE 8300GMT SERIAL 6CM243OMP4	Segundo piso	2010	Institucional	Sin Licencia
DISCO DURO 1TB SERIE 9ZPF2A5500	Segundo piso	2014	Institucional	Sin Licencia
EQUIPO DE COMPUTO MARCA ACCER SERIE 13205889885	Segundo piso	2011	Institucional	Sin Licencia

Marca Y Modelo Del Equipo	Ubicación	Año De Compra	Uso	Licencia De Software
EQUIPO DE COMPUTO MARCA FLATRON LG MOD.L17185 SERIE 608UXXU29570	Segundo piso	2011	Institucional	Sin Licencia
EQUIPO DE COMPUTO MARCA HP SERIE CNT9356918	Segundo piso	2012	Institucional	Sin Licencia
IMPRESORA HP LASER JET P1005 SERIE VND3X24861	Segundo piso	2012	Institucional	
EQUIPO DE COMPUTO MARCA COMPAQ SERIE CNT012VCJG	Segundo piso	2011	Institucional	Sin Licencia
IMPRESORA HP MULTIFUNCIONAL ESCANEADORA SERIE F4480	Segundo piso	2012	Institucional	
EQUIPO DE COMPUTO COMPAQ SERIE CNC037RDJ3	Segundo piso	2011	Institucional	Sin Licencia
IMPRESORA HP LASER JET P1102 SERIE VNB4G03890	Segundo piso	2012	Institucional	
EQUIPO DE COMPUTO MARCA ACCER SND13205929985 SERIE SNID13205929985	Segundo piso	2011	Institucional	Sin Licencia
EQUIPO DE COMPUTO MARCA ACCER SERIE SNID13205929985	Segundo piso	2011	Institucional	Sin Licencia
EQUIPO DE COMPUTO COMPAQ. SERIE CNC37RDHH	Segundo piso	2011	Institucional	Sin Licencia
IMPRESORA HPLASERJET P1102W SERIE UNB30577	Segundo piso	2012	Institucional	
IMPRESORA HP LASSER JET P1102W. SERIE VNB3Q53580	Segundo piso	2012	Institucional	
PORTATIL MARCA COMPAQ	Segundo piso	2012	Institucional	Sin Licencia
IMPRESORA HPLASEJET P1102W SERIE VNAB4G03803	Segundo piso	2011	Institucional	
EQUIPO DE COMPUTO COMPAQ SERIE CNC017U3N8	Segundo piso	2012	Institucional	Sin Licencia
PORTATIL MARCA COMPAQ SERIE 2CE830F3WT	Segundo piso	2012	Institucional	Sin Licencia
IMPRESORA MARCAS LASER JET P1102W SERIE VNB4G03855	Segundo piso	2011	Institucional	
IMPRESORA HP LASER JETP 1102W SERIE VNB3Q575	Segundo piso	2011	Institucional	

Marca Y Modelo Del Equipo	Ubicación	Año De Compra	Uso	Licencia De Software
EQUIPO DE COMPUTO MARCA COMPAQ SERIE 3CQ11326QM	Segundo piso	2012	Institucional	Sin Licencia
IMPRESORA HP LASER JET P1102W SERIE VNB4L89442	Segundo piso	2011	Institucional	
EQUIPO DE COMPUTO MARCA COMPAQ SERIE CNC037RDHG	Segundo piso	2012	Institucional	Sin Licencia
EQUIPO DE COMPUTO MARCA COMPAQ SERIE CNC017Q2V3	Segundo piso	2011	Institucional	Sin Licencia
IMPRESORA MARCA HPLASEJET P1102W SERIE PSAB1034003548	Segundo piso	2011	Institucional	
EQUIPO DE COMPUTO HP SERIE 3CQ132G51	Segundo piso	2012	Institucional	Sin Licencia
IMPRESORA HP LASER JET P1102W SERIE VNB3Q53574	Segundo piso	2012	Institucional	
EQUIPO DE COMPUTO MARCA ACCER SERIE ETLRFOD001133082188526	Segundo piso	2011	Institucional	Sin Licencia
IMPRESORA MARCA HP LASER JET P1102W SERIE VNB4D44850	Segundo piso	2012	Institucional	
EQUIPO DE COMPUTO MARCA HP SERIE CNT9356919	Segundo piso	2011	Institucional	Sin Licencia
IMPRESORA MARCA HP LASER JEP1102W SERIE VNB3Q53601	Segundo piso	2012	Institucional	
EQUIPO DE COMPUTO HP SERIE	Segundo piso	2011	Institucional	Sin Licencia

Fuente. Información Concejo Distrital de Cartagena- visitas y confirmación con inventario consignado en almacén.

En el análisis general del levantamiento de la información realizada en el Concejo:

Tabla N° 26. Tabla General de Recursos Tecnológicos Concejo Distrital de Cartagena.

INFORMACIÓN GENERAL RECURSOS TECNOLÓGICOS		
Por elemento	**Cantidad**	**Observaciones**
PC (equipo de Computo)	44	Todos cuentan con S.O Windows 2007
Impresora	40	Conectadas localmente
Scanner	1	Conectado localmente
Portátil	2	Todos cuentan con S.O Windows 2007

Fuente. Información Concejo Distrital de Cartagena- visitas y confirmación con inventario consignado en almacén.

En la pregunta el inventario contiene activos de datos, software, equipos y servicios el 94% de los encuestados no sabe o no responde, mientras el 6% manifiesta que no. Al revisar el inventario que posee el área de almacén se observa que no están ni activos de datos, ni software, ni servicios, se encuentra detallado los equipos y el hardware, tal como se puede observar en la tabla número 25.

A la pregunta se dispone de una clasificación de la información según la criticidad de la misma. El 53% de los encuestados infiere que no se dispone una clasificación de la información según su criticidad mientras el 47 no sabe o no responde. Al consultar al contratista del área de sistemas y a los diferentes jefes de área responden que no poseen esa información en la entidad, la información no es clasificada de acuerdo a su nivel de riesgo.

Para la pregunta existe un responsable de los activos el 47% de los encuestados no existe un responsable de los activos de la entidad, un 41% no sabe o no responde mientras un 12% infiere que sí. Un 12% afirma que si, manifestando que el responsable de los activos es el director administrativo quien es el jefe responsable del área del almacén, nómina y servicios generales.

A la pregunta 19 ¿Existen procedimientos para clasificar la información? Los encuestados responden no existen procedimientos para clasificar la información de acuerdo al 59% de los encuestados mientras el 41% no sabe o no responde. El área de sistemas no posee ningún tipo de procedimiento, No cuentan con un espacio físico para realizar la labor, solo existe una persona contratada para realizar la función.

Para la pregunta 20 ¿Existen procedimientos de etiquetado de la información? No existen procedimientos para el etiquetado de la información de acuerdo al 67% de los encuestados, mientras el 33% no sabe no responde. Tal como se manifestó en anteriores apartes la entidad no posee procedimientos documentados para el área de sistemas.

9.5.4. Dimensión Seguridad de los R. R. H. H

En la dimensión seguridad de los recursos humanos, con 6 preguntas se pretende mostrar con claridad si los empleados y contratistas del Concejo Distrital de Cartagena tienen claridad de las amenazas a la seguridad de la información, también acerca del mal uso de sus sistemas de información y el procedimiento en caso de incidentes

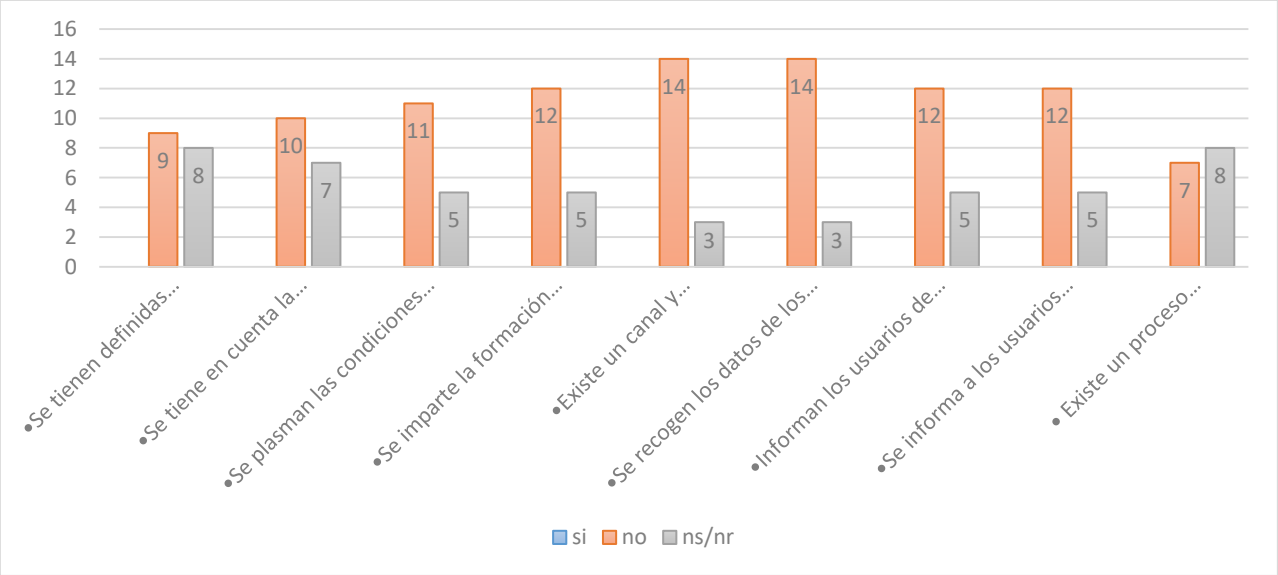
Tabla N° 27. Dimensión Seguridad de los Recursos Humanos.

Pregunta	si	%	no	%	ns/nr	%
21. Se tienen definidas responsabilidades y roles de seguridad	0	0%	9	53%	8	47%
22. Se tiene en cuenta la seguridad en la selección y baja del personal	0	0%	10	59%	7	41%
23. Se plasman las condiciones de confidencialidad y responsabilidades en los contratos	0	0%	11	65%	5	29%
24. Se imparte la formación adecuada de seguridad y tratamiento de activos	0	0%	12	71%	5	29%
25. Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad	0	0%	14	82%	3	18%
26. Se recogen los datos de los incidentes de forma detallada	0	0%	14	82%	3	18%
27. Informan los usuarios de las vulnerabilidades observadas o sospechadas	0	0%	12	71%	5	29%

Pregunta	si	%	no	%	ns/nr	%
28. Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades	0	0%	12	71%	5	29%
29. Existe un proceso disciplinario de la seguridad de la información	0	0%	7	41%	8	47%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas

Grafico N° 12. Dimensión Seguridad de los RR.HH.



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas

En la tabla N° 27 y el Gráfico 12 se observan los resultados de la dimensión seguridad del recurso humano del Concejo Distrital de Cartagena al respecto la pregunta número 21, evalúa si se han definido las responsabilidades y roles de seguridad dentro de la entidad, a lo que del 53% de los encuestados, el 47% no sabe o no responde.

Para el diseño y desarrollo de un modelo de seguridad de los sistemas de información es necesario tener claridad acerca de las personas que harán parte de la seguridad, además de tener una definición adecuada de los roles a cumplir.

Pregunta número 22 ¿Se tienen en cuenta la seguridad en la selección y baja del personal?, En el Concejo Distrital de Cartagena los colaboradores tienen la percepción

de un 59% que no se tienen en cuenta la seguridad en la selección y baja del personal y un 41 % contesta que, si se tienen en cuenta, siendo un aspecto de cuidado, se debe evaluar el personal a contratar, si cumple con las competencias para la vacante a cubrir, crear políticas que ayuden a que el proceso de selección del personal va a asegurar la productividad y va a asegurar que sus procesos sean seguros.

De acuerdo a lo inferido por los encuestados en la pregunta número 23, acerca de si se plasman las condiciones de confidencialidad y responsabilidades en los contratos el Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas, un 69% de los colaboradores expresaron que no se cumple con la política de seguridad de la información, y un 31% expresa que si se está cumpliendo con esta. Se debe establecer una política clara de confidencialidad y responsabilidades en los contratos, donde se estipule que la información para llevar a cabo las funciones estipuladas en el contrato firmado entre las partes es de carácter institucional y por ninguna circunstancia puede ser utilizada para otro medio, una buena estrategia seria implementar un formato de compromiso de confidencialidad.

Los colaboradores del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas, en la pregunta número 24 ¿Se imparte la formación adecuada de seguridad y tratamiento de activos? piensan en un 71% que no se imparte la formación adecuada de seguridad y tratamiento de activos, y en un 29% de ellos expresa que si lo hacen. La entidad debe fortalecer sus procesos para tener asegurada su activo más valioso que es la información, realizar una matriz de riesgos priorizando sus riesgos y amenazas.

Para la pregunta 25 donde se evalúa si existe un canal y procedimientos claros a seguir en caso de incidente de seguridad. Los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas, opinan en un 82% que no se existe un canal de procedimientos claros a seguir en caso de incidente de seguridad, y en un 18% expresa que, si los conoce, se puede concluir que no existe o no lo conocen, la organización debe establecer las pautas de actuación en el caso de incidentes y definir las responsabilidades.

Para la pregunta 26 acerca de que si, ¿Se recogen los datos de los incidentes de forma detallada? Los empleados del Concejo Distrital de Cartagena en las áreas de

Financiera, Administrativa, Secretaria General y Contratista de Sistemas, opinan en un 82% que no se recogen datos de los incidentes y en un 18 % de los trabajadores expresa que si, además de establecer las pautas para actuar en caso de incidentes se deben tener claros los riesgos y las amenazas a las cuales está expuesta la organización. En todo este proceso se debe de involucrar a todos los miembros de la organización para concientizar al personal y crear una cultura de seguridad de la información.

De acuerdo a la pregunta 27 si se informan los usuarios de las vulnerabilidades observadas o sospechadas, los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas, manifiestan en un 71% que no informan de las vulnerabilidades observadas a los usuarios y en un 29 % opina que esto si se realiza. En el análisis de riesgos y amenazas que se deben implementar se debe tener en cuenta las vulnerabilidades porque afecta la confidencialidad, integridad y disponibilidad de los sistemas.

Para la pregunta 28 ¿Se evalúa si se informan a los usuarios de que no deben, bajo ninguna circunstancia probar las vulnerabilidades? a lo que los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas, manifiestan en un 71% que no informan de las vulnerabilidades, ni como probarlas y en un 29 % opina que esto si se realiza, se debe de analizar en análisis y valoración de la vulnerabilidad encontrada, socializarla con todos sus colaboradores.

Y por último en el ítem 29 se les pregunta que si existe un proceso disciplinario de la seguridad de la información los colaboradores del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas, en un 53% coinciden en que SI existe un proceso disciplinario de la seguridad de la información y en un 47% opina que no, la entidad debe realizar contar con un proceso disciplinario y capacitar a todos los colaboradores para que ellos conozcan cuales son las violaciones a la seguridad de la información, políticas de fallas y cuales con las acciones que se toman por las diferentes violaciones.

9.5.5. Dimensión Seguridad Física y del Ambiente

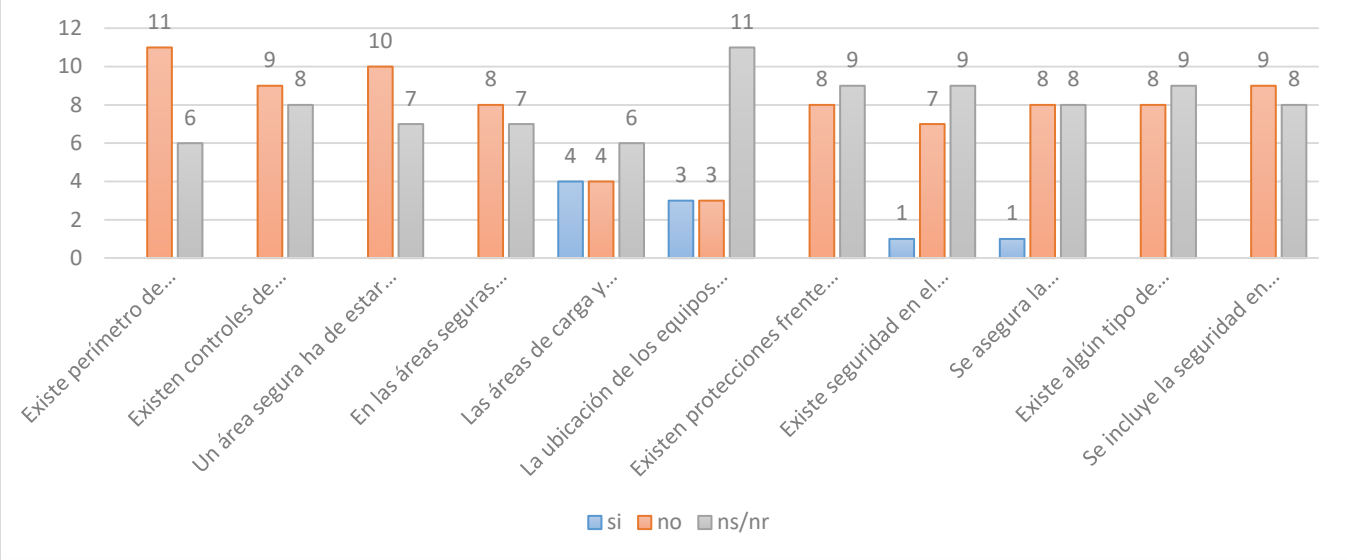
En la dimensión seguridad física y del ambiente la cual contiene 11 preguntas, se espera poder conocer la información acerca de Seguridad física y perimetral, control de entradas, seguridad de los equipos se pretende mostrar con claridad si los empleados, contratistas y usuarios del Concejo Distrital de Cartagena tienen claridad de las amenazas a la seguridad de la información, también acerca del mal

Tabla N° 28. Resultados Dimensión Seguridad Física y del ambiente

Pregunta	si	%	no	%	ns/nr	%
30. Existe perímetro de seguridad física (una pared, puerta con llave).	0	0%	11	65%	6	35%
31. Existen controles de entrada para protegerse frente al acceso de personal no autorizado	0	0%	9	53%	8	47%
32. Un área segura ha de estar cerrada, aislada y protegida de eventos naturales	0	0%	10	59%	7	41%
33. En las áreas seguras existen controles adicionales al personal propio y ajeno	0	0%	8	47%	7	41%
34. Las áreas de carga y expedición están aisladas de las áreas de SI	4	24%	4	24%	6	35%
35. La ubicación de los equipos está de tal manera para minimizar accesos innecesarios.	3	18%	3	18%	11	65%
36. Existen protecciones frente a fallos en la alimentación eléctrica	0	0%	8	47%	9	53%
37. Existe seguridad en el cableado frente a daños e intercepciones	1	6%	7	41%	9	53%
38. Se asegura la disponibilidad e integridad de todos los equipos	1	6%	8	47%	8	47%
39. Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente	0	0%	8	47%	9	53%
40. Se incluye la seguridad en equipos móviles	0	0%	9	53%	8	47%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas

Grafico N° 13. Dimensión Seguridad Física y del ambiente



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas

Para la pregunta número 30 donde se les pregunta su existe un perímetro de seguridad física los colaboradores del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas, en un 65% expresa en que no existe perímetro de seguridad física (una pared, puerta con llave), y en un 35% no sabe o no responde, la entidad debe definir y usar los perímetros de seguridad física para proteger sus áreas que contengan información crítica y todas las instalaciones que manejen su activo más importante que es la información.

La pregunta 31: ¿Existen controles de entrada para protegerse frente al acceso de personal no autorizado?, Los colaboradores del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas, en un 53% contestaron en la encuesta que si cuentan con los controles de entrada para protegerse frente al acceso de personal no autorizado y en un 47% de los colaboradores siente y piensa que están inseguros, que cualquier ciudadano puede ingresar principalmente cuando se hacen sesiones de los concejales, se debe realizar un control de acceso a las áreas más sensibles para asegurar que solamente ingrese personal autorizado.

Los colaboradores del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas, a la pregunta número 32 un área segura ha de estar cerrada, aislada y protegida de eventos naturales en un 59% contestaron en la encuesta que SI, tienen un área segura cerrada, aislada y protegida de eventos naturales y en un 41% expresa que NO, se le debe aplicar controles de seguridad física a todas las oficinas que comprende el edificio donde funciona el Concejo y que estas cuentan con protección física contra desastres naturales, ataques maliciosos o accidentes.

En las áreas seguras existen controles adicionales al personal propio y ajeno correspondiente a la pregunta numero 33 los colaboradores del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas, en un 53%, expresaron si, cuentan con controles adicionales para el ingreso a las áreas seguras y en un 47% manifiesta que no existen tales controles. La entidad debe pormenorizar controles en el acceso, diseñar y sensibilizar a todos los colaboradores en todos estos controles y aplicar procedimientos de trabajo seguro en áreas seguras para no exponer la información sensible.

La pregunta número 34 que trata de acerca si las áreas de carga y expedición están aisladas de las áreas de SI, los colaboradores del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas, en un 43%, consideran que las áreas de carga y expedición están aisladas de las áreas SI, en un 29% expresa que estas áreas no están aisladas y un 28% opina que no sabe, no responde, se evidencia de manera clara que los trabajadores no tienen claro cuáles son las áreas sensibles, se debe realizar el diseño de los controles de acceso, proteger las áreas de procesamiento de información para evitar el acceso no autorizado.

¿La ubicación de los equipos está de tal manera para minimizar accesos innecesarios? que se infiere en la pregunta número 35, Los colaboradores del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas, en un 65%, no sabe o no responde sobre si la ubicación de los equipos se encuentra diseñada para minimizar accesos innecesarios, en un 18% expresa que no, y un 17% de ellos opina que sí, la entidad debe de distribuir los espacios de las oficinas en busca que ubicar bien los equipos para evitar o disminuir en lo posible los

riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.

En la pregunta 36 se busca conocer si existen protecciones frente a fallos en la alimentación eléctrica a lo que colaboradores del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas, en un 53% no sabe o no responde en que si existen protecciones antes las fallas eléctricas y un 47% expresa que estas protecciones NO existen, se recomienda a la mesa directiva del Concejo de Cartagena tomar acciones en busca de proteger los equipos contra las fallas de energía y cualquier interrupción por fallas en el suministro.

En la pregunta número 37 se busca conocer si existe seguridad en el cableado frente a daños e intercepciones, los colaboradores del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas, en un 53% expresa que si existen controles en la seguridad del cableado, un 41% opina que estos controles NO existen y un 6% no sabe o no responde, se deben establecer controles en el cableado de potencia y de telecomunicaciones que lleva los datos de información, protegerlos de cualquier interceptación, interferencia o daño. Para la información se asegura la disponibilidad e integridad de todos los equipos de la pregunta 38, se asegura la disponibilidad e integridad de todos los equipos los colaboradores del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas, en un 6% no sabe o no responde sobre si se asegura la disponibilidad e integridad de todos los equipos, coinciden en un 47% de los trabajadores que, si y no se asegura, evidenciándose que no se tienen claros cuales son estos controles, se deben tomar acciones claras y concretas sobre el mantenimientos de los equipos para asegurar su disponibilidad e integridad de forma continua.

En la pregunta 39 si existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente los colaboradores del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas, en un 53% manifiesta que si existe controles de seguridad para los equipos retirados o que se ubican exteriormente, y un 47% de los colaboradores expresa que estos controles de seguridad no existen, se debe establecer un proceso que despliegue las medidas de seguridad a todos los equipos que son retirados y/o los que están fuera de las

instalaciones, teniendo en cuenta la matriz de riesgos y peligros a los cuales están expuestos estos equipos por estar fuera de las áreas seguras y que no cuentan protección física. Se incluye la seguridad en equipos móviles en la pregunta número 40 los colaboradores del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas, en un 53% expresa que no hay seguridad para la utilización de equipos móviles y un 47% opina que este no sabe o no responde si se incluye seguridad para el manejo de la información. Se debe verificar todos los elementos que contenga medios de almacenamiento y/o diseñar un protocolo de manejo de equipos móviles dentro de las instalaciones del Concejo.

9.5.6. Dimensión Gestión de Comunicaciones y Operaciones

En la dimensión gestión de comunicaciones y operaciones se evalúan 22 ítems en donde se espera evaluar la operación de los recursos de información del Concejo Distrital de Cartagena.

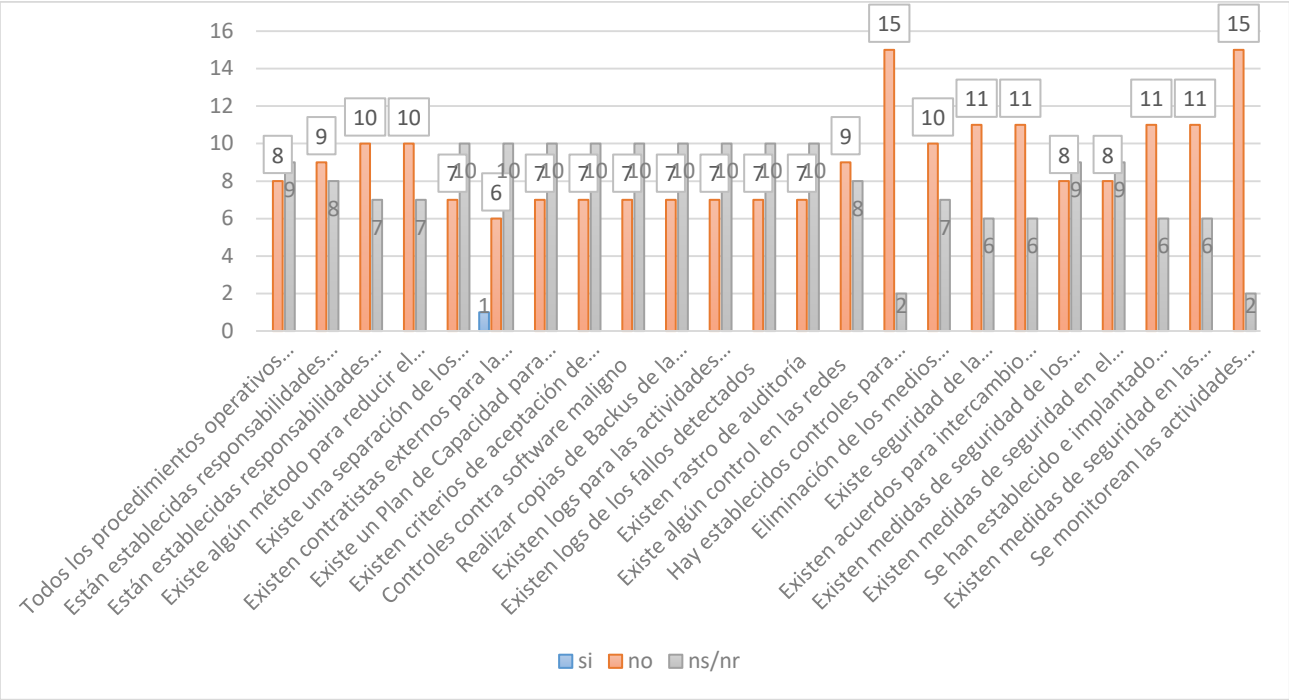
Tabla N° 29. Resultados Dimensión Gestión de Comunicaciones y Operaciones.

Pregunta	si	%	no	%	ns/nr	%
41. Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados	0	0%	8	47%	9	53%
42. Están establecidas responsabilidades para controlar los cambios en equipos	0	0%	9	53%	8	47%
43. Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad	0	0%	10	59%	7	41%
44. Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas	0	0%	10	59%	7	41%
45. Existe una separación de los entornos de desarrollo y producción	0	0%	7	41%	10	59%
46. Existen contratistas externos para la gestión de los Sistemas de Información	1	0%	6	35%	10	59%

Pregunta	si	%	no	%	ns/nr	%
47. Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento	0	0%	7	41%	10	59%
48. Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones	0	0%	7	41%	10	59%
49. Controles contra software maligno	0	0%	7	41%	10	59%
50. Realizar copias de Backus de la información esencial para el negocio	0	0%	7	41%	10	59%
51. Existen logs para las actividades realizadas por los operadores y administradores	0	0%	7	41%	10	59%
52. Existen logs de los fallos detectados	0	0%	7	41%	10	59%
53. Existen rastro de auditoría	0	0%	7	41%	10	59%
54. Existe algún control en las redes	0	0%	9	53%	8	47%
55. Hay establecidos controles para realizar la gestión de los medios informáticos.(cintas, discos, removibles, informes impresos)	0	0%	15	88%	2	12%
56. Eliminación de los medios informáticos. Pueden disponer de información sensible	0	0%	10	59%	7	41%
57. Existe seguridad de la documentación de los Sistemas	0	0%	11	65%	6	35%
58. Existen acuerdos para intercambio de información y software	0	0%	11	65%	6	35%
59. Existen medidas de seguridad de los medios en el tránsito	0	0%	8	47%	9	53%
60. Existen medidas de seguridad en el comercio electrónico.	0	0%	8	47%	9	53%
61. Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada	0	0%	11	65%	6	35%
62. Existen medidas de seguridad en las transacciones en línea	0	0%	11	65%	6	35%
63. Se monitorean las actividades relacionadas con la seguridad	0	0%	15	88%	2	12%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas

Grafico N° 14. Dimensión Gestión de Comunicaciones y Operaciones



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas

En la tabla N° 29 y el Gráfico 14 las investigadoras indagamos acerca de los procedimientos y responsabilidades de operación de la información, en la pregunta 41 se inquiere acerca de que si todos los procedimientos operativos identificados en la política de seguridad han de estar documentados, Los colaboradores del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas, en un 53% expresa que no sabe o no responde si todos los procedimientos operativos identificados en la política de seguridad han de estar documentados y un 47% de los trabajadores dice que estos no han sido documentados. La entidad debe de asegurar el correcto funcionamiento de las instalaciones de procesamiento de la información y debe diseñar un procedimiento de operación este debe ser difundido en todos los colaboradores.

En la Pregunta 42: ¿Están establecidas responsabilidades para controlar los cambios en equipos en El Concejo Distrital de Cartagena? A lo que los encuestados manifiestan que no tiene establecidas las responsabilidades para controlar cambios en los diferentes equipos tal como responde el 53% de los encuestados, 43% no sabe o no responde. La

entidad al no poseer en la planta un área del más alto nivel encargada del área de sistema no ha establecido ningún tipo de responsabilidad sobre los equipos que utilizan para el desarrollo de sus funciones. Se debe diseñar y socializar un control de cambio en los equipos, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.

Las responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad no están establecidas, de acuerdo al 59% no se han establecido responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad, el 41% restante no sabe o no responde.

Se indago en la pregunta 43 si están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad a lo que el 59% de los empleados encuestados en la entidad manifiesta que no se han establecido responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad, el 41% restante no sabe o no responde.

Sobre si existe algún método para reducir el mal uso accidental o deliberado de los sistemas ítem número 44, los encuestados manifiestan que no existe ningún método que permita reducir el mal uso accidental o deliberado de los sistemas de la entidad de acuerdo al 59% de los empleados encuestados, un 41% no sabe o no responde. Ningún colaborador de los encuestados sabe que método debe seguir en el caso que se le presente una contingencia en los sistemas, exponiéndose a la perdida de información sensible para la entidad. Para la pregunta 45 si ¿Existe una separación de los entornos de desarrollo y producción? El 59% de los empleados encuestados manifiesta que no existe separación de los entornos de desarrollo con los de producción, el 41% no sabe o no responde. La entidad al no tener programadores web no tiene un área de desarrollo, solo poseería en dado caso el entorno de producción donde se ejecutan las aplicaciones que utilizan los usuarios finales.

En la pregunta 46 ¿no existen contratistas externos para la gestión de los Sistemas de Información? el 59% no sabe o no responde a la pregunta de que, si existen contratistas externos para la gestión de los sistemas de información, el 35% dice que no y un 6% manifiesta que sí, el empleado infiere que existe un ingeniero por prestación de servicios que es el que cuando se cae la red soluciona el problema.

Se indago en el ítem 47 si existe un plan de capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento, un 59% de los encuestados no sabe o no responde si existe un plan de capacidad para asegurar la adecuada capacidad de proceso y almacenamiento de la información mientras un 41% piensa que no existe como tal un plan para asegurar el proceso y almacenamiento de la información.

En la pregunta 48 acerca si existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones, los encuestados respondieron no sabe o no responde el 59% y un 41% que no a la pregunta existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones, lo que demuestra que en la entidad no se ha creado procedimientos para realizar actualizaciones a los sistemas.

Se pregunta en el ítem 49 si existen Controles contra software maligno, El 59% no sabe o no responde si existen controles contra software maligno el 41% dice que no, en dialogo con los encuestados manifiestan que la mayoría de los computadores de la entidad se encuentran infectados de virus, están lentos y no son adecuados para el tratamiento de la información.

Se les pregunta a los empleados en el ítem 50 si se realizan copias de Backups de la información esencial para el negocio, el 59% de los encuestados no sabe o no responde si se realizan copias de backups de la información esencial para el negocio, el 41% piensa que no, a los encuestados se les indago que como protegían la información algunos manifestaron que la imprimen y la guardan por lo que no hay copia magnética si se llega a perder la información.

Se indaga si existen logs para las actividades realizadas por los operadores y administradores, el 41% manifiesta que no existen y el 59% que no sabe o no responde. Ítem 52 los encuestados no saben o no responde el 59% de los encuestados si existen logs para los fallos detectados, el 41% manifiesta que no. Se deben es necesario proteger la integridad de la información.

Si existen rastros de auditoria para la pregunta 53, no existen rastros de auditoria de acuerdo al 59% de los encuestados, un 41% no sabe o no responde la pregunta.

Los funcionarios manifiestan que solo hasta el año pasado la oficina de control interno realizo un informe sobre el funcionamiento del sistema.

Un 53% de los encuestados manifiesta que no existe algún control en las redes de la entidad, el 47% no sabe o no responde, de acuerdo a lo que se le pregunto en el ítem 54. Al no estar asignado un funcionario de planta no existe un control en las redes de la entidad lo que genera un riesgo alto de sufrir fallos en ella. En la entidad no hay establecido controles para realizar la gestión de los medios informáticos. (Cintas, discos, removibles, informes impresos) de acuerdo al 88% de los encuestados. Un 12% no sabe o no responde. De acuerdo a lo inquirido en la pregunta 55.

No existe ningún tipo de política que permita proteger la información que se encuentra en custodia por parte de los funcionarios del Concejo Distrital de Cartagena, la eliminación de los medios informáticos no se realiza con medidas de protección de acuerdo al 59% de los encuestados, lo que permitiría que la información sensible la pueda obtener fácilmente otras personas, tal como se les pregunto en el ítem 56.

En el ítem 57 se indago si existe seguridad en la documentación de los sistemas, a lo que los encuestados infieren en que no existe seguridad de la documentación de los sistemas de acuerdo al 65% de los encuestados, mientras el 35% no sabe o no responden. No existen acuerdos para el intercambio de información y software de acuerdo al 65% de los encuestados, el 35% no sabe o no responde. De acuerdo a lo consultado en el ítem 58. En la pregunta número 59 se indaga si existen medidas de seguridad de los medios en el tránsito a lo que los encuestados manifiestan que no existen medidas de seguridad de los medios en tránsito de acuerdo al 47% de los encuestados, el 53% no sabe o no responde.

En la pregunta número 60 se investiga si existe existen medidas de seguridad en el comercio electrónico, el 53% de los encuestados no sabe o no responde si existen medidas de seguridad en el comercio electrónico, el 47% manifiesta que no existen estas medidas. Los empleados pueden utilizar las redes para realizar actividades y comercio electrónico desde sus computadores generando riesgos de virus. Se indaga en la pregunta 61 si se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada, el 63% de los encuestados manifiesta que no se han establecido e implantado medidas para proteger la confidencialidad e integridad de la información publicada en la entidad, el 35% no sabe o no responde.

La pregunta 62 si existen medidas de seguridad en las transacciones en línea los encuestados responden que no existen medidas de seguridad en las transacciones en línea que se realizan en la entidad, de acuerdo al 65% de los encuestados, el otro 35% no sabe o no responde. Para el ítem 63, ¿Se monitorean las actividades relacionadas a la seguridad? No se realiza monitoreo sobre las actividades relacionadas con la seguridad, de acuerdo al 88% de los encuestados, al no existir una persona encargada del área no existe procedimientos de ningún tipo en el área de sistemas y en la seguridad de la información. El 12% de los encuestados restantes no sabe o no responde a la pregunta.

9.5.7. Dimensión Control de Accesos

En la dimensión control de accesos se evalúan 17 ítems donde se podrá observar si se controla que los usuarios autorizados, accedan solo a los recursos a los cuales tiene derecho en el Concejo Distrital de Cartagena.

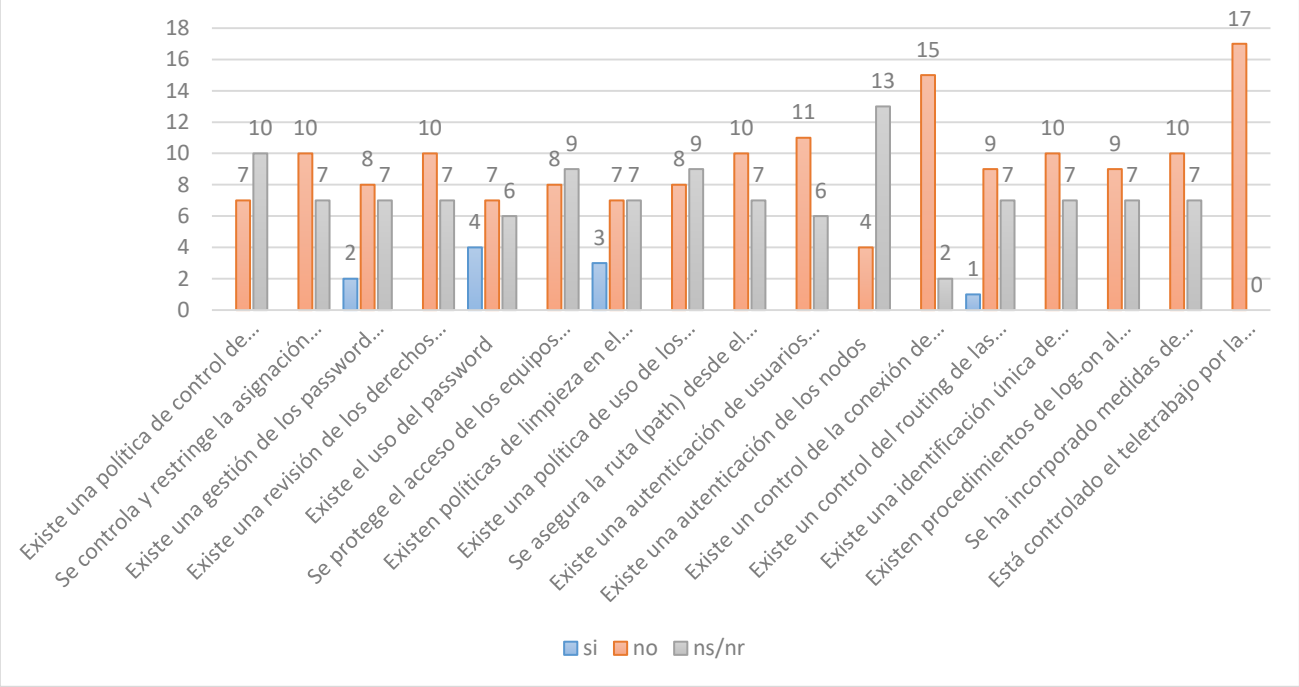
Tabla N° 30. Resultados Dimensión Control De Accesos.

Pregunta	si	%	no	%	ns/nr	%
64. Existe una política de control de accesos	0	0%	7	41%	10	59%
65. Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario	0	0%	10	59%	7	41%
66. Existe una gestión de los password de usuarios	2	12%	8	47%	7	41%
67. Existe una revisión de los derechos de acceso de los usuarios	0	0%	10	59%	7	41%
68. Existe el uso del password	4	24%	7	41%	6	35%
69. Se protege el acceso de los equipos desatendidos	0	0%	8	47%	9	53%
70. Existen políticas de limpieza en el puesto de trabajo	3	18%	7	41%	7	41%

Pregunta	si	%	no	%	ns/nr	%
71. Existe una política de uso de los servicios de red	0	0%	8	47%	9	53%
72. Se asegura la ruta (path) desde el terminal al servicio	0	0%	10	59%	7	41%
73. Existe una autenticación de usuarios en conexiones externas	0	0%	11	65%	6	35%
74. Existe una autenticación de los nodos	0	0%	4	24%	13	76%
75. Existe un control de la conexión de redes	0	0%	15	88%	2	12%
76. Existe un control del routing de las redes	1	6%	9	53%	7	41%
77. Existe una identificación única de usuario y una automática de terminales	0	0%	10	59%	7	41%
78. Existen procedimientos de log-on al terminal	0	0%	10	59%	7	41%
79 Se ha incorporado medidas de seguridad a la computación móvil	0	0%	10	59%	7	41%
80. Está controlado el teletrabajo por la organización	0	0%	17	100%	0	0%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas

Grafico N° 15. Dimensión Control De Accesos



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas

De acuerdo a si existe una política de control de accesos establecida en el ítem 64, El 59% de los encuestados no sabe o no responde si existen políticas para el control de accesos en la entidad, un 41% manifiesta que no. El control de accesos permite proteger la información de usuarios malintencionados lo que garantizara una protección adecuada de la información, al contar con parámetros claves para el acceso a los sistemas de información, por lo tanto, es necesario contar con políticas claras en este tema.

En el ítem 65 se evalúa si se controla y restringe la asignación y uso de privilegios en entornos multi-usuario, a lo que responden que, no se controla ni se restringe la asignación y uso de privilegios en entornos multiusuarios de acuerdo al 59% de los encuestados, el 41% no sabe o no responde. Al no existir políticas, ni procesos y procedimientos de control se deja sin seguridad la información de la entidad.

Si existe una gestión de los password de usuarios de acuerdo al ítem 66, el 47% de los empleados encuestados manifiesta que no existe una gestión de los password de los usuarios, un 41% no sabe o no responde y el 12% manifiesta que si, al consultar el porqué de su respuesta ellos responden que no existe gestión de password, que ellos

tienen contraseña en sus equipos, que la han creado como una medida de autocontrol con el fin de proteger su información. Y tampoco existe una revisión de los derechos de acceso de los usuarios tal como lo manifestaron el 59% de los empleados encuestados, el 41% no sabe o no responde en el ítem 67, al no contar con la oficina de sistemas no existe este tipo de procesos dentro de la entidad.

En relación a que, si existe el uso del password en la pregunta 68, el 41% de los encuestados responde que no existe el uso de contraseñas, un 35% no sabe o no responde y un 24% manifiesta que sí. Como se observa no existe claridad ni conocimiento acerca del uso de password en las personas encuestadas solo 4 personas usan contraseña para el acceso a sus computadores y han sido configuradas por ellos mismos como una medida de autocontrol con el fin de proteger la información que procesan.

En relación a si se protege el acceso de los equipos desatendidos en la pregunta 69 en el Concejo Distrital de Cartagena, no se protege el acceso de los equipos desatendidos de acuerdo al 47% de los encuestados, el 53% no sabe o no responde. La entidad no ha implementado ninguna política para proteger sus equipos sin uso, lo que genera un alto riesgo para la entidad.

Se indaga si existen políticas de limpieza en el puesto de trabajo en el ítem 70 a lo que los encuestados responden, que no existen políticas de limpieza en el puesto de trabajo de acuerdo al 41% de los encuestados, mientras un 41% no sabe o no responde. El 18% de los encuestados afirma que no existen políticas escritas sin embargo hay personas encargadas del aseo de la entidad que limpian las oficinas y la persona asignada al puesto de trabajo trata de mantener el orden.

Existe una política de uso de los servicios de red pregunta número 71, el 53% de los encuestados no sabe o no responde si existe una política de uso de los servicios de red, mientras el 47% de los encuestados dice que no. Lo que denota que la entidad no tiene reglamentado como debe usarse los servicios de red, lo que hace necesario que la entidad regule acerca de las políticas de uso de los servidos de red.

Se pregunta que si se asegura la ruta (path) desde el terminal al servicio en el ítem 72 el 59% de los encuestados responden que no se asegura la ruta desde el terminal de servicio de los sistemas de información, el 41% no sabe o no responde. Las personas

no saben acerca de los directorios, ni los terminales de ruta, la falta de una oficina de sistemas interna dificulta la labor de los funcionarios por lo tanto los trabajos son demorados y la mayoría manuales.

En relación a que si existe una autenticación de usuarios en conexiones externas el ítem 73 se indaga el tema, a lo que los encuestados responden que no existe autenticación de usuarios en conexiones externas de acuerdo al 65% de los encuestados, un 35% no sabe o no responde. Las conexiones externas no son reguladas cualquier persona que obtenga la clave puede conectarse sin hacer ningún tipo de proceso que asegure que la información de la entidad estará protegida. Igualmente se indaga se existe una autenticación de los nodos en la pregunta 74, El 76% de los encuestados no saben o no responden si existe una autenticación de los nodos, mientras un 24% responde que no existe.

La entidad posee un solo servidor para la conexión a internet, los ordenadores no se autentican en la red, de acuerdo al ingeniero de sistemas no se ha realizado este procedimiento. Existe un control de la conexión de redes se pregunta en el ítem 75 a lo que los encuestados responden que no hay control en la conexión de las redes de acuerdo al 88% de los encuestados, no hay un ingeniero de planta que lleve un registro de control acerca de las personas que se conectan diariamente a las redes el 12% no sabe o no responde.

En relación al control del routing de las redes se realiza la pregunta 76, a lo que se responde la entidad no cuenta con un control de routing en las redes de acuerdo al 59% de los encuestados, mientras el 41% no sabe o no responde. Dentro de la norma ISO 27001 es uno de los factores importantes ya que es necesario establecer controles de enrutamiento en las redes para asegurar que las conexiones de los ordenadores y flujos de información no incumplen la política de control de accesos a las aplicaciones de negocio. (Punto 1.4.7).

En relación a si existe una identificación única de usuario y una automática de terminales de acuerdo a los 59% empleados encuestados no existe una identificación única de usuario ni una automática de terminales, el 41% no sabe o no responde a la pregunta.

El ítem 78 pregunta sobre, ¿Existen procedimientos de Log-on al terminal?, a lo que los encuestados responden que no existen procedimientos Log- On al terminal de acuerdo al 59% de los encuestados manifiesta que no existen procedimientos para evitar el ataque de intrusos a los terminales informáticos de la entidad. Un 44% de los encuestados no sabe o no responde lo que indica el poco conocimiento que se tiene acerca de la seguridad de la información en la entidad. La pregunta 79 indaga acerca si se ha incorporado medidas de seguridad a la computación móvil a lo que El 59% de los encuestados manifiesta que no se han incorporado medidas de seguridad en la computación móvil, mientras el 41% no sabe o no responde, esto permite inferir que no hay medidas de seguridad para cualquier equipo móvil que sea utilizado en las instalaciones de la corporación.

El ítem 80 evalúa si está controlado el teletrabajo por la organización y de acuerdo al 100% de los encuestados en la entidad no está controlado el teletrabajo, la entidad no maneja este tipo de contrato, todo se hace de manera presencial dentro de las instalaciones de la entidad.

9.5.8. Dimensión Desarrollo y Mantenimiento de los Sistemas

En la dimensión desarrollo y mantenimiento de los sistemas se evalúan 8 ítems en donde se espera evaluar si la seguridad está implantada en los sistemas de información del Concejo Distrital de Cartagena y si se previene los errores, perdida o modificación o mal uso de las aplicaciones.

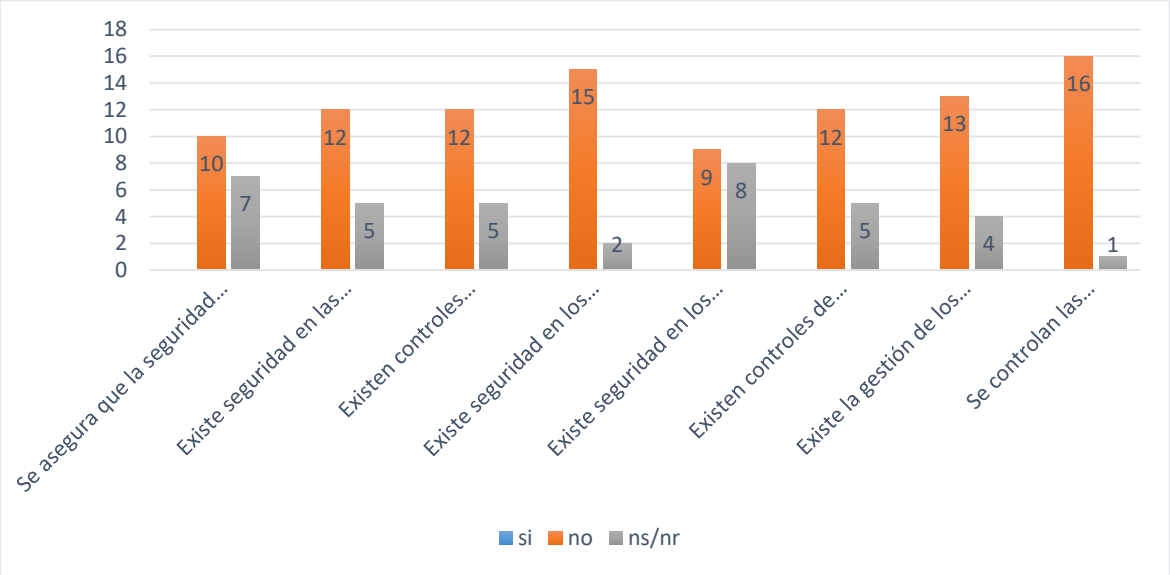
Tabla N° 31. Resultados Dimensión Desarrollo y Mantenimiento

Pregunta	si	%	no	%	ns/nr	%
81. Se asegura que la seguridad está implantada en los Sistemas de Información	0	0%	10	59%	7	41%
82. Existe seguridad en las aplicaciones	0	0%	12	71%	5	29%
83. Existen controles criptográficos.	0	0%	12	71%	5	29%

Pregunta	si	%	no	%	ns/nr	%
84. Existe seguridad en los ficheros de los sistemas	0	0%	15	88%	2	12%
85. Existe seguridad en los procesos de desarrollo, testing y soporte	0	0%	9	53%	8	47%
86. Existen controles de seguridad para los resultados de los sistemas	0	0%	12	71%	5	29%
87. Existe la gestión de los cambios en los SO.	0	0%	13	76%	4	24%
88. Se controlan las vulnerabilidades de los equipos	0	0%	16	94%	1	6%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas

Grafico N° 16. Dimensión Desarrollo y Mantenimiento



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas

En la tabla número 31 y en la gráfica número 16 se evalúa la dimensión desarrollo y mantenimiento de los sistemas de información, mostrando los diferentes resultados de acuerdo a la percepción de los encuestados, para la pregunta 81 se asegura que la seguridad está implantada en los Sistemas de Información, en la encuesta realizada a los empleados de la Dirección administrativa, financiera, secretaria general y contratista de sistemas, se evidencia que no se asegura que la seguridad este implantada en los

sistemas de información de acuerdo a lo que manifiesta el 59% de los empleados del área, el 41% restante no sabe o no responde. Esta situación genera una amplia incertidumbre, debido a que, sin seguridad de los sistemas de información, el riesgo de una pérdida de esta se hace más sensible, lo que podría generar consecuencias catastróficas.

Acerca de si existe seguridad en las aplicaciones la pregunta 82, los empleados aseguran que no existe seguridad en las aplicaciones, de acuerdo a lo manifestado por el 71% de los encuestados, el 29 restante no sabe o no responde. Ninguna aplicación o sistema de información que utiliza la entidad cuenta con la seguridad necesaria para la protección de la información.

A través de los controles criptográficos la entidad puede contar con dispositivos, con información confidencial que se encuentra fuera de la organización, se cuenta con un servidor de archivos con una carpeta en la que todos los trabajadores tienen acceso y otras tantas funciones con las que no se cuentan en la entidad de acuerdo al 71% de los encuestados, un 29% no sabe o no responde. Los controles criptográficos permiten proteger la información cuando esta sale de los límites de la empresa en base a la Norma ISO 27001.

Para la pregunta número 84 ¿Existe seguridad en los ficheros de los sistemas? no existe seguridad en los ficheros de los sistemas, de acuerdo al 88% de los encuestados, lo que no permite garantizar la confidencialidad y la integridad de la información almacenada en estos ficheros, El 12% de los encuestados restantes no sabe o no responde.

El ítem 85 evalúa si existe seguridad en los procesos de desarrollo, testing y soporte. La entidad no ha desarrollado ningún tipo de procesos de desarrollo, testing ni soporte, por lo tanto, no tiene procedimientos establecidos para verificar que propuestas de cambio y desarrollo sean revisadas para verificar que no comprometen la seguridad del sistema o del entorno operativo, tal como lo manifiesta el 53% de los encuestados, el 47% restante no sabe o no responde.

En relación, así existen controles de seguridad para los resultados de los sistemas la pregunta 86 indaga sobre el tema a lo que los encuestados, lo cual manifiestan que no

existe ningún tipo de controles de seguridad para los resultados de los sistemas de acuerdo al 71% de los encuestados, el 29% no sabe o no responde. El ítem 87 es en relación a si existe la gestión de los cambios en los SO, el 76% de los encuestados manifiesta que no existe la gestión de los cambios en los sistemas de SO, el 24% no sabe o no responde. La gestión de cambios es necesaria debido a la actualización que debe realizarse a los servidores, si no existe una gestión de cambios adecuada se coloca en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas de la empresa.

Se controlan las vulnerabilidades de los equipos es el ítem 88, para los encuestados la entidad no controla la vulnerabilidad de los equipos de acuerdo al 94%, un 6% no sabe o no responde. Si la entidad no realiza un control adecuado de las vulnerabilidades coloca en alto riesgo la entidad al quedar expuesto a cualquier ataque.

9.5.9. Dimensión Administración de Incidentes de los Sistemas

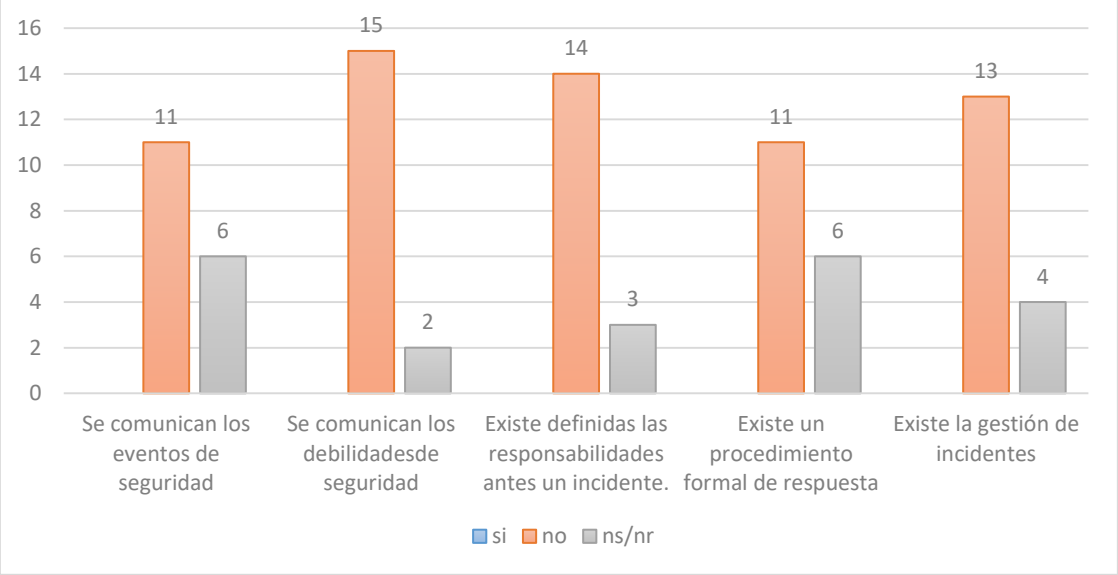
En la dimensión desarrollo y manteamiento de los sistemas se evalúan 8 ítems en donde se espera evaluar si la seguridad está implantada en los sistemas de información del Concejo Distrital de Cartagena y si se previene los errores, perdida o modificación o mal uso de las aplicaciones.

Tabla N° 32. Resultados Dimensión Administración de Incidentes

Pregunta	si	%	no	%	ns/nr	%
89. Se comunican los eventos de seguridad	0	0%	11	65%	6	35%
90. Se comunican los debilidades de seguridad	0	0%	15	65%	2	12%
91. Existe definidas las responsabilidades antes un incidente.	0	0%	14	65%	3	18%
92. Existe un procedimiento formal de respuesta	0	0%	11	65%	6	35%
93. Existe la gestión de incidentes	0	0%	13	65%	4	24%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas

Grafico N° 17. Dimensión Administración de Incidentes



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas

En la tabla número 32 y el Gráfico número 17 se detallan los resultados dados por los sujetos de estudio esto permite obtener información acerca de los eventos y debilidades de la información se realizaron 05 preguntas así:

Pregunta 89: Se comunican los eventos de seguridad: No se realiza comunicación sobre los eventos de seguridad que ocurren a los sistemas de información de acuerdo al 65% de los encuestados, el restante no sabe o no responde.

Pregunta 90: Se comunican las debilidades de seguridad, El 88% de los encuestados manifiesta que nunca le han comunicado las debilidades de seguridad de los sistemas de información, el 12 no sabe o no responde. Si la Dirección Administrativa la cual es la encargada de los sistemas de información no comunica a los interesados los riesgos que se enfrenta de perdida de información, no se crean mecanismos de control para minimizar los riesgos, por lo tanto, es importante contar con planes de comunicación de riesgos sobre los sistemas.

Pregunta 91: Existe definidas las responsabilidades ante un incidente, no han definido responsabilidades ante un incidente informático de acuerdo al 82% de los encuestados, teniendo en cuenta que la entidad actualmente tiene un ingeniero contratado, el cual es

por orden de prestación de servicios, no hay quien asuma la responsabilidad ante cualquier incidente que se presente.

Pregunta 92: ¿Existe un procedimiento formal de respuesta?, el 65% de los encuestados manifiesta que no existe ningún procedimiento formal de respuesta ante cualquier incidente lo que genera incertidumbre sobre cómo afrontar las situaciones que se presenten. El 35% restante no sabe o no responde.

Pregunta 93: ¿Existe la gestión de incidentes?, En la entidad no existe la gestión de incidentes de acuerdo al 76% de los encuestados, el 24% no sabe o no responde.

Como hemos observado no existen procesos ni procedimientos adecuados para el manejo de los incidentes que se puedan presentar dentro de la organización por lo cual se hace necesario establecerlos.

9.5.10. Dimensión Gestión de la Continuidad del Negocio

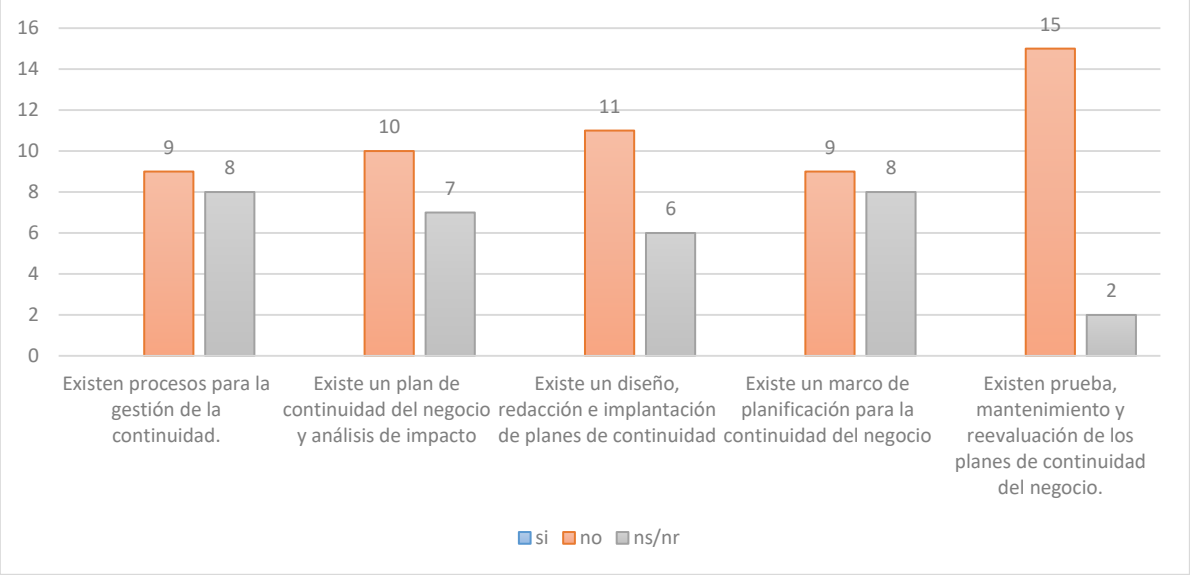
En la dimensión gestión de la continuidad del negocio se evalúan 8 ítems en donde se espera evaluar si la seguridad está implantada en los sistemas de información del Concejo Distrital de Cartagena y si se previene los errores, perdida o modificación o mal uso de las aplicaciones.

Tabla N° 33. Resultados Dimensión Gestión de la Continuidad del Negocio

Pregunta	si	%	no	%	ns/nr	%
94. Existen procesos para la gestión de la continuidad.	0	0%	9	53%	8	47%
95. Existe un plan de continuidad del negocio y análisis de impacto	0	0%	10	53%	7	41%
96. Existe un diseño, redacción e implantación de planes de continuidad	0	0%	11	53%	6	35%
97. Existe un marco de planificación para la continuidad del negocio	0	0%	9	53%	8	47%
98. Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio.	0	0%	15	53%	2	12%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas

Grafico N° 18. Dimensión Gestión de la Continuidad del Negocio



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas

El diagnostico efectuado se puede observar en la tabla número 33 y la gráfica 18 así:

Pregunta 94: ¿Existen procesos para la gestión de la continuidad? No existen procesos para la gestión de la continuidad en el Concejo Distrital de Cartagena, de acuerdo al 53% de los encuestados, el 47% no sabe o no responde. Los procesos de gestión de continuidad son importantes porque a través de estos se logra identificar los riesgos y amenazas potenciales que pueden afectar la entidad y es posible tener una respuesta acertada que construya confianza en los directivos.

Pregunta 95. ¿Existe un plan de continuidad del negocio y análisis de impacto? la entidad no posee un plan de continuidad del negocio y análisis de impacto que le permita asegurar la confianza de la ciudadanía en de los directivos tal como lo manifiesta el 59% de los encuestados de la planta de personal del Concejo Distrital de Cartagena, un 41% no sabe o no responde.

Pregunta 96 ¿Existe un marco de planificación para la continuidad del negocio? No existe un marco para la planificación de la continuidad del negocio de acuerdo al 53% de los encuestados, el restante 47% no sabe o no responde.

Pregunta 97 ¿Existe un diseño, redacción e implantación de planes de continuidad? La entidad no ha diseñado, redactado ni implantado planes de continuidad en el negocio de acuerdo al 65% de los encuestados, el 35% restante no sabe o no responde.

Pregunta 98 ¿Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio? El 88% de los encuestados manifiesta que no existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio. La entidad no ha realizado nunca planes de continuidad para proteger sus sistemas de información.

9.5.11. Dimensión Cumplimiento

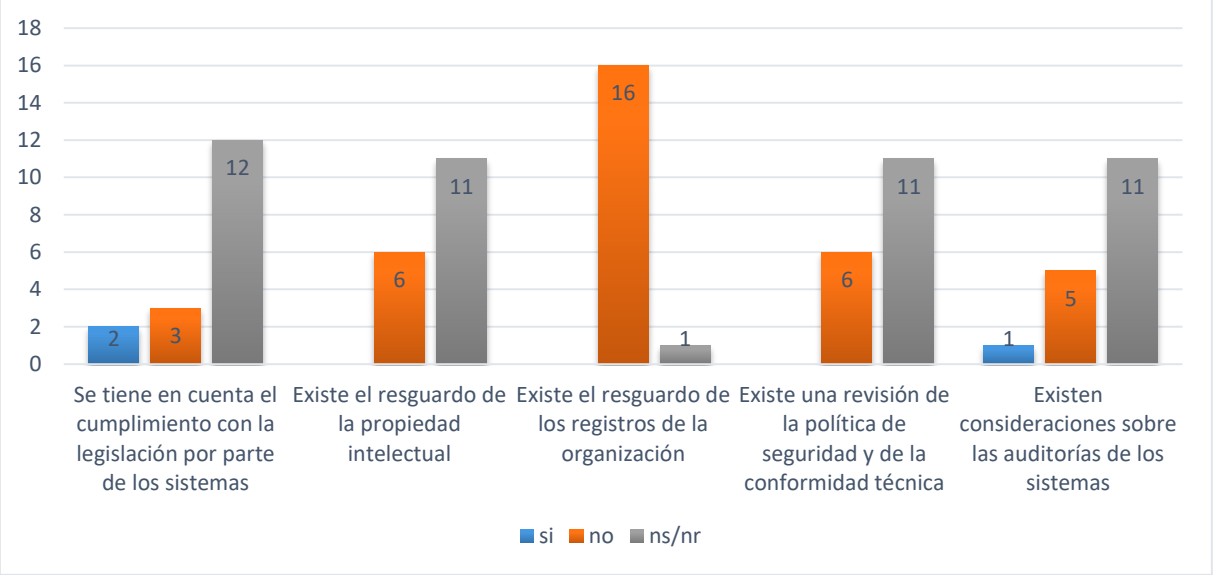
En la dimensión cumplimiento encontramos 5 preguntas relacionadas con que, si la entidad Concejo distrital de Cartagena permite o evita incumplimiento con la ley, obligación, o cualquier legislación de los sistemas y requisitos de seguridad del negocio

Tabla N° 34. Resultados Dimensión Cumplimiento

Pregunta	si	%	no		ns/nr	%
99. Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas	2	12%	3	18%	12	71%
100. Existe el resguardo de la propiedad intelectual	0	0%	6	35%	11	65%
101. Existe el resguardo de los registros de la organización	0	0%	16	94%	1	6%
102. Existe una revisión de la política de seguridad y de la conformidad técnica	0	0%	6	35%	11	65%
103. Existen consideraciones sobre las auditorías de los sistemas	1	6%	5	29%	11	65%

Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas

Grafico N° 19. Dimensión Cumplimiento



Fuente. Los autores de acuerdo a encuesta realizada a los empleados del Concejo Distrital de Cartagena en las áreas de Financiera, Administrativa, Secretaria General y Contratista de Sistemas

En la tabla número 34 y el Gráfico número 19 se puede observar los resultados en porcentajes y en número de personas a la pregunta 99 acerca que, si se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas, El 71% de los encuestados piensa que no se tiene en cuenta el cumplimiento con la legislación de los sistemas, prueba de ello es que no existe ningún tipo de seguridad en la información, el 29% no sabe o no responde.

Para el ítem 100 ¿Existe el resguardo de los registros de la organización lo sujetos de estudio? manifestaron que no existe el resguardo de los registros de la organización de acuerdo a lo expresado por el 94% de las personas encuestadas, el 6% no sabe o no responde. No se protege la información de la entidad generando un alto riesgo de pérdida de esta.

Para el ítem número 101 se indago que, si existe el resguardo de la propiedad intelectual, a lo que los sujetos de estudio manifestaron que no existe resguardo de la propiedad intelectual tal como lo infiere el 65% de los encuestados, el otro 35% no sabe o no responde.

Para la evaluación de si existe una revisión de la política de seguridad y de la conformidad técnica se formuló el ítem 102, a lo que los funcionarios manifestaron que

no existe revisión de la política de seguridad y de la conformidad técnica de acuerdo al 65% de los encuestados, un 35% no sabe o no responde. Los encuestados manifiestan que no existe política de seguridad y si existe no la conocen y nunca se ha implementado, por lo tanto, no se ha realizado ninguna acción ni procedimiento para la seguridad y la conformidad técnica.

Por último, se evaluó si existen consideraciones sobre las auditorías de los sistemas en el ítem 103, el 65% de los encuestados ante la pregunta ¿Existen consideraciones sobre las auditorias de los sistemas? No saben o no responde, un 29% manifestó que no y el 6% restante dijo que si, que, en el año inmediatamente anterior, la oficina asesora de control interno realizo auditoria de sistemas informando las anomalías en el área, además la Contraloría Distrital de Cartagena en sus auditorías integrales viene haciendo las recomendaciones pertinentes.

10. ANÁLISIS CONSOLIDADO DEL DIAGNOSTICO

Revisando los objetivos de la investigación y el análisis a las respuestas dadas por los participantes de las encuestas y las observaciones hechas en relación a los ejes temáticos Tic servicios y Modelo de seguridad y privacidad de la información y las observaciones hechas directamente en relación a los requerimientos de la Estrategia Gobierno en Línea, las conclusiones y recomendaciones del estudio son las siguientes:

10.1. TIC Servicios

La entidad no posee trámites ni servicios en línea, los trámites y servicios que existen se realizan en forma personal

Los siguiente son los tramites que existen actualmente en la entidad en forma personal:

- Radicado de proyectos de acuerdo de interés a la ciudadanía
- Consulta de proyectos de acuerdo de intereses a los entes interesados y ciudadanía
- Consulta de actas de acuerdo a la ciudadanía y entes interesados
- Realización de control político a los funcionarios del distrito de Cartagena.
- inscripción en proyectos de acuerdo, entrega de actas.
- Respuestas a derechos de petición de la ciudadanía.

Es necesario definir los trámites de la entidad que se podrán ofrecer en línea.

La ciudadanía no conoce los trámites y servicios que brinda la entidad, es necesario realizar una socialización de estos con el fin de brindar trámites y servicios adecuados a la ciudadanía.

La entidad no ha caracterizado los usuarios, por lo tanto, es necesario realizar la caracterización de los usuarios de sus trámites y servicios. No se ha realizado la identificación de las necesidades de los usuarios por lo que se hace imposible conocer

sus gustos y preferencias siendo muy difícil proponer servicios y tramites que se ajusten a sus necesidades.

La entidad no informa al usuario sobre sus derechos, obligaciones y las condiciones de uso del trámite o servicio en línea

No se garantiza protección de los datos personales de los usuarios del trámite o servicio

En el sitio web no se han definido los objetivos, la página está en constante mantenimiento, las personas no la conocen, no hay políticas de evaluación del sitio en línea, la mayoría de las personas consideran que la experiencia con la página web es mala.

10.2. Modelo De Seguridad y Privacidad de la Información

No existe un documento de política de seguridad de la información en la entidad incumpliendo lo establecido en el Modelo de seguridad y privacidad de la información el cual establece “Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializado al interior de la Entidad”. Es necesario diseñar procedimientos y documentarlos, realizando la socialización y aprobarlos por el comité de gestión institucional el cual esta designado para tal función. Es necesario realiza el documento con las políticas de seguridad de la información, realizar el plan de seguridad y los procedimientos de seguridad necesarios.

En cuanto a la organización de la seguridad de la información no están definidas las responsabilidades en los temas de seguridad de la información, dado que no existe un acto administrativo a través del cual se creen o se modifica las funciones del comité gestión institucional, en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta dirección, es necesario designar quien será el encargado de seguridad de la información dentro de la entidad, con el fin de que se diseñen directrices en relación a la seguridad de la información.

No existe un documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección.

No se han definido los perímetros de seguridad para las áreas críticas del Concejo Distrital de Cartagena, no hay procedimientos para autorizar el acceso a personal autorizado. Es necesario establecer el perímetro de seguridad para proteger las áreas que contenga información crítica.

No existe matriz con la identificación, valoración y clasificación de activos de información.

No hay conocimiento de los procesos administrativos ni de las fallas significativas de los sistemas de información.

No se lleva una adecuada administración ni control de la red, es decir no se toman medidas para evitar amenazas y mantener la seguridad de los sistemas de información, no se realizan copias de seguridad periódicamente, No hay un documento con la metodología de gestión de riesgos, ni análisis y evaluación de riesgos. Ni está establecido el de plan de tratamiento de riesgos.

No existe una política de control de acceso, es necesario diseñar la política de control de acceso definiendo funciones y responsabilidades

11. SITUACIÓN ACTUAL DEL CONCEJO DISTRITAL DE CARTAGENA DE LOS EJES TEMÁTICOS TIC SERVICIOS Y MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CON RESPECTO A LA ESTRATEGIA GOBIERNO EN LÍNEA.

11.1. Eje Temático TIC Servicios

Se realizó Diagnostico de la Situación actual con respecto a la Estrategia Gobierno en Línea tomando como base la Ficha Técnica Índice Gel Territorial publica en la página web http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-14714.html, y las encuestas, documentos y soportes, al igual que las entrevistas realizadas. Teniendo en cuenta que es importante ceñirse a los lineamientos previstos en el decreto 1151 de 2008 con el fin de garantizar la armonía y articulación del desarrollo de la Estrategia

De acuerdo a la ficha técnica se puede observar:

Tabla N° 35. Diagnóstico Situación Inicial Tic Servicios De Acuerdo A Gobierno En Línea

EJE TEMÁTICO TIC SERVICIOS	NUMERO DE PREGUNTAS	RESULTADO	NIVEL DE MADUREZ
LOGRO SERVICIOS CENTRADOS EN EL USUARIO		0	INICIAL
L4.1 Porcentaje de trámites y servicios en línea que cuentan con caracterización de los usuarios	4		
L4.2 Porcentaje de trámites y servicios en línea que cumplen los criterios de accesibilidad	3		
L4.3 Porcentaje de trámites y servicios en línea que cumplen los criterios de usabilidad	4		
L4.4 Porcentaje de trámites y servicios en línea que fueron promocionados	4		
LOGRO SISTEMA INTEGRADO DE PQRD		0	INICIAL
L5.1 Cuenta con un sistema web para la recepción, trámite y respuesta de PQRD	1		
L5.2 Cuenta con un sistema móvil para la recepción, trámite y respuesta de PQRD	2		
L5.3 Cuenta con un sistema integrado de PQRD	3		
LOGRO TRÁMITE Y SERVICIOS EN LÍNEA		0	INICIAL
L6.1Porcentaje de certificaciones y constancias disponibles en línea	1		
L6.2 Porcentaje de trámites y servicios disponibles en línea	3		
	4		

EJE TEMÁTICO TIC SERVICIOS	NUMERO DE PREGUNTAS	RESULTADO	NIVEL DE MADUREZ
L.6.3 Porcentaje de trámites y servicios en línea integrados a alguna ventanilla única			
RC2. Promedios indicadores de resultado TIC para Servicios RC2.1 Satisfacción con los trámites y servicios en línea RC2.2 Porcentaje de transacciones en línea	1 1	0	INICIAL

Fuente. De acuerdo a la Ficha Gel 2016.

De acuerdo a lo presentado en la Tabla No. 35 se puede observar que de los 4 criterios que hacen parte de los componentes del eje temático Tic servicios de la estrategia Gobierno en línea no cuentan con nivel de avance (0%). Es necesario tener en cuenta que cada uno de los logros tiene actividades determinadas para el cumplimiento del componente y también tienen un valor un peso específico definido por la Estrategia de Gobierno en línea de acuerdo a sus especificaciones.

11.2. Eje Temático Modelo De Seguridad Y Privacidad de la Información

Se realizó Diagnostico de la Situación actual del Modelo de Seguridad y privacidad de la información con respecto a la Estrategia Gobierno en Línea tomando como base el instrumento e evaluación MSPI 2016, y las encuestas, documentos y soportes, al igual que las entrevistas realizadas.

De acuerdo al instrumento de evaluación se observó:

Tabla N° 36. Evaluación efectividad de los Controles

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	0	60	INEXISTENTE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	0	60	INEXISTENTE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	0	60	INEXISTENTE
A.8	GESTIÓN DE ACTIVOS	0	60	INEXISTENTE
A.9	CONTROL DE ACCESO	0	60	INEXISTENTE
A.10	CRIPTOGRAFÍA	0	60	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	0	60	INEXISTENTE
A.12	SEGURIDAD DE LAS OPERACIONES	0	60	INEXISTENTE
A.13	SEGURIDAD DE LAS COMUNICACIONES	0	60	INEXISTENTE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	60	INEXISTENTE
A.15	RELACIONES CON LOS PROVEEDORES	0	60	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	60	INEXISTENTE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	60	INEXISTENTE
A.18	CUMPLIMIENTO	0	60	INEXISTENTE
PROMEDIO EVALUACIÓN DE CONTROLES		0	60	INEXISTENTE

Fuente. Instrumento de evaluación MSPI. Ministerio de las tecnologías de información 2016.

Como se puede observar en la Tabla número 35 donde se detalla la evaluación de los controles de acuerdo a los niveles de madurez del MSPI determinando el estado actual de la seguridad de la información en el Concejo Distrital de Cartagena el cual de acuerdo a la Tabla N° 36 se encuentra en un nivel Inexistente con una calificación de cero (0) lo cual el criterio de valoración de controles significa que existen una total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles

11.2.1. Valoración De Controles ISO 27001:2013

Tabla N° 37. Valoración de controles ISO 27001:2013

Tabla de Escala de Valoración de Controles ISO 27001:2013 ANEXO A		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
Inexistente	0	Total, falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.

Tabla de Escala de Valoración de Controles ISO 27001:2013 ANEXO A		
Descripción	**Calificación**	**Criterio**
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Fuente. Instrumento evaluación MSPI 2016.

Imagen N° 29. Brecha Anexo A ISO 27001: 2013

Fuente. Resultado obtenido al aplicar el instrumento de evaluación MSPI 2016.

Tabla N° 38. Requisitos con calificación de cumplimiento

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

Fuente Ficha diagnostico MSPI

Validando la imagen 29 y la tabla N° 38 se puede evidenciar que la entidad se encuentra en el criterio crítico (0% a 35%), con todos los dominios sin implantar y sin gestionar la entidad debería centrar su enfoque MSPI en todos los controles que se establecen. Es necesario realizar un gran acompañamiento con el fin de diseñar adecuadamente los controles para el cumplimiento de la norma.

11.2.2. Nivel De Madurez Modelo De Seguridad Y Privacidad De La Información

Para calcular el nivel de madurez del modelo de seguridad y privacidad de la información el instrumento de evaluación suministrado por Mintic señala la siguiente tabla:

Tabla N° 39. Niveles de madurez Modelo de Seguridad y Privacidad de la Información

Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

Fuente. Instrumento evaluación MSPI 2016.

Teniendo en cuenta que la entidad está en estado crítico en el cumplimiento de los controles se determina que la entidad está en un estado inicial, tal como establece la Tabla N° 39. En este nivel se encuentran las entidades que no cuentan con una identificación de activos y gestión de riesgos que le permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto no están alineados con la preservación de la confidencialidad, integralidad y disponibilidad.

11.2.3. Avance Ciclo de Funcionamiento del Modelo de Operación

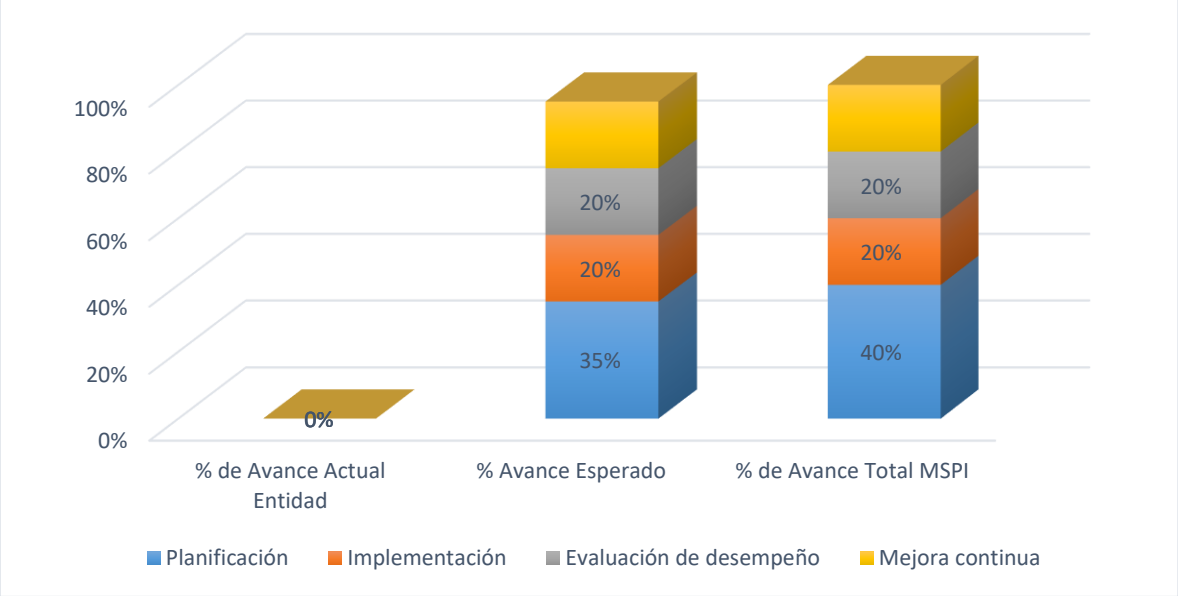
Tabla N° 40. Avance PHVA Concejo Distrital De Cartagena

Año	AVANCE PHVA			
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado	% de Avance Total MSPI
2015	Planificación	0%	35%	40%
2016	Implementación	0%	20%	20%
2017	Evaluación de desempeño	0%	20%	20%
2018	Mejora continua	0%	20%	20%
TOTAL				100%

Fuente. Instrumento de evaluación MSPI 2016.

Observando el resultado derivado en el punto anterior, donde se validó la implementación de los lineamientos gel en materia de seguridad ISO 27001:2013, se procedió a revisar el avance del ciclo de funcionamiento del modelo de operación del Concejo Distrital de Cartagena de acuerdo a la tabla número 40.

Grafico N° 20. Avance Ciclo de Funcionamiento del Modelo de Operación



Fuente. Resultado obtenido al aplicar el instrumento de evaluación MSPI 2016.

Al observar la tabla número 40 y el Gráfico número 20 se puede observar que el porcentaje de avance en la entidad es de 0% en todas las etapas.

Es necesario que la entidad comience a diseñar los respectivos controles del Modelo de seguridad y privacidad de la información que le permita cumplir con los plazos establecidos en la estrategia gobierno en línea.

12. ESTRATEGIAS PARA EL DISEÑO DEL EJE TEMÁTICO TIC SERVICIOS Y SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL CONCEJO DISTRITAL DE CARTAGENA

12.1. TIC Servicios

De acuerdo al diagnóstico realizado para el eje temático Tic Servicios en el Concejo Distrital de Cartagena de Indias y el Manual de Gobierno en Línea se evidenció que la entidad no ha realizado ningún tipo de avance en este componente dado que todos los logros del eje temático tic servicios tienen un nivel de madurez inicial. (Tabla N°34).

Para lograr diseñar Tic Servicios en el Concejo Distrital de Cartagena y con el fin de determinar cómo se puede proveer servicios ciudadanos adecuados a la población Cartagenera se desarrollará el diseño de tic servicios con los siguientes elementos de acuerdo al alcance establecido así:

- Servicios Centrado en el usuario - Tic Servicios en el Concejo Distrital de Cartagena.
- Sistema Integrado de PQRD
- Trámites y servicios en línea

Definiendo las siguientes estrategias:

Tabla N° 41. Estrategias para el diseño del Eje temático Tic Servicios – Logro Servicios Centrados en el Usuario.

Estrategia	Objetivos estratégicos	Iniciativa	Proyectos
Diseño de los ejes temáticos de la Estrategia Gobierno en Línea Tic servicios Servicios centrados en el Usuario	Identificar las características de la población del Concejo Distrital de Cartagena de Indias, para conocer los intereses y necesidades de información con el fin de proponer una estrategia de comunicación para mejorar los servicios tic que presta la entidad	Caracterizar los usuarios de la entidad y Grupos de interés	Diseñar la matriz de caracterización de los usuarios del Concejo Distrital de Cartagena
	Establecer los mecanismos que permitan el acceso a los servicios de información por parte de los diferentes grupos de interés, contemplando características de accesibilidad, seguridad y usabilidad.	Establecer Directrices de accesibilidad y usabilidad	- Diseñar la Guía de accesibilidad y usabilidad de los trámites y servicios del Concejo Distrital de Cartagena
	Diseñar estrategias de promoción de los trámites y servicios disponibles por medios electrónicos de acuerdo a la caracterización de usuarios	Estrategias de promoción de trámites y servicios	Diseñar el plan de comunicaciones para la promoción de trámites y servicios digitales del Concejo Distrital de Cartagena
	Diseñar criterios para la evaluación de la satisfacción del usuario de los servicios y tramites electrónicos	Criterios de Evaluación del usuario	Diseñar una guía donde se establezcan los criterios de evaluación de la satisfacción del usuario.
Diseño de los ejes temáticos de la Estrategia Gobierno en Línea Tic servicios Sistema Integrado de PQRD SISTEMA WEB DE PETICIONES, QUEJAS, RECLAMOS Y DENUNCIAS	Definir las pautas para la elaboración de protocolos de atención en los canales digitales por los cuales presente servicios a los ciudadanos clientes.	Diseño de un protocolo para la atención de los ciudadanos digitales	Diseñar el protocolo general de atención al usuario digital del Concejo Distrital de Cartagena
Diseño de los ejes temáticos de la Estrategia Gobierno en Línea Tic servicios Trámites y servicios en línea	Definir los trámites y servicios en línea de acuerdo al diagnóstico realizado en la entidad	Guía de Tramites del Concejo Distrital de Cartagena	Diseño de la Guía de trámites y servicios ofrecidos por el Concejo Distrital de Cartagena vía web

Fuente. Los autores de acuerdo a Tic Servicios.

12.2. Estrategias Para el Diseño del Eje Temático TIC Seguridad y Privacidad de la Información

De acuerdo al diagnóstico realizado y tomando como referencia los controles del MSPI basado en la norma ISO 27001:2013 (tabla N°35 y 36), se definen las siguientes estrategias para el eje temático Tic seguridad y privacidad de la información.

Tabla N° 42. Estrategias para el diseño del Eje temático Tic Seguridad y Privacidad de la información Concejo Distrital de Cartagena.

Estrategia	Objetivos Estratégicos	Metas	Iniciativa	Proyectos
Diseño del eje temático Seguridad y Privacidad de la Información	Asegurar mejores prácticas de gobernabilidad, seguridad y procedimientos TI	Implementar los distintos controles de seguridad de la ISO 27001 en un 50% en el primer año y así en forma progresiva en los siguientes años	Manual de seguridad y privacidad de la información	Diseñar el Manual de las políticas de seguridad y privacidad de la información el cual contiene el alcance del sistema de gestión, incluyendo los detalles y justificación de cualquier exclusión.
	Asignar los roles y responsabilidades en la estructura organizacional en cuanto a seguridad y privacidad de la información.	Que los funcionarios cumplan en un 80% con sus roles y responsabilidades el primer año	Diseño de matriz de roles y responsabilidades	Diseñar la matriz de roles y responsabilidades del modelo de privacidad y seguridad de la información del Concejo Distrital de Cartagena
	Clasificar los activos de información de los procesos de Atención al Usuario, Administrativa y Financiera.	Implementar en un 70% los distintos salvaguardas propuestos con el fin de disminuir el impacto en el activo	Inventario de activos de información	Diseñar documento de caracterización, valoración y clasificación de activos de información de los procesos de atención al usuario, financiera y administrativa, el cual incluye la identificación de las salvaguardas y los niveles de madurez de estas
Mapa de Riesgos de seguridad de la información	Valorar los riesgos de seguridad que permita definir planes de tratamiento de riesgos de acuerdo a la metodología señalada	Realizar revisión y actualización en forma semestral de la matriz de riesgos.	Identificación, valoración y tratamiento de los riesgos	Diseñar la Matriz de riesgos seguridad de la información de los activos informáticos

Fuente. Los autores de acuerdo a Diagnostico y Manual de gobierno en línea.

13. IDENTIFICAR LAS CARACTERÍSTICAS DE LOS DIFERENTES GRUPOS OBJETIVOS DEL CONCEJO DISTRITAL DE CARTAGENA CON EL FIN DE AUMENTAR EL CONOCIMIENTO SOBRE NUESTROS USUARIOS Y DISEÑAR ESTRATEGIAS PARA MEJORAR LA COMUNICACIÓN E INCREMENTAR LA SATISFACCIÓN DE LOS MISMOS

Con el fin de identificar las características que permitiera lograr la identificación de los diferentes grupos objetivos del Concejo Distrital de Cartagena se definió la siguiente estrategia:

- Diseñar la matriz de caracterización de los usuarios del Concejo Distrital de Cartagena.

A través de la caracterización de los usuarios de la entidad se pretende identificar las características de la población del Concejo Distrital de Cartagena de Indias, para conocer los intereses y necesidades de información con el fin de proponer una estrategia de comunicación para mejorar los servicios tic que presta la entidad.

Este objetivo se tratará en el anexo número 2 en forma explícita.

14. DISEÑAR DIRECTRICES DE ACCESIBILIDAD Y USABILIDAD PARA SER IMPLEMENTADO EN LOS TRÁMITES Y SERVICIOS ELECTRÓNICOS, QUE PERMITA A LOS USUARIOS TENER UNA EXPERIENCIA AGRADABLE AL ACCEDER A LOS SERVICIOS ELECTRÓNICOS DE LA ENTIDAD.

Con el propósito de diseñar directrices de accesibilidad y usabilidad para ser implementado en los trámites y servicios electrónicos, que permita a los usuarios tener una experiencia agradable al acceder a los servicios electrónicos de la entidad, se estableció la estrategia “Diseñar la Guía de accesibilidad y usabilidad de los trámites y servicios del Concejo Distrital de Cartagena”.

En esta guía se abordará, el diseño adecuado dela página web del Concejo distrital de Cartagena de indias, que todos los procedimientos sean comprendidos y se enfoquen en el usuario, también se define y explica los conceptos de usabilidad y accesibilidad, introducción de la arquitectura de la información, detalle de procedimientos, métodos y recomendaciones de la página web. En la guía se podrá observar cómo debe ser el diseño de la página de acuerdo a los estándares de gobierno en línea, W3C, ISO 25000, dando mayor accesibilidad y usabilidad al usuario de la información. La ampliación de este objetivo se podrá ver en el anexo N°3.

De igual forma se diseñó la Guía de trámites y servicios en línea la cual se puede encontrar en el anexo N° 7, en aras de facilitarle a la ciudadanía información acerca de los trámites y servicios del Concejo Distrital de Cartagena y de dar a conocer en forma clara los requisitos para acceder a los diferentes trámites y servicios de la entidad, en esta guía se definen los trámites y servicios en línea de acuerdo al diagnóstico realizado en la entidad y la caracterización de usuarios, específicamente lo concernientes a los temas de las solicitudes y así permitir que un mayor acercamiento de la ciudadanía con la entidad. Con esta guía se espera mejorar la accesibilidad de los trámites y servicios prestados por El Concejo Distrital de Cartagena.

15. DISEÑAR ESTRATEGIAS DE PROMOCIÓN DE LOS TRÁMITES Y SERVICIOS DISPONIBLES POR MEDIOS ELECTRÓNICOS, QUE PERMITA MEJORAR LA RELACIÓN CIUDADANO- ENTIDAD A TRAVÉS DE LA PRESTACIÓN DE CALIDAD DE LOS SERVICIOS.

Con el fin de dar cumplimiento al objetivo “Diseñar estrategias de promoción de los trámites y servicios disponibles por medios electrónicos que permita mejorar la relación ciudadano- entidad a través de la prestación de calidad de los servicios se construye la estrategia:

- Diseñar el plan de comunicaciones para la promoción de trámites y servicios digitales del Concejo Distrital de Cartagena

El plan de comunicaciones que se realiza para la promoción de servicios y trámites digitales de la entidad como estrategia para el diseño del primer logro tic servicios, por medios electrónicos de acuerdo a la caracterización de usuarios. A través del plan de comunicaciones se busca responder a la necesidad que tiene el concejo de promover sus trámites y servicios electrónicos y físicos.

La promoción de trámites y servicios electrónicos se realizará mediante el desarrollo de estrategias que permitirán a los Stakeholder comunicarse en forma efectiva con la entidad a través de las diferentes herramientas con las que cuenta la entidad tales como: página web, Facebook, Instagram, buzón de quejas y sugerencias, ventanilla única (una vez creada). En el anexo N°4 se podrán observar las distintas estrategias que permitirán hacer una adecuada promoción de los trámites y servicios de la entidad.

16. ESTABLECER CRITERIOS PARA LA EVALUACIÓN DE LA SATISFACCIÓN DEL USUARIO DE LOS SERVICIOS Y TRÁMITES ELECTRÓNICOS, CON EL FIN DE CONTAR CON UNA GUÍA QUE MARQUE LA RUTA A SEGUIR.

Con el propósito de cumplir el objetivo de establecer criterios para la evaluación de la satisfacción del usuario de los servicios y trámites electrónicos, con el fin de contar con una guía que marque la ruta a seguir. Se define como estrategia:

- Diseñar criterios para la evaluación de la satisfacción del usuario de los servicios y tramites electrónicos.

Con base a esta se desarrolló una guía dirigida a todos aquellos funcionarios encargados de realizar la evaluación de los trámites y servicios que presta el Concejo Distrital de Cartagena de Indias, señalando que criterios y métodos deben utilizar para la evaluación, esto se puede observar con más detalle en el anexo N°35.

17. DEFINIR LAS PAUTAS PARA LA ELABORACIÓN DE PROTOCOLOS DE ATENCIÓN EN EL CANAL DIGITAL Y ELECTRÓNICO DONDE SE LE PRESTE SERVICIO A LOS CIUDADANOS CON CALIDAD Y OPORTUNIDAD.

Para el cumplimiento del objetivo “Definir las pautas para la elaboración de protocolos de atención en los canales digitales por los cuales presente servicios a los ciudadanos clientes” se establece la estrategia. “Diseñar el protocolo general de atención al usuario digital del Concejo Distrital de Cartagena”.

El protocolo de atención al usuario de la entidad, brindara información primordial para la atención al usuario buscando su satisfacción asegurando una prestación de trámites y servicios de acuerdo a los principios constitucionales de igualdad, celeridad, oportunidad y basándose en estándares de eficacia y eficiencia.

Con el diseño y aplicación del protocolo de atención al usuario y ciudadano por el canal digital y electrónico del Concejo Distrital de Cartagena se busca que la atención brindada por el talento humano vinculado a la entidad en este canal se realice bajo altos estándares de calidad y una agradable atención al ciudadano garantizando trato digno en la prestación de los trámites y servicios. El detalle del protocolo de atención al ciudadano en el canal digital se encuentra en el anexo número 6.

18. REALIZAR LA ASIGNACIÓN DE LOS ROLES Y RESPONSABILIDADES EN LA ESTRUCTURA ORGANIZACIONAL EN CUANTO A SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Con el fin de cumplir el objetivo de asignar los roles y responsabilidades en la estructura organizacional en cuanto a seguridad y privacidad de la información, se realiza la Matriz de Roles y Responsabilidades Modelo de Seguridad y Privacidad de la Información Concejo Distrital de Cartagena, la cual define dentro de la estructura organizacional del Concejo Distrital de Cartagena, los roles y responsabilidades para la seguridad y privacidad de la información de las personas que intervienen en las distintas dependencias de la entidad.

De acuerdo al esquema organizacional del Concejo Distrital de Cartagena se definirán los roles y responsabilidades del Concejo Distrital de Cartagena teniendo en cuenta el Sistema de Seguridad y Privacidad de la Información se detallan los perfiles definidos en cada nivel describiendo las responsabilidades dentro de la seguridad y privacidad de la información. (Anexo 8).

19. DEFINIR LAS POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN DE LA ENTIDAD TOMANDO COMO BASE MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ESTRATEGIA GEL, QUE DEFINA LAS ACCIONES A SEGUIR PARA EL MANEJO DE LA INFORMACIÓN Y DE LOS SISTEMAS DE INFORMACIÓN.

De acuerdo al diagnóstico del eje temático seguridad y privacidad de la información de estrategia Gobierno en Línea se definen las políticas de la Seguridad de la Información de la entidad tomando como base Modelo de Seguridad y Privacidad de la información de la estrategia Gel, donde se proponen acciones a seguir para el manejo de la información y de los sistemas de información, se creó la estrategia "Diseñar el Manual de las políticas de seguridad y privacidad de la información el cual contiene el alcance del sistema de gestión, incluyendo los detalles y justificación de cualquier exclusión" teniendo en cuenta que para la entidad Concejo Distrital de Cartagena de Indias es de gran importancia contar con un marco que asegure la información de la entidad dentro de los criterios de disponibilidad, confiabilidad e integridad todo esto dentro de un sistema de gestión de seguridad de la información (SGSI), de ahí la necesidad de contar con políticas claras para la protección de la información que produce la entidad.

La razón de este manual es describir las políticas de seguridad de la información definidas por la Concejo Distrital de Cartagena de Indias. Para la elaboración del mismo, se toma como base el Anexo A, incluido en la norma ISO 27001:2013, recomendaciones de la ISO 27002:2013 los lineamientos de la estrategia de Gobierno en Línea (GEL), en especial las guías suministradas.

Las políticas de seguridad de la información incluidas en este manual constituyen una parte fundamental del Sistema de Gestión de Seguridad de la Información (SGSI) y el Modelo de Seguridad y Privacidad de la Información (MSPI) de Gobierno en Línea (GEL) y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

La preservación de la confidencialidad, integridad y disponibilidad de la información para la Concejo Distrital de Cartagena de Indias, constituye una prioridad y por tanto, es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

Dentro del manual se define el alcance y los objetivos del Modelo de Seguridad y Privacidad de la información de la estrategia Gel para el Concejo Distrital de Cartagena. (Anexo N°9)

20. REALIZAR LA CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN DE LOS PROCESOS DE ATENCIÓN AL USUARIO, ADMINISTRATIVA Y FINANCIERA

Con el fin de Clasificar los activos de información de los procesos de Atención al Usuario, Administrativa y Financiera del Concejo Distrital de Cartagena se diseñó la estrategia:

- Diseñar documento de caracterización, valoración y clasificación de activos de información de los procesos de atención al usuario, financiera y administrativa, el cual incluye la identificación de las salvaguardas y los niveles de madurez de estas

Con el fin de cumplir con esta fase se procede a realizar un reconocimiento de los activos de información del Concejo Distrital de Cartagena de Indias para la identificación de los activos de información en los procesos de atención al usuario, dirección administrativa y dirección financiera. (Anexo 10).

Con el fin de cumplir el objetivo " **Valorar los riesgos de seguridad que permita definir planes de tratamiento de riesgos de acuerdo a la metodología señalada, buscando la protección de la información y los sistemas de información del acceso, uso, divulgación, interrupción o destrucción no autorizada**" se realiza el análisis y gestión de los riesgos de información dentro del anexo 10, con el fin de proteger la confidencialidad, integridad y disponibilidad de esta se toma como método de análisis y gestión de riesgos informáticos la Metodología MAGERIT 37 versión 3.0, esta metodología de la mano con la norma ISO/IEC 27001 de 2013 la cual permite identificar amenazas y estimar impacto y probabilidad de forma cualitativa.

21. PLAN DE INTERVENCIÓN PARA LA IMPLEMENTACIÓN

El objetivo de este capítulo es definir de acuerdo a los objetivos y estrategias planteadas los proyectos, procedimientos y capa mañas de socialización que lograran en un futuro la implementación de la estrategia Gobierno en Línea TIC servicios y seguridad y privacidad de la información, la cual no está incluida en este proyecto de grado.

Con el fin de lograr la implementación en la entidad de los ejes temáticos TIC servicios y privacidad de la información es preciso conformar un equipo de trabajo, el cual puede ser el mismo para el eje temático TIC servicios y para el eje temático Seguridad y Privacidad de la información (Anexo 8).

Es de resaltar que para lograr la implementación es necesario el compromiso de la alta dirección, por lo tanto, es necesario realizar procesos adecuados de socialización de la estrategia mostrando a estos las sanciones a las cuales se vería expuesta la entidad por la no aplicabilidad de la entidad. En la tabla N° 43 se propone el plan de implementación para la intervención de los ejes temáticos de la estrategia Gobierno en Línea TIC servicios y privacidad de la información para el Concejo Distrital de Cartagena.

21.1. Plan De Intervención Para La Implementación

Tabla N° 43. Plan De Intervención Para La Implementación

ACTIVIDAD	OBJETIVOS	RESPONSABLES	RECURSOS	TIEMPO	RIESGO	TRATAMIENTO DE RIESGOS
Socialización de la estrategia gobierno en Línea Ejes temáticos Tic Servicios y Seguridad y privacidad de la información e importancia de un plan de implementación. - Curso intensivo de 40 horas para el conocimiento de la estrategia a través de la contratación de un experto en el tema. Campaña de publicidad por medio de redes sociales, carteleras ejes temáticos estrategia gobierno en línea.	Dar a conocer la importancia de la estrategia Gobierno en línea en los ejes temáticos tic servicios y seguridad y privacidad de la información y la importancia de la implementación para la mejora de sus trámites y servicios y protección de la información.	Equipo Del Proyecto (Director Financiero, Administrativo, Comunal, Jefe De Comunicaciones Y Protocolo). - Consultor experto en temas de gobierno en línea	tiempo, tecnología, ambiente de trabajo, personal competente, papelería y recurso financiero	1 mes	Poca asistencia de los funcionarios. Mala interpretación de la estrategia. No contextualización de los términos en la organización. Incumplimiento	Premios a los mejores equipos de trabajo. Sanciones a los que no asistan a la capacitación. Lista de funcionarios en servicio.
Socialización de los resultados del Diagnóstico de la Estrategia Gobierno en línea TIC Servicios y seguridad y privacidad de la información	Mostrar el estado actual de la estrategia gobierno en línea dentro de la entidad y la	Coordinador Implementación Del Modelo De Seguridad De La Información Comité de seguridad y equipo del proyecto.	tiempo, tecnología, ambiente de trabajo, personal competente, papelería y recurso financiero	1 mes	Inadecuada comprensión del diagnóstico.	Capacitación al personal en forma continua.

ACTIVIDAD	OBJETIVOS	RESPONSABLES	RECURSOS	TIEMPO	RIESGO	TRATAMIENTO DE RIESGOS
- cartillas con los resultados por oficinas. - explicación de los resultados de la estrategia	importancia de su implementación	Secretario Del Comité – Asesor Jurídico				
Socialización de las estrategias establecidas en TIC servicios y seguridad y privacidad de la información para el Concejo Distrital de Cartagena. Entrega de la documentación a cada área de la entidad. Socialización de documentos a explicar Publicación en carteleras de los diferentes servicios y trámites de la entidad. Divulgación de los documentos mediante sesiones de capacitación	Explicar de manera detallada y clara la terminología e importancia de la estrategia Gobierno en línea después de haber realizado un diagnostico con el fin de llevar a cabo una mejora continua en general	Líder del proyecto Presidente	tiempo, tecnología, ambiente de trabajo, personal competente, papelería y recurso financiero	2 meses	Poca asistencia de los funcionarios. Mala interpretación de la estrategia. No contextualización de los términos en la organización. Incumplimiento. Error /o desacierto en la socialización	Capacitación al personal en forma continua Citar a la capacitación en forma oportuna. Ser claro en los conceptos.
Socialización de la caracterización de usuarios del Concejo Distrital de Cartagena.	Presentar la caracterización de los usuarios al	Equipo del proyecto de implementación de la estrategia	tiempo, tecnología, ambiente de trabajo, personal	1 mes	Error o desacierto por falta de comunicación en	Claridad en los conceptos.

ACTIVIDAD	OBJETIVOS	RESPONSABLES	RECURSOS	TIEMPO	RIESGO	TRATAMIENTO DE RIESGOS
- Entregar documentación al proceso de atención al usuario para aplicabilidad a la página web. - socializar el proceso de recolección de la información. -	personal encargado de los procesos con el fin de dar a conocer por qué la importancia de implementar trámites y servicios para mejorar la relación estado – ciudadano		competente, papelería y recurso financiero		los encargados de los procesos.	Capacitación continua
Divulgar **directrices** de accesibilidad y usabilidad en los trámites y servicios electrónicos para que los usuarios tengan una experiencia agradable al acceder a los servicios electrónicos de la entidad. - Entregar documentación al proceso de atención al usuario. - Capacitar el personal encargado de la página sobre las normas de accesibilidad y usabilidad.	Presentar y explicar las directrices que los usuarios tendrán, a la otra de usar esta herramienta electrónica que les será de mucha ayuda.(no acercarse a la entidad, falta de tiempo ,más comodidad desde sus casas, entre otras)	Equipo del proyecto	Tiempo, tecnología, ambiente de trabajo, personal competente, papelería y recurso financiero	1 mes	Error o desacierto en el momento de la divulgación. Falta de presupuesto.	Capacitación continua. Programación oportuna.

ACTIVIDAD	OBJETIVOS	RESPONSABLES	RECURSOS	TIEMPO	RIESGO	TRATAMIENTO DE RIESGOS
Socializar y publicar el plan de comunicaciones para la promoción de los trámites y servicios disponibles por medios electrónicos. - imprimir plan de comunicaciones y entregar al personal responsable. - Realizar charla de 40 horas	Presentar el plan de comunicaciones a los responsables del proceso de comunicaciones de la entidad.	Equipo del proyecto	Tiempo, tecnología, ambiente de trabajo, personal competente, papelería y recurso financiero	1 mes	Error o desacierto en el momento de la divulgación.	Capacitación continua
Socialización de la guía de evaluación de la satisfacción del usuario de los servicios y trámites electrónicos. - entrega de la guía al personal responsable. - capacitación en instrumentos de evaluación (curso de 16 horas)	Presentar a los responsables de los procesos la guía para realizar la evaluación de la satisfacción del usuario de los servicios y tramites electrónicos.	Equipo del proyecto Consultor	tiempo, tecnología, ambiente de trabajo, personal competente, papelería y recurso financiero	1 mes	Error o desacierto en el momento de la socialización. Falta de compromiso de los asistentes.	Capacitación continua Personal experto Motivación constante a los funcionarios.
Socializar el Protocolo De Atención Al Ciudadano Y Usuarios De Canales	Presenta el protocolo de atención al	Equipo del proyecto.	tiempo, tecnología, ambiente de trabajo, personal	1 mes	Error o desacierto en el momento de la socialización.	c

ACTIVIDAD	OBJETIVOS	RESPONSABLES	RECURSOS	TIEMPO	RIESGO	TRATAMIENTO DE RIESGOS
Electrónicos Y Digitales Del Concejo Distrital De Cartagena. -Entrega en medio físico del protocolo de atención al ciudadano. - reuniones diarias de 1 hora por 1 mes con el fin de conocer las estrategias a aplicar por el personal	ciudadano al responsable del proceso de atención al usuario		competente, papelería y recurso financiero		Falta de compromiso de los asistentes.	
Socializar la guía de trámites y servicios digitales del Concejo Distrital de Cartagena. - Entrega de la guía a todos los funcionarios en medio electrónicos. - Charla informativa de los trámites y servicios digitales de la entidad (semanal- 1 hora)	Presentar los trámites y servicios a prestar por la entidad a la alta dirección, a los funcionarios y ciudadanía.	Equipo del proyecto	tiempo, tecnología, ambiente de trabajo, personal competente, papelería y recurso financiero	2 meses	Error o desacierto en el momento de la socialización. Falta de compromiso de los asistentes.	Capacitación continua Personal experto Motivación constante a los funcionarios
Socialización de las políticas de la Seguridad de la	Presentar la política de la seguridad de la información	Equipo del proyecto	tiempo, tecnología, ambiente de trabajo, personal	2 meses y en forma continua	Error o desacierto en el momento de la socialización.	Capacitación continua Personal experto

ACTIVIDAD	OBJETIVOS	RESPONSABLES	RECURSOS	TIEMPO	RIESGO	TRATAMIENTO DE RIESGOS
Información del **Concejo** Distrital de Cartagena - Publicar y comunicar las políticas al personal por medio de divulgaciones semanales de 1 hora. - Firma de acta de compromiso con el cumplimiento de las políticas. - establecer protocolos de cumplimiento de las políticas de seguridad generales y específicas. - Realizar claridad de las sanciones por no cumplimiento de la política. - Evaluación y seguimiento de las políticas en forma periódica.	generales y especificas con el fin de crear conciencia de la importancia para la permanencia de la organización	Comité de seguridad y privacidad de la organización. - jefe de control interno	competente, papelería y recurso financiero		Falta de compromiso de los asistentes.	Motivación constante a los funcionarios
Socializar la matriz de roles y responsabilidades para la seguridad y privacidad de la información. - Socialización de las responsabilidades al equipo	Presentar matriz de roles y responsabilidades de todas las personas de la organización	Líder del proyecto - presidente	tiempo, tecnología, ambiente de trabajo, personal competente, papelería y recurso financiero	1 mes y en forma constante	Error o desacierto en el momento de la socialización.	Capacitación continua Personal experto Motivación constante a los funcionarios

ACTIVIDAD	OBJETIVOS	RESPONSABLES	RECURSOS	TIEMPO	RIESGO	TRATAMIENTO DE RIESGOS
del proyecto por medio de la entrega de la guía de roles y responsabilidades (se imprimirá una cartilla por responsable). Se comunicará en la cartelera de la entidad luego de la firma de la resolución que acredite la conformación del equipo del proyecto					Falta de compromiso de los asistentes.	
Socializar la clasificación, riesgos y planes de tratamiento de los riesgos de información de las diferentes áreas (**Atención** al Usuario, Administrativa y Financiera). - realizar socialización de los diferentes riesgos a los que se expone la seguridad y privacidad de la información). - concientización de la importancia de aplicar las medidas de tratamiento para reducir los riesgos.	Explicar de una detallada y clara la clasificación y los planes de tratamiento de los riesgos con el fin de evitar la pérdida de información importante para garantizar la integridad, confidencialidad y disponibilidad de la información.	Líder del proyecto Comité de seguridad Equipo del proyecto	tiempo, tecnología, ambiente de trabajo, personal competente, papelería y recurso financiero	2 meses	Error o desacierto en el momento de la socialización. Falta de compromiso de los asistentes.	Personal experto en temas de riesgos

ACTIVIDAD	OBJETIVOS	RESPONSABLES	RECURSOS	TIEMPO	RIESGO	TRATAMIENTO DE RIESGOS
-Comprometer a la alta dirección en la implementación de los controles para prevenir los riesgos.						
Socializar la valoración de riesgo de seguridad definiendo de una manera clara los planes y tratamientos de riesgos de la entidad. - Presentación en Video Ven del proceso para clasificar los activos. - entrega de la valoración y clasificación de activos al área responsable	Explicar la valoración, planes y tratamientos de riesgo de seguridad con el fin de buscar la protección de la información y los sistema de información de acceso, uso, etc.	Equipo del proyecto Comité de seguridad	tiempo, tecnología, ambiente de trabajo, personal competente, papelería y recurso financiero	2 meses	Error o desacierto en el momento de la socialización. Falta de compromiso de los asistentes	Capacitación continua.
Auditoria de evaluación de la implementación de la Estrategia Gobierno en Línea para los dos ejes temáticos.	Revisar si se ha realizado en forma adecuada la implementación y propones mejoras	Jefe de control interno Profesionales de control interno	Papelería, recursos	1 mes	Error o desacierto en la evaluación	Aplicación de procedimientos de auditoria adecuados.

Fuente. Los autores de Acuerdo al Diseño de los Ejes temáticos de la estrategia Tic servicios y seguridad y privacidad de la información del Concejo Distrital de Cartagena.

21.2. Tiempo de Implementación

De acuerdo al número de procesos de la entidad y los procesos, subprocesos, y controles a implementar se tiene un estimado de 18 meses para la implementación de los ejes temáticos de la estrategia en línea, contando con el apoyo de la Mesa directiva del Concejo Distrital de Cartagena y con la conformación del Equipo del proyecto responsable y comprometido con la implementación de los ejes temáticos TIC servicios y privacidad de la información.

21.3. Costos de implementación de los ejes Temáticos de la Estrategia Gobierno en Línea, TIC Servicios y Privacidad y Seguridad de la Información

Tabla N° 44. Costos de Implementación

PROPUESTA		CONCEPTO	COSTO	COSTO TOTAL
Curso de capacitación con experto en estrategia gobierno en línea		40 Horas	60.000	2.400.000
Plan de divulgación de los ejes temáticos TIC servicios y privacidad y seguridad de la información estrategia Gobierno en línea	Carteleras	Papelería y marcadores	20.000	20.000
	capacitación y socialización	Tiempo y Material	100.000	100.000
	impresión de documentos	impresión de 1500 hojas	600	900.000
curso instrumentos de evaluación		16 horas	60.000	960.000
COSTO APROXIMADO				4.380.000

Fuente. Los Autores

CONCLUSIONES

A través del diagnóstico de la situación actual del Concejo Distrital de Cartagena frente a los ejes temáticos de la estrategia Gobierno en línea TIC Servicios y Seguridad y privacidad de la información se pudo observar que el cumplimiento frente a esta es nulo dado que entidad no posee tramites ni servicios en línea, los trámites y servicios que existen se realizan en forma personal y el nivel de madurez corresponde al 0% en logros centrados en el usuario de TIC servicios, logro sistema integrado de PQRD y logro trámites y servicios en línea, y el eje seguridad y privacidad de la información encuentra en un nivel inexistente con una calificación de cero (0) en el criterio de valoración de los controles.

Para el eje TIC servicios en el diagnóstico inicial se encontró:

- La entidad no posee trámites ni servicios en línea, los trámites y servicios que presta la entidad se realizan en forma personal, ocasionando demoras en la atención, la información solicitada se demora más de 10 días hábiles ante la falta de sistemas de información, colocando quejas los usuarios por demoras y tutelas por falta de oportunidad en la entrega.
- La entidad no había caracterizado los usuarios, ni identificado cuales eran sus necesidades, no conocían sus gustos y preferencias siendo muy difícil proponer servicios y tramites que se ajustarán a sus necesidades, por lo cual se realiza la caracterización de los usuarios, determinando una serie de variables y se diseña las estrategias adecuadas para que los usuarios gestionen los servicios requeridos para una mayor comodidad, sin desplazamientos y de forma más ágil.
- Al no tener claridad acerca de sus trámites y servicios no se cuenta con plan de comunicaciones para su promoción, es por esto que se diseña el plan de comunicaciones de promoción de servicios y trámites digitales de la entidad con el objetivo de lograr la promoción de los trámites y servicios disponibles por medios electrónicos de acuerdo a la caracterización de usuarios y así mejorar en un 80% la imagen de la entidad frente de los usuarios de los trámites y servicios

- La entidad no informa al usuario sobre sus derechos, obligaciones y las condiciones de uso del trámite o servicio en línea, ante esta situación se diseña la guía de usabilidad y accesibilidad para la página web de la entidad, que permitirá que los trámites y servicios que ofrece la entidad por medios electrónicos tengan las características necesarias para que toda la población pueda acceder a ellos, sean de fácil uso, proporcionando una agradable experiencia a los usuarios y grupos de interés, en miras de lograr que el 70% de la población que utiliza los servicios digitales de la entidad cuente con un servicio o tramite acorde a sus necesidades.

- No se garantiza protección de los datos personales de los usuarios del trámite o servicio, a su vez en el sitio web no se habían definido los objetivos, se evidencia que la página web está en constante mantenimiento, la población no la conoce, no hay políticas de evaluación del sitio en línea, se sugiere a alta dirección que se debe contar con una persona idónea que maneje la página web y que se ajuste a la estrategia en Línea, prestando los servicios a la comunidad de manera adecuada, cumpliendo la normatividad existente.
- No se realiza evaluación de la satisfacción de los servicios y tramites ofrecidos, no contando con una ruta a seguir para lograr mejorar en la atención al usuario, de ahí que se realiza el diseñó de una guía de criterios para la evaluación de la satisfacción del usuario de los servicios y trámites electrónicos, con el fin de contar con una ruta a seguir, esperando que, con la evaluación continua de esta, se mejore en un 80% de la satisfacción de los usuarios de los trámites y servicios.
- La entidad no posee protocolos de atención al usuario digital, por lo que se elabora el protocolo de atención al ciudadano y usuarios de canales electrónicos y digitales del Concejo Distrital de Cartagena, con el fin de contar con unas pautas para realizar la atención en forma digital y electrónica la prestación de los servicios y trámites que se ofrecen en la página web de la entidad, logrando un 60% de cumplimiento y efectividad en la prestación del trámite o servicio.

De acuerdo al diagnóstico y los objetivos planteados en el desarrollo del proyecto para el eje temáticos seguridad y privacidad de la información encontramos:

- Para el objetivo “verificar el nivel de cumplimiento de la entidad frente a los requisitos del Modelo de Seguridad y Privacidad de la información de la estrategia Gel definiendo las acciones a seguir para su cumplimiento dentro de la entidad”, se verifico el nivel de cumplimiento de la entidad, detallando los controles de acuerdo a los niveles de madurez del MSPI determinando el estado actual de la seguridad de la información en el Concejo Distrital de Cartagena encontrándose en un nivel Inexistente con una calificación de cero (0) lo cual el criterio de valoración de controles significa que existen una total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles. Es necesario un compromiso de la organización que conlleve a crear controles adecuados para minimizar el impacto ante una posible materialización del riesgo.
- “Realizar la asignación de los roles y responsabilidades en la estructura organizacional en cuanto a seguridad y privacidad de la información”. De acuerdo a las entrevistas y el resultado del diagnóstico, se observó que no están definidos las responsabilidades en los temas de seguridad e la información ante esto se realizó un análisis de la estructura organizacional en cuanto a funciones y cargo, se planteó una matriz de roles y responsabilidades, la cual se puede utilizar no solo para el eje temático Seguridad y privacidad de la información sino también para el eje Temático Tic Servicios.
- “Definir las políticas de la Seguridad de la Información de la entidad tomando como base Modelo de Seguridad y Privacidad de la información de la estrategia Gel, que defina las acciones a seguir para el manejo de la información y de los sistemas de información”. La entidad de acuerdo al diagnóstico no posee políticas de seguridad que le garanticen protección a los activos de información exponiendo en alto grado la entidad ante esto y de acuerdo al Modelo de seguridad y privacidad de la información se definieron las políticas generales y específicas de

seguridad de la información para el Concejo Distrital de Cartagena, con el Manual de políticas de Seguridad que encontramos en el anexo 9.

- "Definir el alcance y los objetivos del Modelo de Seguridad y Privacidad de la información de la estrategia Gel para el Concejo Distrital de Cartagena", el alcance y objetivos del modelo se definieron dentro del manual de políticas de seguridad.
- Realizar la clasificación de los activos de información de los procesos de Atención al Usuario, Administrativa y Financiera que permita determinar los riesgos en la seguridad de la información y definir los planes de tratamiento de los riesgos, con el fin de evitar la pérdida de información importante para el funcionamiento de la entidad garantizando la integridad, confidencialidad y disponibilidad de la información", en base al diagnóstico, entrevistas y encuestas realizadas se encontró que no existe un documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección.

Con el fin de cumplir con esta fase se hizo un reconocimiento de los activos de información del Concejo Distrital de Cartagena de Indias, se realizó la identificación de los activos de información en los procesos de atención al usuario, dirección administrativa y dirección financiera, de igual manera se realizó el análisis y gestión de los riesgos de información gestión de riesgos informáticos con la Metodología MAGERIT 37 versión 3.0, esta metodología de la mano con la norma ISO/IEC 27001 de 2013 la cual permite identificar amenazas y estimar impacto y probabilidad de forma cualitativa.
Se definieron las estrategias para proteger la información se establecía un plan de mitigación de riesgo, donde se diseñó los controles para el tratamiento.
Para la caracterización y valoración de los activos de información se realizó un levantamiento del inventario de activos de información existentes en los procesos de atención al usuario, dirección administrativa y dirección financiera. La caracterización y valoración de los activos se realiza de acuerdo al Libro II de la metodología MAGERIT versión 3, en donde nos presenta el catálogo de elementos (Anexo 10).

Una vez realizada la clasificación y valoración de activos, teniendo claridad a los riesgos que se expone la información de la entidad se procedió a identificar las salvaguardas para estos, es imperioso tener claro que sin el acompañamiento de la alta gerencia no se puede implementar los ejes temáticos tanto el de seguridad y privacidad de la información como TIC servicios, por esto es necesario establecer los roles y responsabilidades en la aplicación de las políticas que se establecen dentro del modelo de seguridad y privacidad de la información

Con el desarrollo del presente trabajo se desarrollaron las estrategias para alinear los procesos del Concejo Distrital de Cartagena con la estrategia Gobierno en línea desarrollando documentos que permitan desplegar las estrategias para la implementación del Gobierno en línea en la entidad.

Con las entrevistas y visitas realizadas a la entidad se evidencio el desconocimiento de la normatividad en cuanto a tecnologías de información y comunicación, en especial a los servicios y tramites de la empresa, y la importancia de la seguridad y privacidad de la información, por esto es de vital importación realizar capacitación acerca de esta estrategia a los 50 empleados y 19 Concejales de la organización, sensibilizar e informar las consecuencias de no implementar la Estrategia.

Entendiendo la importancia que la información tiene para la permanencia de las entidades en el mercado, se reconoce esta como uno de los activos más importantes, de ahí la necesidad de poseer medidas de protección que les permitan contar con controles para la prevención y/o actuación en caso de una emergencia o materialización de un riesgo, por esto es imperioso diseñar el eje temático seguridad y privacidad de la información en base al modelo de seguridad y privacidad de la estrategia gobierno en línea para el Concejo Distrital de Cartagena, como una corporación político administrativa que busca cooadministrar el Distrito de Cartagena buscando un interés general para la ciudadanía. Por último, para el Concejo Distrital de Cartagena es muy importante la implementación de la estrategia gobierno en línea en los ejes temáticos Tic servicios y seguridad y privacidad de la información no solo por el cumplimiento normativo si no por la mejora de sus procesos, la mejora en percepción de la ciudadanía acerca de la entidad, y la protección de sus activos de información tal como se ha demostrado en el desarrollo de este trabajo de grado.

RECOMENDACIONES

Se recomienda para la implementación del diseño de los ejes temáticos TIC Servicios y privacidad y seguridad de la información:

- Contar con la participación de la alta gerencia que logre un mayor compromiso por parte de los funcionarios de todas las áreas.
- Que se realice una sensibilización y socialización acerca de la importancia de la estrategia gobierno en línea, conociendo con claridad los ejes temáticos.
- Que se capacite al personal en el manejo de la página web y en la promoción de los trámites y servicios de la entidad.
- Que se incluyan en los trámites y servicios prestados las características de accesibilidad y usabilidad teniendo en cuenta la caracterización de los usuarios.
- Socializar al personal la importancia de los protocolos de atención al ciudadano.
- Se recomienda para el eje temático seguridad y privacidad de la información, el uso de estándares de buenas prácticas en seguridad de la información, buscando las más acordes con la entidad y actualizar constantemente de acuerdo a las necesidades.
- Es necesario implementar el Modelo de seguridad y privacidad de la información, para proteger los activos especialmente el más importante “la información” para esto es necesario contar con personal experto en el área de manera permanente.
- De igual manera es necesario que la entidad desarrolle controles para mitigar los riesgos de seguridad y privacidad de la información.
- Capacitar al personal de sistemas en temas de seguridad informática y estos a su vez capaciten a todos los funcionarios de la entidad, además se debe adoptar y socializar la política de seguridad de la información con el fin de mejorar las prácticas en los sistemas de información.
- Es necesario que dentro de la Oficina Asesora de Control Interno se incluya una persona experta en el área con el fin de realizar auditorías permanentes a los activos de información para actualizar controles y contribuir con el desarrollo de mejores prácticas relacionadas con la seguridad de la información.

- La implementación de la Estrategia Gobierno en línea permitirá un mayor acercamiento estado – ciudadano, logrando la mejora continua de los procesos de atención al ciudadano.

REFERENCIAS BIBLIOGRÁFICAS

- ABRAHAM, S. (200l): «El E-Government: Estrategia para la innovación en el Gobierno Federal. recuperado En www.narxiso.com
- Arnaud Laurans, (2012) Qué es el gobierno electrónico y para qué sirve? Recuperado de http://www.elespectador.com/tecnologia/estos-son-los-beneficios-de-profundizar-la-relacion-entre-tecnologia-y-sector-financiero-articulo-707401
- Asamblea Nacional Constituyente, (1991) Constitución Política de Colombia recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4125
- Asociación Española de La Calidad (2012), Seguridad de la Información recuperado en https://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-INFORMACIÓN
- Ayuntamiento castello 2014. Encuesta de Satisfacción recuperado de http://www.castello.es/web20/archivos/menu0/10/adjuntos/MANUAL%20DE%20EVALUACIoN%20DE%20LA%20SATISFACCIoN%20DEL%20CIUDADANO%20vs8%20CARLOS_20140429060943.pdf
- Ballester Fernández, 2018 GOBIERNO CORPORATIVO TIC recuperado de http://www.isacamty.org.mx/archivo/Standard_ISO38500.pdf
- Castro, Devis y Olivera , 2011 Impacto de las Tecnologías de la Información y las Comunicaciones (TIC) en el Desarrollo y la Competitividad del País recuperado en http://www.fedesarrollo.org.co/wp-content/uploads/2011/08/Impacto-de-las-Tecnolog%C3%ADas-de-la-Informaci%C3%B3n-y-las-Comunicaciones-TIC-Informe-Final-Andesco.pdf
- CERT – Software Engineering Institute (2008). OCTAVE. Disponible en: http://www.cert.org/octave/
- Concejo de Cartagena (2017) “Misión y Visión” recuperado en http://concejocartagena.gov.co/mision-vision/

- Congreso de la Republica (2015) Ley 1755 de 2015 por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=62152
- Congreso de la republica (2003) Plan nacional de desarrollo “Hacia un estado comunitario “recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=8795
- Congreso de Colombia (2009) Ley 1273 de 2009 Delitos informáticos recuperado en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492
- Congreso de Colombia, (2009) Ley 1341 de 2009 recuperado de http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf
- Congreso de la Republica, (2002) Ley 790 de 2002 Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6675
- Congreso de Colombia (2012). Ley 1581 de 2012. Principio de Tratamiento de Datos personales Recuperado en http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html
- Congreso de Colombia (2013). Decreto Reglamentario 1377 de 2013 Datos personales recuperado en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646
- Congreso de la Republica 2011, Código de Procedimiento Administrativo y de lo Contencioso Administrativo recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=41249
- Corletti Alejandro (2006), ISO 27000 Los Controles parte ii Recuperado en http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_II.pdf
- Contraloría Distrital de Cartagena, 2017. Informe de auditoría regular vigencia 2017 archivo oncejo Distrital.
- Contraloría Distrital de Cartagena, (2017). *Informe de Auditoria Modalidad* Regular Vigencia 2015. Cartagena. Archivo Concejo Distrital de Cartagena
- Contraloría Distrital de Cartagena, (2016). Informe de Auditoria Modalidad Regular Vigencia 2014. Cartagena recuperado en

http://contraloriadecartagena.gov.co/wp-content/uploads/2016/04/IDEFINITIVO_CONCEJODECARTAGENA_2014.pdf

- Contraloría Distrital de Cartagena, 2017. Informe preliminar Auditoria Modalidad regular Concejo Distrital de Cartagena.
- Cruz y Martínez (2011) Modelo de Integración entre Mecí y un marco de referencia para Gobierno de TI aplicado a entidades territoriales municipales en Colombia recuperado de https://repository.icesi.edu.co/biblioteca_digital/bitstream/10906/5609/1/modelo_integraci%C3%B3n_meci.pdf
- Dafp 2011, Guía de Administración del Riesgo recuperado de http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba
- David A. Chapin -CISA, CISM, CISSP, IAM- y Steven Akridge -JD, CSM, CM, CISSP, IAM (2005) Cómo puede medirse la seguridad recuperado de http://www.iso27000.es/download/HowCanSecurityBeMeasured-SP.pdf
- Dnp, Gobierno en línea, Secretaria de transparencia presidencia de la Republica, Pnsc (2016). Guía metodológica para la caracterización de ciudadanos, usuarios y grupos de interés recuperado de http://bibliotecanacional.gov.co/es-co/Footer/Estudio%20de%20Usuarios/Guia%20de%20Caracterizaci%C3%B3n%20de%20Ciudadanos.pdf
- Departamento Nacional de Planeación (2004) CONPES 3292 recuperado de http://www.mintic.gov.co/portal/604/articles-3501_documento.pdf
- Duque Ochoa, 2010. Metodología de Gestión de Riesgos, disponible en https://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+de+Gesti%C3%B2n+de+Riesgos.pdf
- Departamento nacional de planeación, (2003) Documento Conpes 3248 de 2003 recuperado de https://www.mintic.gov.co/portal/604/articles-3499_documento.pdf
- El universal (2014) Cartagena pasa a Categoría especial a nivel nacional por finanzas recuperado de http://www.eluniversal.com.co/cartagena/local/cartagena-pasa-categoria-especial-nivel-nacional-por-finanzas-15153

- Enerlis, Ernst and Young, Ferrovial and Madrid Network (2012). Libro blanco recuperado de http://www.innopro.es/pdfs/libro_blanco_smart_cities.pdf
- Fenacon, 2017. Historia de los Concejos Municipales recuperado en https://sites.google.com/site/fenaconcolombia/concejos
- FERNANDEZ, C.(1999) La Comunicación en las Organizaciones. Editorial Trillas, México,
- FISKE, J.(1982) Introducción al Estudio de la Comunicación. Editorial Norma, Colombia
- Funcicar(2016) Observatorio al Concejo de Cartagena de
- Indias y Asamblea de Bolívar Recuperado de http://www.funcicar.org/Observatorio%20al%20Consejo%20de%20Cartagena%20de%20Indias/abc-del-concejo
- Funcicar,2017 recuperado en http://www.funcicar.org/Observatorio%20al%20Consejo%20de%20Cartagena%20de%20Indias/abc-del-concejo
- Kosutic, D(2013). “Lista de documentación obligatoria requerida por ISO/IEC 27001”. Disponible en ISO 27001 Academy: https://advisera.com/27001academy/es/knowledgebase/lista-de-documentos-obligatorios-exigidos-por-la-norma-iso-27001-revision-2013/
- KREPS, G. L (1995) La Comunicación en las Organizaciones. Addison-Wesley Iberoamericana, España
- Gallardo y Moreno(1999) Aprender a Investigar Modulo 3 recuperado de http://www.unilibrebaq.edu.co/unilibrebaq/images/CEUL/mod3recoleccioninform.pdf
- Gallo Oñate, 2014, Diagnóstico de cumplimiento del modelo gestionado por el sistema de administración de la seguridad de la información de gobierno en línea – sasigel alineado con la norma 27000 para el instituto nacional de formación técnica profesional de la guajira
- Gobierno de España, (2012) MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información recuperado de

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WSNGX5KGOvE

- Gonzales Agudelo (2014) el riesgo y la falta de políticas de seguridad informática una amenaza en las empresas certificadas Basc recuperado en http://repository.unimilitar.edu.co/bitstream/10654/12251/1/ENSAYO%20FINAL.pdf
- H, F y Baptista, (2003). Metodología de la Investigación recuperado en https://www.esup.edu.pe/descargas/dep_investigacion/Metodologia%20de%20la%20investigaci%C3%B3n%205ta%20Edici%C3%B3n.pdf.
- 5482_Modelo_de_Seguridad_Privacidad.pdf
- Instituto andaluz de tecnología, 2007 Guía para la medición directa de la satisfacción de los clientes recuperado de http://madridexcelente.com/wp-content/uploads/2015/08/GUIASATISFACCION.pdf
- ISO/IEC 27000:2014, Tercera Edición, Pág. 4
- López Neira y Ruiz Spohr, (2012) recuperado en (Iso 27000, (http://www.iso27000.es/download/doc_sgsi_all.pdf, 2017)
- Lozada, (2014) Investigación Aplicada: Definición, Propiedad Intelectual Recuperado en http://www.gobiernoenlinea.com.co/app/webroot/index.php/intradocuments/webExplorer/documentos-de-gobierno-en-linea
- Ministerio de Comunicaciones (2000) Documento Conpes recuperado de http://www.mintic.gov.co/portal/604/articles-3499_documento.pdf
- Mintic, 2018 CONOCE LA ESTRATEGIA DE GOBIERNO EN LÍNEA recuperado de http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.html
- Mintic(2015) Guía de datos abiertos en Colombia recuperado de http://estrategia.gobiernoenlinea.gov.co/623/articles-9407_Guia_Apertura.pdf
- Mintic (2011) GUÍA PARA LA CARACTERIZACIÓN DE USUARIOS DE LAS ENTIDADES PÚBLICAS http://estrategia.gobiernoenlinea.gov.co/623/articles-8536_recurso_1.pdf
- Mintic, 2011. Guía de diseño e implementación de servicios por múltiples canales recuperado de http://www.vive.gobiernoenlinea.gov.co/apc-aa-

files/da4567033d075590cd3050598756222c/MultiplesCanales_GuiaDise_oV1.0_2011.pdf

- Mintic (2008), Decreto 1151 de 2008 por medio del cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia recuperado de http://artesaniasdecolombia.com.co/Documentos/Contenido/8561_decreto_1151_de_2008.pdf
- Mintic, (2008) decreto 1151 recuperado de http://www.mintic.gov.co/portal/604/articles-3643_documento.pdf
- Mintic (2008) Manual para la implementación de la estrategia de gobierno en línea de la república de Colombia recuperado de http://www.cordoba.gov.co/v1/gobierno_en_linea/manual_gobierno_en_linea_2008.pdf
- Mintic (2011) Guía para la caracterización de usuarios de las entidades públicas. Mintic recuperado en http://estrategia.gobiernoenlinea.gov.co/623/articles-8536_recurso_1.pdf
- Mintic (2011) Guía de atención al ciudadano cliente por múltiples canales recuperado de http://estrategia.gobiernoenlinea.gov.co/623/articles-7995_archivo_pdf.pdf
- Mintic(2012) Manual para la implementación de la estrategia de gobierno en línea de la república de Colombia recuperado de http://www.minambiente.gov.co/images/tecnologias-de-la-INFORMACIÓN-y-comunicacion/pdf/minticmanual3.1.pdf
- Mintic(2014) Decreto 2573 recuperado en https://www.mintic.gov.co/portal/604/articles-14673_documento.pdf
- Mintic(2015) Manual Estrategia de Gobierno en Línea recuperado de http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf
- MINTIC (2015). Arquitectura TI Marco de Referencia Colombia. Obtenido de Arquitectura TI Marco de Referencia Colombia: http://www.mintic.gov.co/marcodereferencia/624/w3-channel.html

- Mintic (2016) informe 2013-2016 de gestión estrategia ti Colombia recuperado de http://www.consultorsalud.com/sites/consultorsalud/files/informe_gestion_estrategiati.pdf
- Mintic (2017) Estrategia Gobierno en Línea http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.html
- Mintic (2017) Gobierno en Línea recuperado de http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.html. (2017). Mintió (2016) Modelo de seguridad y privacidad de la información recuperado de Recuperado en https://www.mintic.gov.co/gestionti/615/articles-International
- Mintic, (2017)Para qué es el Marco de Referencia recuperado de http://www.mintic.gov.co/arquitecturati/630/w3-article-9443.html
- Mintic 2017,Preguntas arquitectura TI recuperado de http://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8171.html
- Mintic (2016) Guía N°4 Roles y Responsabilidades Seguridad y privacidad de la información recuperado en https://www.mintic.gov.co/gestionti/.../articles-5482_G4_Roles_responsabilidades.pdf
- Sánchez Nicolás, Segura Juan (2006). Una guía metodológica para el cálculo del retorno a la inversión (ROI) en seguridad informática. Un caso de estudio recuperado de http://escuelainformatica.uniacc.cl/wordpress/wp-content/uploads/2013/12/ROIs.pdf
- Telecommunication Union Plac des Nations, (2015). *Measuring the Information Society Report*. Recuperado en http://www.itu.int/en/ITU-D/StatisTIC/Documents/publications/misr2016/MISR2016-w4.pdf
- ISO, (2005). Sistema de Gestión de Seguridad de la Información recuperado en http://www.iso27000.es/index.html
- Mintic, (2016). Roles y responsabilidades Seguridad y privacidad de la Información – Guía Numero 4 (pag7-8). Recuperado en http://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

- Ocampo, Fernando (2003): «El gobierno electrónico: ¿reforma de última generación? En Revista Electrónica de Derecho Informático (REDI)dell ° de julio de 2003. www.alfa...redi.org
- PASQUALI A (1978) ., Comprender la Comunicación, Monte Ávila Editores
- Peraza Henríquez, (2010) PROPUESTA DE UN MODELO GERENCIAL ESTRATÉGICO SOCIALMENTE RESPONSABLE BASADO EN EL GOBIERNO ELECTRÓNICO PARA LA GESTIÓN DE LOS GOBIERNOS LOCALES EN EL ESTADO ARAGUA recuperado de http://mriuc.bc.uc.edu.ve/bitstream/handle/123456789/580/aperaza.pdf?sequence=1
- Periódico el Tiempo, (2015) Seis de cada 10 colombianos interactúan con el Estado por Internet recuperado de http://www.eltiempo.com/archivo/documento/CMS-16432817
- Presidencia de la republica (2000) Directiva presidencial 002 de 2000 recuperado de https://www.mintic.gov.co/portal/604/articles-3646_documento.pdf
- Presidencia de la Republica, (2002) Directiva presidencial 010 de 2002 recuperado de http://www.mintic.gov.co/portal/604/articles-3652_documento.pdf
- Pulido Daza y Tibaduiza Ávila (2013) Dificultades técnicas para la implementación de la nueva normativa en el desarrollo de la estrategia de gobierno en línea y la gestión documental en Colombia: decretos 2578 y 2609 de 2012 (AGN) y 2693 de 2012 (mintic) recuperado de https://revistas.lasalle.edu.co/index.php/co/article/download/2704/2323
- Pulido y Mantilla, (2016) Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina TIC de la alcaldía municipal de Fusagasugá recuperado de http://repository.unad.edu.co/bitstream/10596/6327/1/35250225.pdf
- Pnud 2015 Objetivos de Desarrollo del Milenio informe 2015 recuperado de http://www.co.undp.org/content/dam/colombia/docs/ODM/undp-co-odsinformedoc-2015.pdf
- Naciones unidas (2012) Estudio de las Naciones Unidas sobre el Gobierno Electrónico recuperado de

https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2012-Survey/Complete-Survey-Spanish-2012.pdf

- Naciones unidas (2014) Informe 2014 de Naciones Unidas sobre Gobierno Electrónico http://www.casatic.org/wp-content/uploads/2015/03/Informe-de-las-naciones-unidades-sobre-gobeirno-electronico-2015.pdf
- NTC-ISO-IEC 27001: 2013. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Recuperado en https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27001.pdf
- NTC-ISO-IEC 27001: 2013 recuperado https://es.wikipedia.org/wiki/ISO/IEC_27001
- Ramón Voces Merayo. (2011) Rich Internet Applications (RIA) y Accesibilidad Web [on line]. "Hipertext.net", núm. Recuperado de http://www.upf.edu/hipertextnet/numero-9/ria-accesibilidad-web.html
- Red GEALC, SEDI- OEA y ICA / IDRC (2008) De la teoría a la práctica: Cómo implementar con éxito el gobierno electrónico. Recuperado de redgealc.org/download.php len=es&id=1502&nbre=frick.pdf&ti.../pdf...
- Revista Edu – Física. LAS ACTITUDES recuperado de http://www.edu-fisica.com/Formato.pdf
- Rodríguez Gladys (2004). Gobierno Electrónico: hacia la modernización y transparencia de la gestión pública recuperado en http://ciruelo.uninorte.edu.co/pdf/derecho/21/1_GOBIERNO%20ELECTRONICO_DERECHO_No%2021.pdf
- Rodríguez, Flores y García (1996). Metodología de la Investigación Cualitativa recuperado en http://metodosdeinvestigacioninterdisciplinaria.bligoo.com.co/media/users/10/528344/files/53953/INVESTIGACION_CUALITATIVA_Rodriguez_et_al.pdf
- Rojas Soriano, R. (1981). Guía para realizar investigaciones sociales. México, DE: Universidad Nacional Autónoma de México. Sexta Edición
- Sandoval y Massal (2010) Gobierno electrónico. ¿Estado, ciudadanía y democracia en internet? Recuperado de

http://www.scielo.org.co/scielo.php?script=sci_abstract&pid=S0121-47052010000100001&lng=es

- Sánchez torres, Carlos Ariel, rincón cárdenas, Erick. (2012) Municipio digital y gobierno electrónico. Universitas. Disponible en: http://www.javeriana.edu.co/juridicas/pub_rev/documents/21ariel
- Sánchez y Rincón (2015) Gobierno electrónico, en el contexto local de la administración colombiana recuperado de http://repository.usergioarboleda.edu.co/bitstream/handle/11232/279/CienciasSocialesyHumanas473.pdf?sequence=1
- Secretaria general de Bogotá (2009) Concepto 41 de 2009 Secretaría General Alcaldía Mayor de Bogotá D.C recuperado de .http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=38222
- Symons, C. (2005) “IT Governance Framework: Structures, Processes, and Communication”. Disponible en Forrester Research: (http://i.bnet.com/whitepapers/051103656300.pdf)
- Sitio Web de TAW, Test de Accesibilidad Web, http://www.tawdis.net/tools/accesibilidad/?lang=es-
- Tarazona Cesar, (2007) Amenazas informáticas y seguridad de la información. Universidad Del Externado, 137. Recuperado en http://revistas.uexternado.edu.co/index.php/derpen/article/download/965/91
- Unam, 2017 Definiciones e historia de la seguridad informática recuperado de http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/217/A4.pdf?sequence=4.
- Uribe Vélez (2002) Decreto 2170 de 2002 recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5798
- Zaid Agustín (2014) cuadro comparativo de normas y estándares ti recuperado de https://agustinzaidti.wordpress.com/2014/09/20/cuadro-comparativo-de-normas-y-estandares-ti/
- Yusef Hassan & Francisco J. Martín Fernández & Ghzala Iazza. (2004) Diseño *Web Centrado en el Usuario: Usabilidad y Arquitectura de la Información* [en línea]. "Hipertext.net", recuperado http://www.hipertext.net

- W3C España, Guía breve de accesibilidad recuperado en https://www.w3c.es/Divulgación/GuiasBreves/Accesibilidad
- Zapata y Pineda (2014) LA GESTIÓN DOCUMENTAL ELECTRÓNICA EN LA ESTRATEGIA DE GOBIERNO EN LÍNEA: ANÁLISIS DEL COMPONENTE GOBIERNO –CIUDADANO recuperado de http://repository.lasalle.edu.co/bitstream/handle/10185/18020/33032651_2014.pdf?sequence=3

GLOSARIO DE TÉRMINOS Y DEFINICIONES

- **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000)
- **Activo de Información**: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Accesibilidad**: Busca que los trámites y servicios disponibles por medios electrónicos cuenten con las características necesarias para que toda la población pueda acceder a ellos, incluso aquella que se encuentra en situación de discapacidad. (Mintic, 2015)
- **Análisis de riesgos de seguridad de la información**: Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.
- **Autenticidad**: Permite que la información transmitida o intercambiada provenga de fuentes auténticas y de quiénes dicen ser que son.
- **Autenticación**: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
- **Confidencialidad**: Protege a la información de que esté disponible a usuarios, entidades o procesos no autorizados.
- **Centros de cableado**: Es el lugar donde se instalan los cables y dispositivos de comunicación. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y

techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

- **Cifrado**: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.
- **Confidencialidad**: Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
- **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- **Criptografía**: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.
- **Custodio**: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado (ISO/IEC 27002:2013)
- **Datos abiertos**: Son todos aquellos datos primarios (sin procesar) que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos. (Mintic, 2015)
- **Derechos de Autor**: Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

- **Derecho a la Información**: Derecho constitucionalmente reconocido que tiene toda persona de buscar, recibir y difundir información. (Mintic, 2015)
- **Disponibilidad**: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. (ISO/IEC 27002:2013)
- **Equipo de cómputo**: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.
- **Evaluación de la satisfacción de los usuarios**: Busca conocer el grado de satisfacción de los distintos usuarios respecto a la oferta de trámites y servicios electrónicos habilitados por la entidad. (Mintic,2015)
- **Gobierno en línea**: Gobierno en Línea es una estrategia definida por el Gobierno Nacional mediante el Decreto 1151 de 2008, que pretende lograr un salto en la inclusión social y en la competitividad del país a través de la apropiación y el uso adecuado de las Tecnologías de la Información y las Comunicaciones (Mintic, 2015)
- **Incidente de Seguridad**: Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).
- **Integridad**: Permite que la información sea correcta y que no haya sido alterada por usuarios, entidades o procesos no autorizados. Propiedad de salvaguardar la exactitud y estado completo de los activos (ISO/IEC 27002:2013)
- **Licencia de software**: Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.
- **Medios removibles**: Todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores.
- **Perfiles de usuario**: Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos

tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

- **Promoción**: Busca aumentar el conocimiento, uso y preferencia de trámites y servicios electrónicos por parte de los usuarios internos y externos. (Mintic,2015)
- **Propiedad intelectual**: es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.
- **Propietario de la información**: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso (ISO/IEC 27002:2013)
- **Recursos tecnológicos**: Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior del Concejo Distrital De Cartagena de Indias.
- **Registros de Auditoría**: Son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos del instituto. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o

ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

- **Responsable por el activo de información**: Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.
- **SGSI**: Sistema de Gestión de Seguridad de la Información.
- **Sistema de información**: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por el Concejo Distrital de Cartagena de Indias o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.
- **Software malicioso**: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.
- **Tramite**: Conjunto o serie de pasos o acciones reguladas por el Estado, que deben efectuar los usuarios para adquirir un derecho o cumplir con una obligación prevista o autorizada por la ley. El trámite se inicia cuando ese particular activa el aparato público a través de una petición o solicitud expresa y termina (como trámite) cuando la administración pública se pronuncia sobre éste, aceptando o denegando la solicitud. (Mintic, 2015)
- **Tramite en línea**: Trámite que puede ser realizado por medios electrónicos a través del portal de una entidad, ya sea de manera parcial, en alguno de sus pasos o etapas, o total, hasta obtener completamente el resultado requerido. (Mintic, 2015)
- **Terceros**: Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

- **TIC Servicios**. Comprende la provisión de trámites y servicios a través de medios electrónicos, enfocados a dar solución a las principales necesidades y demandas de los usuarios y empresas, en condiciones de calidad, facilidad de uso y mejoramiento continuo. (Mintic, 2015).
- **Radicado**: Asignación de las PQR y Derechos de Petición recibidos por la entidad a través del Sistema de Gestión Documental o dependencia asignadas, donde se incluye fecha, hora y un número consecutivo. (Mintic, 2015).
- **Reclamo**: Es la solicitud dirigida a la instancia competente, para que se revisen, ajusten o modifiquen los resultados obtenidos por el cliente frente a un servicio requerido por él y que son motivo de su inconformidad. (Mintic, 2015).
- **Usabilidad**: Busca que los trámites y servicios disponibles por medios electrónicos sean de fácil uso, y proporcionen una mejor experiencia a los usuarios, ciudadanos y grupos de interés. (Mintic, 2015).
- **Ventanilla única virtual**: Sitio virtual desde el cual se gestiona de manera integrada la realización de trámites que están en cabeza de una o varias entidades, proveyendo la solución completa al interesado. (Mintic, 2015)
- **Vulnerabilidades**: son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por el instituto (amenazas), las cuales se constituyen en fuentes de riesgo.