PROYECTO DE PRINCIPIO, POLÍTICA Y LINEAMIENTOS DE CONSULTAS DE INFORMACIÓN DE LA "MAESTRA DE USUARIOS"

TRABAJO DE GRADO

WILLIAM MAURICIO ATEHORTUA GARCIA

RAFAEL FRANCISCO REYES ALVAREZ

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2015

PROYECTO DE PRINCIPIO, POLÍTICA Y LINEAMIENTOS DE CONSULTAS DE INFORMACIÓN DE LA "MAESTRA DE USUARIOS"

TRABAJO DE GRADO

WILLIAM MAURICIO ATEHORTUA GARCIA

RAFAEL FRANCISCO REYES ALVAREZ

Asesor
Giovanny Andres Piedrahita Solorzano

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2015

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Bogotá, 06 de noviembre de 2015

INTRODUCCIÓN

Guardar y proteger la información de cualquier entidad es una labor que implica gran esfuerzo y trabajo; más aún cuando ésta se encuentra protegida por las leyes de nuestro país; debido a estas situaciones se hace necesario el establecimiento de principios, políticas y lineamientos al uso de la información lo cual permite a los actores y usuarios interesados tener reglas claras sobre el alcance que tienen ellos en cada una de las tareas que se llevan a cabo dentro del sistema.

De igual forma, al implementar esta documentación, se definen protocolos de seguridad que permiten garantizar el acceso de la información junto con las características del sistema a los usuarios interesados según las funciones que lleven a cabo y su nivel jerárquico en la entidad.

Otra característica importante que beneficiará el manejo de la información, es poder hacer seguimiento y monitorear las actividades que llevan a cabo cada uno de los usuarios en el sistema con el fin que estas sean controladas y se detecten hechos fraudulentos que pueden ser nocivos para el buen uso de la información al igual que la reputación de la entidad.

Un elemento que apoya todo el marco de seguridad de la información es la disponibilidad de la información; hay que tener en cuenta que éste va de la mano con la confiabilidad de los datos ya que ellos son parte fundamental en el análisis de la entidad, extracción de indicadores y toma de decisiones por parte de los interesados.

Por último, la implementación de todas estas características y medidas en la organización dará a los directivos de la organización la capacidad de generar indicadores estratégicos, misionales y tácticos dentro del sistema y así tener un panorama de la manera en que se comporta la información, analizar necesidades nuevas, desechar funcionalidades no existentes y modificar las políticas o lineamientos de funcionamiento de la aplicación justificados en los sensores y alertas programados para dicho fin.

AGRADECIMIENTOS

El gran científico Nikola Tesla inmortalizó una gran frase que dice: “Nuestras virtudes y nuestros defectos son inseparables, como la fuerza y la materia. Cuando se separan el hombre no existe”.

Éste proyecto es fruto de combinaciones (el trabajo, el estudio y la familia) que en principio no son compatibles; pero sin la existencia de alguno de ellos, su realización no tendría ningún sentido y pasaría a la historia como un documento más.

Primero que todo a Dios, a nuestras familias, a nuestros padres que han dado un impulso gigantesco en esta nueva travesía; pese a dificultades y con mucha paciencia han servido de apoyo en este largo camino lleno de conocimientos y aprendizajes. Sin ellos, difícilmente la meta se hubiera cumplido. “Porque todo lo que sucede, sucede para bien.”

A Giovanny Andres Piedrahita Solorzano profesor de la Institución Universitaria Politécnico Grancolombiano por las orientaciones y asesorías en el desarrollo del trabajo.

A nuestros docentes que durante el trascurso de la especialización, siempre estuvieron dispuestos a brindarnos su conocimiento a nivel personal y profesional.

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

LISTA DE TABLAS

1. RESUMEN EJECUTIVO

1.1. Descripción general

La entidad cuenta con una aplicación administradora del sistema de información que se encarga de cargar, validar y centralizar la información básica disponible de todos los usuarios que son beneficiados por parte de la entidad; sin embargo, esto ha generado cuestionamientos y debates al interior de la misma sobre las personas que pueden ingresar a la aplicación, los accesos que los trabajadores tienen sobre las funcionalidades que tiene y los controles que se deben establecer para evitar el uso indebido de la información.

Si bien, es claro el funcionamiento, los requisitos y la responsabilidad del uso de dicha información; dichos procesos no se encuentran documentados y tampoco está delimitado por alguna normatividad que evite la configuración del sistema de manera subjetiva, afectando la integridad, funcionamiento y la visión de la aplicación.

Es importante definir de manera urgente el protocolo de funcionamiento de la aplicación, sus principios, políticas y lineamientos en virtud de garantizar el objetivo con el cual fue concebido y evitar la manipulación fraudulenta de información que pueda afectar la integridad de los funcionarios y de la organización.

Las características disponibles a la fecha en la aplicación son las siguientes:

- Carga de información de usuarios.
- Parametrización de características del sistema (Permisos, entorno gráfico, configuraciones de carga entre otros).
- Consulta de Hoja de Vida.
- Tablero de Control de Usuarios.
- Herramienta de Cruce de Información.
- Reportes Personalizados.
- Tablero de Control de la Maestra (Indicadores).

De igual manera, se han identificado actores relevantes los cuales cumplen una función importante en la definición e identificación de los problemas de la entidad. Son ellos los que día a día tienen que luchar con el sistema para cumplir sus funciones o pueden brindar recomendaciones útiles para mejorar y asegurar los procesos de consulta de información de la Maestra de usuarios.

Aquí realizamos una descripción de los actores relevantes involucrados en el proceso:

- JEFES DE OFICINAS Y DIRECTORES MISIONALES: Son aquellos actores cuya función se concentra en el análisis de la información consolidada, indicadores y toma de decisión de acuerdo a los datos extraídos del sistema; sobre ellos recae la decisión estratégica y los lineamientos de la entidad.

- DIRECTORES REGIONALES: Son los actores encargados de representar a la entidad en los eventos que se llevan a cabo en el territorio. En la actualidad existen 35 Direcciones Regionales distribuidas de tal forma que 32 corresponden a territorios departamentales y 3 que poseen características especiales de atención a la población. Son los responsables de dar respuesta a las consultas de Hoja de Vida disponible en la aplicación en el territorio.

- ADMINISTRADORES DEL SISTEMA: Son actores que realizan las operaciones de parametrización, configuración y carga de la información entregada por cada una de las entidades involucradas en el sector. Por ser administradores del sistema, tienen la posibilidad de realizar consultas y reportes desde cualquiera de las funcionalidades del sistema. Estos actores trabajan para la Oficina de Tecnologías de la Información como ingenieros de Sistemas especializados en Inteligencia de Negocios.

- ANALISTAS DE INFORMACIÓN: Estos actores, además de realizar consultas desde la hoja de vida del sistema y el cruce de información, tienen la posibilidad de generar reportes personalizados para analizar de manera predeterminada o dinámica el comportamiento de la información y los datos que han sido suministrados por cada una de las Direcciones Misionales del Sector.

- CONSULTORES DE INFORMACIÓN: Estos actores sólo tienen la posibilidad de consultar información a partir de la funcionalidad de la Hoja de Vida del sistema. Por lo general, estos actores no pertenecen a un alto nivel jerárquico en la entidad lo cual impacta su nivel de responsabilidad con la información y trabajan en territorio.

1.2. Objetivos

Objetivo General

Definir el principio, política y lineamientos necesarios para el buen funcionamiento y la gobernanza de la información contenida en la “Maestra de Usuarios” contenida en la entidad.

Objetivos Específicos

- Analizar las características tanto de las fuentes de información recolectadas para la carga en la “Maestra de Usuarios” como la información publicada en cada una de las funcionalidades de la herramienta.

- Diseñar el documento que permita establecer la gobernanza de información de la “Maestra de Usuarios” que funciona en la entidad.

- Establecer los indicadores de gestión que permitan analizar los avances y dificultades en la aplicación de la gobernanza de la información de la “Maestra de usuarios” de la entidad.

1.3. Alcance

El alcance del Proyecto de principio, política y lineamientos de consultas de información de la “maestra de usuarios” se llevará a cabo en las instalaciones del Departamento Administrativo para la Prosperidad Social y estará acompañado por la Oficina Asesora de Planeación, Monitoreo y Evaluación al igual que la Oficina de Tecnologías de la Información; estas oficinas son las encargadas de hacer seguimiento y verificar todo lo relacionado con el tema de información en la entidad.

Teniendo en cuenta que la Entidad es de carácter gubernamental, ésta debe seguir los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones en el documento de Modelo de Seguridad de la Información para la Estrategia Gobierno en Línea 2.0 el cual es coherente con los lineamientos del estándar NTC:ISO/IEC 27001:2005.

El proyecto contempla la entrega de la toda la documentación relacionada con el levantamiento de los requerimientos por parte de cada uno de los actores involucrados en el proceso, las encuestas, definición de alcance, definición de política, gestión de riesgos y definición de indicadores, métricas y medidas del lineamiento con el fin de cumplir con el Nivel Inicial del Plan de Seguridad establecido en el Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0; el proceso de implementación se llevará a cabo a comienzos del año 2016 debido a que la entidad se encuentra en un proceso de transición.

1.4. Resultados esperados

Con la implementación del Proyecto de principio, política y lineamientos de consultas de información de la “maestra de usuarios” lograremos dar una visión objetiva y a largo plazo al funcionamiento del sistema aplicando los requerimientos necesarios para que el mismo posea un documento de

gobierno de datos que permita su control, seguimiento, monitoreo y sustentación a lo largo del tiempo.

Para conseguir estos resultados, se han establecido una serie de documentos que permitirán identificar los requerimientos de la entidad y plasmar el gobierno de datos necesario para el buen funcionamiento del sistema; estos documentos son:

- Documento de identificación de responsables
- Análisis de encuestas
- Documento de definición de brechas
- Plan de trabajo para reducción de brechas
- Documento de definición del alcance del sistema
- Documento de definición de las políticas del sistema
- Documento de Gestión de Riesgos
- Documento de definición de indicadores, métricas y/o medidas de desempeño

Con estos documentos se pretende obtener los siguientes resultados sobre la información del sistema:

- Disminuir la cantidad de registros consultados de manera no permitida o no autorizada sobre el sistema.
- Disminuir la cantidad de información modificada de manera no permitida sobre el sistema.
- Reducir la cantidad de fallas en la asignación de permisos sobre los usuarios del sistema.
- Aumentar la cantidad de capacitaciones y entrenamientos sobre los usuarios que usan la aplicación.
- Mejorar la calidad de la información almacenada en el repositorio de la Maestra de Usuarios
- Auditar las modificaciones realizadas sobre los registros en el momento que se realiza una carga de información por parte de los programas misionales.

1.5. Cronograma

El cronograma va en función a los entregables del proyecto, los cuales se encuentran en las etapas de Preparación, Análisis, Planeación y Ejecución (como se puede ver en el Anexo 2. Cronograma).

2. JUSTIFICACIÓN

El Departamento para la Prosperidad Social (D.P.S.) ha implementado y puesto en marcha un Sistema de “Maestra de Usuarios” con el fin unificar la población atendida en el Sector Social y la Reconciliación. Éste proceso no tuvo incidentes hasta el momento en el cual se encontraron problemas jurídicos que evidenciaron que antes de la realización de la misma debía ser necesario una serie de protocolos, principios, políticas y lineamientos de la información llamados Gobierno de la Información o Arquitectura de Información para solucionar de manera sencilla y conociendo el impacto que esto tiene sobre la aplicación (U otras arquitecturas de la aplicación).

La definición de principios, políticas y lineamientos de consultas de información de la “Maestra de Usuarios” dará una guía de las características y el comportamiento que poseen los registros que se cargan, cómo se deben exponer y proteger a cada uno de los diferentes usuarios que interactúan en la aplicación; igualmente brindará documentación a cualquier usuario para éste conozca el impacto que se origina con los cambios de criterios o características en la información cargada y así no entorpezca la operación que se lleva a cabo.

Esta definición servirá de marco para otras aplicaciones, programas y entidades que necesiten documentar su proceso de arquitectura de información, unificando los diferentes criterios que se deben tener en cuenta para la carga de los registros y su publicación dependiendo de las reglas de negocio existentes en cada una de ellas. También se promoverá una cultura a las buenas prácticas de documentación de los sistemas de información y gracias a esto se conocerá el impacto que tiene la modificación de un criterio de información sobre las diferentes arquitecturas que componen la arquitectura empresarial.

Todo esto con el objetivo principal de “gobernar” de manera apropiada la información haciendo seguimiento al comportamiento que esta posee y cómo la información puede brindar a la dirección un argumento de decisión justificado para la mecánica de operación; así, los recursos que se administran en la entidad serán aprovechados y ejecutados tomando como base los principios de equidad, paz y educación para la población colombiana.

3. MARCO TEÓRICO Y REFERENTES

3.1. Antecedentes

El Departamento Administrativo para la Prosperidad Social (D.P.S.), es una entidad de orden nacional, conformada por 5 entidades adscritas (Agencia Nacional para la Superación de la Pobreza Extrema – ANSPE, Unidad para la Atención y Reparación Integral a Víctimas – UARIV, Unidad para la Consolidación Territorial – UCT, Instituto Colombiano de Bienestar Familiar – ICBF, Centro de Memoria Histórica – CMH) creada por el gobierno el 3 de Noviembre de 2011 a través del Decreto 4155 de 2011; en este decreto, a través del artículo 13 se crea la Oficina de Tecnologías de la Información y se determinan las funciones entre las cuales se encuentra en el ítem 5 "Administrar una plataforma unificada de los sistemas de información del Departamento Administrativo que permita articular las diferentes fuentes de información del Sector Administrativo de Inclusión Social y Reconciliación en una sola herramienta de gestión, que permita efectuar análisis de información con procesamiento en tiempo real"; esta función se debe realizar de manera compartida con la Oficina Asesora de Planeación, Monitoreo y Evaluación como lo determina el artículo 14 del decreto en el ítem 5 que indica: "Promover una cultura de gestión, calidad, uso y valor de la información como bien de uso colectivo y público".

Con el firme propósito de cumplir con esta función en conjunto, la entidad realizó un entrenamiento de "Arquitectura Empresarial" con aquellos funcionarios encargados de cumplir estas funciones entre octubre y diciembre de 2012; como resultado de este entrenamiento (entre los cuales se encontraba el gobierno de información), se determinó que la entidad tenía dos debilidades que tenían que ser solucionadas a la brevedad: Problemas de infraestructura y problemas con la información.

Se evidenció que los problemas de información habían aumentado con la creación del Departamento Administrativo para la Prosperidad Social, ya que anteriormente la Alta Consejería para la Acción Social y Cooperación Internacional (Actual D.P.S) manejaba programas los cuales estaban sujetos directamente a la Alta Consejería pero dichos programas se convirtieron en entidades adscritas por lo cual cada una de ellas tenía independencia en su funcionamiento.

En el año 2013 empezó el proceso de licitación y modernización de equipos de infraestructura los cuales serían utilizados para los nuevos desarrollos que se licitaron y desarrollaron en el año 2014 mejorando el funcionamiento de algunos procesos estratégicos en la entidad; sin embargo, dichos desarrollos se realizaron sin políticas y lineamientos de gobierno de datos (entre otras características) generando incertidumbre y malestar en algunos funcionarios porque la gobernanza de los datos se realiza de manera informal, desorganizada y arbitraria.

La entidad ha llevado a cabo a finales de 2014 la publicación de documentos que indican las políticas y algunos lineamientos informáticos, sin embargo, estos lineamientos dejan serios vacíos en el manejo de la información por lo que cada persona nueva que llega a administrar las principales herramientas de la entidad asume el manejo de estas como mejor le convenga sin importar el impacto que pueda tener sus modificaciones.

En la actualidad, no existe una política, lineamiento, directriz o algo parecido que permita controlar o hacer seguimiento de manera oficial a la información que se encuentra almacenada por parte de la organización y una de las herramientas más afectada por esta ausencia es el sistema que administra la Maestra de usuarios.

3.2. Conceptos teóricos y Conceptual

Para el desarrollo del siguiente trabajo de grado, es necesario investigar y colocar en contexto algunos aspectos teóricos que serán utilizados para su desarrollo. Los conceptos que se tratarán en el documento serán los siguientes:

3.2.1. Activo de información

Existen diferentes conceptos sobre la definición de activo de información, sin embargo, todos llegan a la misma conclusión y es que el activo de información, como lo indica su concepto, gestiona información y adicional a ello dicha información brinda un valor agregado a la organización. En resumidas cuentas, podemos ajustarnos a la definición dada por la norma ISO 27001:2005 en los términos y definición que dice: “cualquier cosa que tenga valor para la organización” (Organización Internacional de Estándares, 2005). Es por ello, que dependiendo de la organización, podemos indicar que un activo de información es un archivador y para otra, el mismo archivador no posee ninguna importancia.

3.2.2. Estrategia de Gobierno en Línea 3.0

Es una estrategia del gobierno colombiano iniciada en el año 2008 a través del decreto 1151 que definió los lineamientos generales de la Estrategia de Gobierno en Línea. El propósito fundamental de dicha estrategia de Gobierno

es "… contribuir a la construcción de un Estado más eficiente, más transparente y participativo y que presta mejores servicios con la colaboración de toda la sociedad, mediante el aprovechamiento de las TIC. Lo anterior, mediante el logro de cuatro objetivos específicos:

- Facilitar la eficiencia y colaboración en y entre las entidades del Estado, así como con la sociedad en su conjunto.
- Contribuir al incremento de la transparencia en la gestión pública.
- Promover la participación ciudadana haciendo uso de los medios electrónicos.
- Fortalecer las condiciones para el incremento de la competitividad y el mejoramiento de la calidad de vida" (Ministerio de Tecnologías de la Información y las Comunicaciones, 2008)

Dado esta normatividad, las entidades gubernamentales están en la obligación de implementar estrategias que cumplan los lineamientos descritos en cada uno de los decretos y anexos dispuestos para el mismo.

3.2.3. Amenaza

Podemos definir que una amenaza es todo lo que puede causar un riesgo para la organización en sus diferentes áreas o dimensiones. Cada organización es libre de determinar la calificación de las mismas teniendo en cuenta que su mala calificación puede incurrir en un riesgo para la misma. Podemos ajustarnos a la definición indicada en la Metodología de Magerit la cual nos indica: "Las amenazas son cosas que ocurren. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño." (Administración Electrónica, 2006)

Al lograr identificar las amenazas podemos definir de una forma más precisa la gobernanza que debe tener el sistema de información.

3.2.4. C.D.P.

También llamado en el gobierno Certificado de Disponibilidad Presupuestal, es un documento que da constancia que existe una apropiación disponible para ser usado; esto quiere decir, que existe un monto de dinero disponible para ser ejecutado por parte del responsable financiero de la entidad de acuerdo al rublo asignado por el Ministerio de Hacienda.

3.2.5. Confidencialidad

La confidencialidad es un aspecto importante en la seguridad de la información. Como lo define la norma técnica ISO 27001:2005, la confidencialidad es "la propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados".

Si no se puede garantizar la confidencialidad de la información, la organización se puede involucrar en problemas judiciales y de reputación costosas para gobierno que es el responsable de la entidad.

3.2.6. Disponibilidad

La información debe encontrarse en el momento que se necesita siempre y cuando tenga permisos para ello; es por ello que este atributo de la seguridad de la información es importante. A ninguna persona le gusta esperar mucho tiempo sobre algún tipo de consulta y por ello esto se debe responder de manera adecuada y en los tiempos adecuados. La norma técnica ISO 27001:2005 define este atributo como “la propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada” (Organización Internacional de Estándares, 2005).

3.2.7. Información

Dar una definición de información no es sencillo, pero si consolidamos todos los conceptos relacionados a la informática, podemos concluir que es el conjunto de registros o datos que poseen algún tipo de organización y es utilizada para un fin específico. La información tiene diferentes características y atributos por los cuales se puede clasificar los cuales deben ser tenidos en cuenta para que éstos sean aprovechados de la mejor manera.

3.2.8. Integridad

“mantenimiento de las características de completitud y corrección de los datos”. (Administración Electrónica, 2006)

3.2.9. Autenticidad

De nada sirve tener la información si no se puede garantizar que la misma es confiable. Los expertos en seguridad dan un énfasis sobre este atributo ya que todo lo que se realice es tiempo perdido si no se puede verificar que la información que se encuentra es certera y si no se puede garantizar el origen, responsable y destino de la misma. Magerit nos indica una definición muy precisa al respecto: “que no haya duda de quién se hace responsable de una información o prestación de un servicio, tanto a fin de confiar en él como de poder perseguir posteriormente los incumplimientos o errores.” (Administración Electrónica, 2006)

3.2.10. SISAGEL

Siglas del Sistema de Administración de la Seguridad de la Información para el Gobierno en Línea el cual permite dar cumplimiento a los principios definidos en la Ley 1341 de 2009 al igual que la estrategia de Gobierno en Línea; éste surge para dar dirección y controlar todos los actores involucrados en el proceso de la seguridad de la información generando confianza y transparencia entre cada una de las partes.

3.3. Marco legal

La normatividad que soporta la implementación del proyecto de principio, política y lineamientos de consulta de información de la “Maestra de Usuarios”

está basada en el Artículo 15 de la Constitución Política de Colombia que indica entre sus derechos fundamentales: “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.” Y complementada en la Ley Estatutaria 1266 de 2008 la cual “disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”.

Igualmente, la Ley Estatutaria 1581 de 2012 en su artículo 17, ítem d) ordena: “Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento” y en su ítem e) “Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible” por lo cual la entidad, al contener información que ha sido clasificada como sensible (Al almacenar información que pueden afectar la intimidad del titular o su uso indebido puede generar su discriminación) se encuentra en la obligación de aplicar esta Ley apoyándose en el Decreto Reglamentario parcial 1377 de 2013 en su artículo 18 donde se indican los Procedimientos para el adecuado tratamiento de los datos personales.

4. METODOLOGÍA

Teniendo en cuenta el ámbito de la organización sobre la cual se va a desarrollar el proyecto de principio, política y lineamientos de consultas de información de la “maestra de usuarios”, se utilizarán los “Lineamientos para la implementación del modelo de seguridad 2.0” los cuales fueron publicados por el Ministerio de Tecnologías de la Información y las Comunicaciones en el año 2011 con el fin que cada una de las entidades del sector gubernamental cumpla con los mismos para facilitar la eficiencia y colaboración entre las entidades del Estado, contribuir al incremento de la transparencia en la gestión pública, promover la participación ciudadana a través de los recursos de electrónicos y fortalecer las condiciones para el incremento de la competitividad y el mejoramiento de la calidad de vida.

Estos lineamientos se complementan con estándares internacionales ya que la arquitectura del modelo se basa en el ciclo PHVA; de igual forma, y como parte de la estrategia del Gobierno en Línea también se encuentra alineada con los niveles de madurez del manual de GEL 3.0 y es completamente coherente con los lineamientos estándares de ISO/IEC 27001:2005 lo cual permite a cualquier organización que se encuentre certificada con esta norma, implementar estos lineamientos sin mayores dificultades.

Vale la pena aclarar que aunque una entidad gubernamental del orden nacional cumpla con todos los requisitos estipulados en la estrategia de Gobierno en Línea – GEL, ello no implica que la entidad cumpla con los estándares internacionales de seguridad de la información (ISO/IEC 27001) o con alguna otra norma que se relacione con la misma. Para que la entidad adquiera el certificado, ésta debe continuar alineando sus esfuerzos de tal manera que logre la certificación sin afectar todo el trabajo realizado para el GEL.

De acuerdo a los “Lineamientos para la implementación del modelo de seguridad 2.0” y las características del desarrollo del proyecto, empezaremos identificando los responsables involucrados en el proyecto al igual que sus roles y responsabilidades.

4.1. Metodología de identificación de Responsables

Una de las fases más importantes en el proyecto es la Identificación acertada de los responsables en cada una de las tareas que se tienen a cabo. Si el gerente encargado del proyecto tiene todos los recursos disponibles pero se equivoca en la asignación de responsables para cada una de las tareas, el

proyecto se irá a pique y su fracaso será inevitable; es por ello que se debe tomar el tiempo necesario para definir las tareas que permitan la feliz culminación del proyecto y, sobre todo, asignar a personas idóneas y responsables que las puedan llevar a cabo de manera eficiente y proactiva.

La primera tarea que se debe realizar es establecer la organización del gobierno. La organización del gobierno permite definir la estructura organizacional que la compone y cuál es su comportamiento jerárquico para las discusiones y decisiones que se llevarán a cabo en su interior, esto de acuerdo a los roles y responsabilidades adquiridas por cada uno de los integrantes.

Con esto enfocamos a los actores que son realmente importantes en la posición que deben tomar para que el gobierno administre y establezca definiciones sobre temas cruciales o conflictos divididos con el único objetivo que la herramienta sea explotada a su máxima potencia de manera objetiva.

Posterior a ello, se deben definir otros responsables que de manera individual responsan por cada una de las actividades que se deben desarrollar durante la ejecución del proyecto. Dichos responsables deben tener una injerencia directa en el proyecto y deben pertenecer a los mandos medios o altos de la organización para facilitar en avance y toma de decisiones en momentos cruciales.

4.2. Encuestas

Las encuestas son una herramienta importante para la recolección de cualquier tipo de información; las encuestas permiten detectar distintos puntos de vista sobre las áreas o personas involucradas y de allí, establecer qué necesidades deberían ser atendidas de manera inmediata, qué aspectos se pueden resaltar sobre las preguntas realizadas y qué aspectos deben ser analizados a profundidad para que sean mejorados.

El objetivo de la encuesta es que la misma sirva de soporte para la identificación de las necesidades, dificultades y riesgos percibidos por cada uno de los funcionarios en cada uno de los niveles de la entidad (tanto al interior como al exterior) y sobre ello se empiece a plasmar el documento de brecha que sirve como antesala para definir la estrategia para la reducción de la brecha en el Gobierno de la Información en el sistema.

En ésta encuesta realizaremos una búsqueda sistemática de información, en la que preguntaremos la información que deseamos obtener a partir de datos individuales, teniendo como premisa que a todos los entrevistados se les desarrollarán las mismas preguntas, en el mismo orden, y en una situación similar; de modo que las diferencias serán atribuibles a las variación de conceptos existente entre las personas entrevistadas.

La finalidad de la encuesta aplicada es de tipo Descriptiva; está acompañada de preguntas estructuradas y nos permitirá definir la realidad y la caracterización del proyecto, de igual forma nos dará ideas sobre la identificación de las necesidades para que se implemente el gobierno de datos de manera satisfactoria sobre el sistema.

4.3. Documento de definición de brechas

Para el proyecto, la definición de brecha es un documento importante que permite a la entidad establecer un punto de ubicación o de partida inicial a partir de la definición de cómo debe estar funcionando el gobierno de datos de información de la aplicación; éste documento es base de la estrategia que debe realizar la entidad para reducir la brecha TO-BE/AS-IS.

Teniendo en cuenta la definición realizada por el Ministerio de Tecnologías de Información y Comunicaciones en el marco del Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0., se definen una serie de preguntas claves que permitirán a la entidad conocer su estado de madurez en:

- **Estructura organizacional:** Permite determinar la relevancia y el impacto de la seguridad de la información en cada una de las áreas que conforman la entidad.
- **Nivel de gestión de la seguridad de la información:** Permite establecer de manera aproximada cuál es el nivel de maduración de la seguridad de la información en la cual se encuentra la organización.
- **Políticas, controles y métricas indicando el estado:** De acuerdo a la norma ISO 27000 y sus dominios, sirve como herramienta de control y seguimiento para la evolución del proyecto indicando qué existe y qué debería existir.
- **Análisis de las variables que existen en el sistema de la maestra de usuarios:** Realiza un análisis básico sobre las variables disponibles en el sistema y el comportamiento de la información registrada disponible en la misma.

Éste cuestionario propuesto será respondido más adelante en el ítem de Resultados y Discusión y se establecerá el punto de madurez en el cual la entidad se encuentra en la actualidad; parte de este trabajo se llevará a cabo con los Jefes de las oficinas responsables del sistema al igual que con los líderes en el manejo y funcionamiento del mismo.

4.4. Plan de trabajo para reducción de brecha

Para establecer el plan de trabajo para la reducción de brecha, es importante tener claramente definidos dos elementos en el proceso; estos son el cómo estamos y a dónde queremos llegar.

A partir de todo el trabajo realizado en la definición de brecha podemos establecer cuál será el punto en el cual se encuentra la organización; se tomará como documento base los resultados arrojados en el Nivel de Gestión de Seguridad de la Información sin olvidar los demás resultados realizados en ese ítem.

Para definir a dónde debemos llegar, basta con leer el título del proyecto (PROYECTO DE PRINCIPIO, POLÍTICA Y LINEAMIENTOS DE CONSULTAS DE INFORMACIÓN DE LA “MAESTRA DE USUARIOS”) y establecer cuál es el Nivel de Gestión de Seguridad de la Información que se debe cumplir para que tanto el título como los objetivos se lleven a cabo; analizando esto, podemos establecer que basta con cumplir el Nivel Inicial de Plan de Seguridad sobre el sistema. Algunas tareas ya se han realizado, sin embargo, tareas fundamentales de definición no se han llevado a cabo por lo que se han presentado todos los problemas expuestos en ítems anteriores y manifestados por los encuestados.

Por último, para la definición del plan de trabajo, si bien se ha tomado la definición de brecha establecida por el Ministerio de Tecnologías de la Información y las Comunicaciones en el Modelo de Seguridad de la Información, éste documento no posee ningún anexo o documento que sirva como guía para establecer el plan de trabajo de reducción de brecha; lo único que sugiere es que se debe llevar a cabo una hoja de ruta a seguir para reducir la brecha teniendo en cuenta la información recolectada en el Anexo 4.

Por este motivo, para el establecimiento de la reducción de brecha colocaremos un listado de actividades que se deben desarrollar acompañadas de las fechas en las cuales éstos deben encontrarse listos para cumplir con el Nivel Inicial del Plan de Seguridad propuesto por el Ministerio de Tecnologías de la Información y Comunicación en su Anexo 4 del Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0.

4.5. Definición del Alcance del sistema

Para la definición del alcance del sistema, el cual hace parte integral de la política que se va a desarrollar, se tomará como base la información recolectada en el punto 5.3. Resultados de Definición de Brecha y 5.4. Plan de trabajo para reducción de Brecha. Estos dos ítems permitirán establecer a quienes les cobija la definición y las condiciones de las mismas. La definición del alcance debe ir alineada a la Estrategia de Gobierno en Línea 2.0 de acuerdo al Modelo de Seguridad de la Información y, por ente, al estándar internacional ISO/IEC 27001.

4.6. Definición de las políticas del sistema

La información es, en la actualidad, el elemento primordial de cualquier organización, de tal manera se hace importante la implementación de medidas que propendan por salvaguardar la integridad, la confidencialidad y la disponibilidad de la información que maneja la entidad, con el fin de asegurar la operación de la misma.

Para la implementación de los mecanismos de seguridad de la información, se ha definido un conjunto de políticas que se deben cumplir, sin embargo, estas políticas son generales y buscan dar directrices para lograr el aseguramiento de la información en todas sus formas.

La definición de políticas está basada en la norma técnica internacional ISO/IEC 27001, en la Estrategia de Gobierno en Línea 2.0 y buscan alinearse con el Modelo de Seguridad de la Información planteado.

Una buena política es concisa, fácil de leer y comprender, flexible y fácil de hacer cumplir para todos aquellos dentro del alcance sin excepción. Son cortas, y enmarca los principios que guían las actividades dentro de la entidad.

4.7. Gestión de Riesgos

En la era digital, el uso de las tecnologías de información automatizadas se requiere para aproximar a las empresas a ejecutar su misión por lo que la gestión correcta de los riesgos de tales tecnologías juega un papel fundamental en la protección de los activos de información.

El proceso de gestión del riesgo, es un componente importante cuando se desea un programa exitoso de seguridad de TI ya que su principal meta es proteger la entidad y su capacidad de alcanzar su misión. Por tanto, el proceso de gestión del riesgo no debiera ser tratado como una función únicamente técnica llevada a cabo por los expertos o “magos” de TI; este proceso debe ser implementado desde las áreas de negocio a nivel funcional y estratégico, hasta las áreas operativas y de infraestructura IT ya que es una función esencial de cada organización.

La gestión del riesgo comprende tres (3) procesos: análisis de riesgos, mitigación de riesgos, evaluación y valoración continúa. El proceso de análisis de riesgos incluye la identificación de vulnerabilidades y riesgos, la evaluación de riesgos, sus impactos, y las recomendaciones para la reducción de los riesgos. La mitigación de los riesgos se refiere a la priorización, implementación y mantenimiento de las apropiadas medidas de reducción de riesgos. La evaluación y valoración continúa son las prácticas para el

mantenimiento de un proceso exitoso de gestión del riesgo. Es responsabilidad del cargo autorizado, determinar cuándo el riesgo residual tiene un nivel aceptable o cuándo son requeridos controles adicionales que debieran implementarse para reducir o eliminar el riesgo residual antes que se autorice la puesta en producción de los sistemas de TI.

La gestión del riesgo es el proceso que permite a los administradores de TI establecer un balance entre los costos operativos y económicos de las medidas de protección y su efectividad versus el logro de los objetivos de la entidad y la protección real brindada a los sistemas y datos que soportan tales objetivos.

La documentación y recolección de información que se utilizará para llevar a cabo la Gestión del Riesgo del proyecto será la realizada extrayendo las ventajas o fortalezas que posee la ISO/IEC 27001 y Magerit. De igual manera, se extrajo parte de documentación y formatos del Sistema de información de Documentos de la Universidad Tecnológica y Pedagógica de Colombia.

Como se mencionó anteriormente, de toda la información recolectada se tomaron las mejores prácticas y elementos necesarios que cumplieran con una adecuada identificación de los activos de información, un análisis eficiente y práctico de los riesgos identificados sobre los activos y contenedores de la entidad, un análisis que visibilizara los controles necesarios para reducir los riesgos y un tratamiento eficaz para la empezar a reducir la brecha existente; estos formatos definitivos fueron utilizados anteriormente en el curso de Análisis de Riesgos donde se trabajó una temática relacionada al proyecto actual.

4.8. Definición de Indicadores

Los indicadores son importantes para cualquier tipo de negocio, ya que a través de ellos se permite establecer puntos, límites y criterios que determinar el estado particular y general de un área a evaluar.

Para la definición de los indicadores que permitan valorar el desempeño del proyecto de principio, política y lineamientos de consultas de información de la “maestra de usuarios” es fundamental conocer el negocio, su funcionamiento, cómo está compuesto, que factores interno y externos lo influencian entre otras características; es por ello que para su definición es necesario empaparse de la entidad.

Otro aspecto para tener en cuenta, es que la definición de los indicadores debe realizarse de manera clara y comprensible para los evaluadores garantizando que los datos sean un insumo sustentable y evidente de lo que se está desarrollando en el proyecto.

Existen una gran cantidad de maneras de agrupar y organizar los indicadores de la entidad, pero todos ellos deben ir enmarcados en el principio de cualificación de eficiencia o eficacia del sistema y los más relevantes harán parte del cuadro de mando de la aplicación.

Todos los indicadores presentados estarán compuestos por las siguientes características:

- Código
- Nombre del indicador
- Eje de valoración
- Ámbito
- Descripción
- Unidad de Medida
- Tipo de indicador
- Periodicidad
- Fórmula de cálculo
- Observaciones
- Unidad de medida

5. RESULTADOS Y DISCUSIÓN

Una vez plasmada toda la información concerniente a la metodología con la cual se desarrollará el "Proyecto de principio, política y lineamientos de consultas de información de la maestra de usuarios", es necesario evidenciar los resultados de proyecto teniendo en cuenta las evidencias recolectadas y a partir de ello, realizar el análisis que pueda permitir brindar resultados a los usuarios de la herramienta al punto que se logre atacar sus necesidades.

De acuerdo a cada uno de los puntos desarrollados en la metodología, empezaremos colocando los resultados:

5.1. Resultados de la identificación de responsables

Como ya se comentó en la metodología, es necesario que exista un ente rector principal conformado por diferentes áreas que garanticen la objetividad en la definición de los lineamientos, la política y el principio; es por ello que el gobierno que lo administre debe ser establecido de la siguiente manera:

Ilustración 1 Fuente: Investigación Propia

De acuerdo al anterior gráfico, se propone implementar la siguiente estructura de gobierno indicando la ubicación del rol y su responsabilidad:

5.1.1. Comité de gobierno de Información

Es un Comité Estratégico multifuncional que está integrado por un grupo de personas pertenecientes a las áreas involucradas en el proceso de gestión de información; este comité revisa y aprueba los procesos, políticas y procedimientos, gestionando las prioridades y evaluando su adecuada consecución para la buena utilización de la herramienta. Éste comité debe reunirse periódicamente para tratar asuntos relacionados con el gobierno de la información.

Debido a la estructura plasmada por el Decreto 4155 de 2011, el comité debe estar conformado por los siguientes integrantes cuyas funciones asignadas están relacionadas con las responsabilidades del gobierno de información:

Integrante	Justificación
Director del Departamento para la Prosperidad Social o un representante delegado por el mismo.	Como Director de la entidad, debe estar al tanto de todas las acciones estratégicas y misionales. Es la persona que firma los memorandos y decretos expedidos en la entidad de orden nacional; son de cumplimiento obligatorio.
Jefe de la Oficina Asesora de Planeación, Monitoreo y Evaluación o un representante delegado por el mismo.	Como Jefe de ésta oficina, debe indicar las pautas y lineamientos de la información de acuerdo a las metas de gobierno y la inversión ejecutada sobre la población sujeto de la atención.
Jefe de la Oficina de Tecnología e Información o un representante delegado por el mismo.	Como Jefe de ésta oficina, es el responsable de todas las metas y lineamientos relacionados con la tecnología; desde la compra de infraestructura hasta el comportamiento de la información para cumplir con las funciones de la entidad.
Jefe de cada una de las Direcciones Misionales que componen la Entidad o un representante delegado por el mismo.	Las direcciones misionales de la entidad son las responsables de atender directamente a la población; por esto, es necesario que cada una tenga un representante en el comité ya que conocen el comportamiento de la información y el flujo que ella posee.
Secretaria General o un representante delegado por el mismo.	La Secretaria General responde por el buen funcionamiento interno de la entidad; específicamente, es la responsable de mantener disponible los recursos y servicios tecnológicos de la entidad utilizando como canal de comunicaciones la mesa de ayuda.
Administrador Técnico líder del sistema de	Como administrador(es) de la(s) herramienta(s) de almacenamiento de la información, recae la

Inteligencia de Negocio o Administrador de Bases de Datos.	responsabilidad de apoyar técnicamente al comité en cada uno de los asuntos que se deban tratar.
Oficial de Seguridad de la Información	Es la persona encargada de velar por que los principios de Seguridad de la Información se cumplan a cabalidad. Ésta persona debe tener un análisis muy objetivo de los riesgos y conocer el funcionamiento del negocio.

Tabla 1 Fuente: Investigación Propia

Éste comité tiene la responsabilidad de realizar las siguientes tareas:

Planear, delegar y controlar los procesos de gestión de los datos en los cuales se involucra la información de la “Maestra de Usuarios”.

Establecer y publicar las políticas de Confidencialidad, Disponibilidad, Integridad, Usabilidad, Trazabilidad y Seguridad de la información contenida en la “Maestra de Usuarios”.

Discutir y dirimir diferencias sobre las inquietudes que se presenten en cuanto a la información.

5.1.2. Jefe de la Oficina de Tecnología e Información

Es la persona nombrada por el Director de la entidad que se encarga de Asesorar a la dirección en la ejecución y seguimiento de todas las actividades concernientes a la tecnología de la información. Su labor es muy importante en el proyecto ya que es uno de los influenciadores que tiene comunicación directa con la dirección y en función a sus decisiones, la entidad determina la hoja de ruta que se establece para lograr los objetivos del Departamento y del Sector.

Bajo su responsabilidad, y por Resolución del 1 de Julio de 2014, le están asignadas funciones entre las cuales vale la pena resaltar las siguientes:

1. “Diseñar y proponer la política de uso y aplicación de tecnologías, estrategias y herramientas para el mejoramiento continuo de los procesos del Departamento Administrativo y del Sector Administrativo de la Inclusión Social y Reconciliación.
2. Promover la aplicación de buenas prácticas y principios para el manejo y la custodia de la información institucional, siguiendo los lineamientos y directrices del gobierno actual.
4. Vigilar y coordinar que en los procesos tecnológicos del Departamento y del Sector Administrativo de Inclusión Social y Reconciliación se tengan en cuenta los estándares y lineamientos dictados por el Ministerio de las Tecnologías de la Información y las Comunicaciones, que permitan la aplicación de las políticas que en materia de información expida el

Departamento de Planeación Nacional y el Departamento Administrativo Nacional de Estadística – DANE.

9. Proponer al Director General planea, estrategias y proyectos que en materia de Tecnologías de la Información se deban adoptar. (Departamento Administrativo para la Properidad Social - DPS, 2014)

5.1.3. Administrador de Base de Datos

Es la persona asignada por la entidad de administrar y garantizar el funcionamiento óptimo de los diferentes motores de bases de datos instalados; dicha administración debe ser acorde a los diferentes lineamientos establecidos por las áreas encargadas y debe cumplir con los principios de seguridad de la información. En la actualidad se cuenta con los motores de bases de datos SQL Server y Oracle.

Bajo su responsabilidad, y por Resolución del 1 de Julio de 2014, le están asignadas funciones entre las cuales vale la pena resaltar las siguientes:

1. “Administrar las bases de datos y servidores de aplicación de la entidad con el propósito de garantizar la integridad, disponibilidad, confiabilidad y confidencialidad de las mismas, de acuerdo con las mejores prácticas en la materia y el plan estratégico de tecnologías de información.
2. Efectuar y administrar las copias de respaldo de las bases de los sistemas de información de la entidad, a fin de garantizar la disponibilidad de la información, según el plan de contingencia.
3. Diseñar, evaluar y realizar seguimiento a los proyectos que estén relacionados con la plataforma de bases de datos, con el objeto de dar recomendaciones sobre su viabilidad, según los lineamientos de la entidad.
4. Diseñar y realizar el modelamiento de bases de datos estructurales y no estructurales que se requieran con el propósito de facilitar el correcto funcionamiento de las aplicaciones de la entidad, conforme con los lineamientos establecidos.” (Departamento Administrativo para la Properidad Social - DPS, 2014)

De igual manera, aparte de las funciones asignadas por resolución, también le corresponde:

1. Administrar todas las consideraciones arquitectónicas y recomendar las alternativas que sean necesarias para su mejora.
2. Proporcionar asistencia y gestionar todas las solicitudes de aplicación de las normas de acuerdo a los lineamientos y directrices dadas por la Entidad.

5.1.4. Administrador Técnico Líder del sistema de Inteligencia de Negocios

Es la persona asignada por la entidad de administrar y garantizar el funcionamiento óptimo de los diferentes cubos y modelos de inteligencia de

negocios implementados para responder a las diferentes necesidades plasmadas en la entidad; dicha administración debe ser acorde a los diferentes lineamientos establecidos por las áreas encargadas y debe cumplir con los principios de seguridad de la información.

Bajo su responsabilidad, y por Resolución del 1 de Julio de 2014, le están asignadas funciones entre las cuales vale la pena resaltar las siguientes:

1. “Diseñar e implementar proyectos de desarrollo de Software de BI, de acuerdo con los estándares internacionales.
2. Orientar en el desarrollo de los Sistemas de Información de las áreas misionales, administrativas y a las Entidades del Sector, en cuanto a los criterios de consolidación de información, de acuerdo con los parámetros establecidos por la entidad.
3. Orientar en el desarrollo de los Sistemas de Información de BI, de acuerdo con los lineamientos establecidos por la Entidad.” (Departamento Administrativo para la Properidad Social - DPS, 2014)

De igual manera, aparte de las funciones asignadas por resolución, también le corresponde:

1. Optimizar los componentes de los diferentes Sistemas de Inteligencia de Negocio al nivel de modelos relacionales y multidimensionales.
2. Gestionar las necesidades de nuevos requerimientos de negocio.
3. Desarrollar y mantener las normas de todas las bodegas de datos al igual que las ETL que se vean involucradas.
4. Supervisar la ejecución y mantenimiento (Si fuera el caso) sobre el proceso de integración a través de modelos de ETL y de bases de datos, garantizando un rendimiento óptimo en la ejecución de los procesos.
5. Garantizar el seguimiento histórico de los cambios que se originen sobre los datos.

5.1.5. Administrador Funcional de la Maestra de Beneficiarios

Es la persona asignada por la entidad o el responsable del sistema; de administrar y supervisar el buen funcionamiento de los componentes aplicativos de la Maestra de Beneficiarios (Entre los cuales se encuentra la administración de usuarios, permisos, accesos, validación y consistencia de la información, entre otros). Igualmente, deberá velar por la calidad de la información plasmada en cada uno de los informes que el sistema posee garantizando que dichos datos correspondan a la realidad ejecutada por la entidad de acuerdo a los filtros seleccionados.

Bajo su responsabilidad se encuentra la realización de las siguientes actividades:

1. Evaluar el funcionamiento eficiente de la Maestra de Beneficiarios y brindar apoyo a los usuarios en el proceso de funcionamiento.
2. Velar por el cumplimiento de todas las especificaciones técnicas y funcionales establecidas en los manuales de usuario y técnicos.
3. Garantizar el cumplimiento de las políticas de calidad de datos que son cargados por cada uno de los enlaces de información.
4. Proporcionar a cada uno de los suministradores de información (Enlaces) una definición clara y precisa de la estructura de carga de datos.
5. Coordinar con cada uno de los suministradores de información (Enlaces) actividades que garanticen el correcto cumplimiento de las políticas de reporte de información para la bodega de datos.
6. Garantizar la administración adecuada del sistema de información de tal manera que, en coordinación con cada uno de los actores involucrados, se aproveche al máximo los componentes y ventajas disponibles.
7. Revisar y gestionar la presentación de los informes de auditoría que posee la aplicación.

5.1.6. Oficial de Seguridad de la Información

Es la persona asignada por la entidad de planear, coordinar y administrar los procesos de seguridad de la información en la entidad diseñando de manera planeada y coordinada la administración de cada uno de los procesos de seguridad donde se ve involucrada.

Bajo su responsabilidad le están asignadas las siguientes responsabilidades:

1. Definir la política de seguridad de la información de la entidad.
2. Definir los procedimientos para aplicar la política de seguridad de la información.
3. Seleccionar los mecanismos y herramientas adecuados que permitan las políticas dentro de la entidad.
4. Asegurar el cumplimiento de las políticas de seguridad de la información.
5. Crear un grupo de respuesta de incidentes de seguridad que atienda los problemas relacionados al área de seguridad informática en la entidad.
6. Promover la aplicación de auditorías enfocadas a la seguridad, tales como capacitaciones, charlas, correos, instructivos, entre otros.
7. Crear y vigilar lineamientos necesarios que apoyen a tener los servicios de seguridad de la información en la entidad.

5.1.7. Suministradores de información - Enlaces de información

Son las personas asignadas por cada uno de las entidades, direcciones y programas existentes en el sector para generar y cargar los archivos en la bodega de datos del sistema de acuerdo a las especificaciones indicadas en el manual de usuario y manual técnico.

Bajo su responsabilidad le están asignadas las siguientes responsabilidades:

1. Consolidar y depurar los datos de la entidad, dirección o programa al cual pertenece.
2. Cumplir con el proceso de cargue de datos en las fechas y dentro del rango de tiempo que determinados para esta actividad.
3. Garantizar el cargue de datos, de acuerdo a los parámetros de cumplimiento dados por la entidad en cuanto a responsabilidad, confiabilidad, oportunidad, completitud, consistencia, obligatoriedad, realidad y calidad de la información de cada programa.
4. Mantener actualizado la información de los metadatos identificados que se encuentren operativos en el negocio.
5. Garantizar que la información que será procesada por el Sistema de Inteligencia de Negocios, cumpla con los requerimientos técnicos dados, de acuerdo a la estructura del archivo de cargue suministrado para tal función o en su defecto cumpla con los criterios de transmisión de datos establecido sobre el servicio de intercambio de información.

5.1.8. Estructura jerárquica del gobierno de información

La estructura jerárquica de una organización es fundamental para determinar cuál es el conducto regular que se debe seguir en todo lo concerniente al gobierno de información; a continuación el organigrama debe estar compuesto de la siguiente manera:

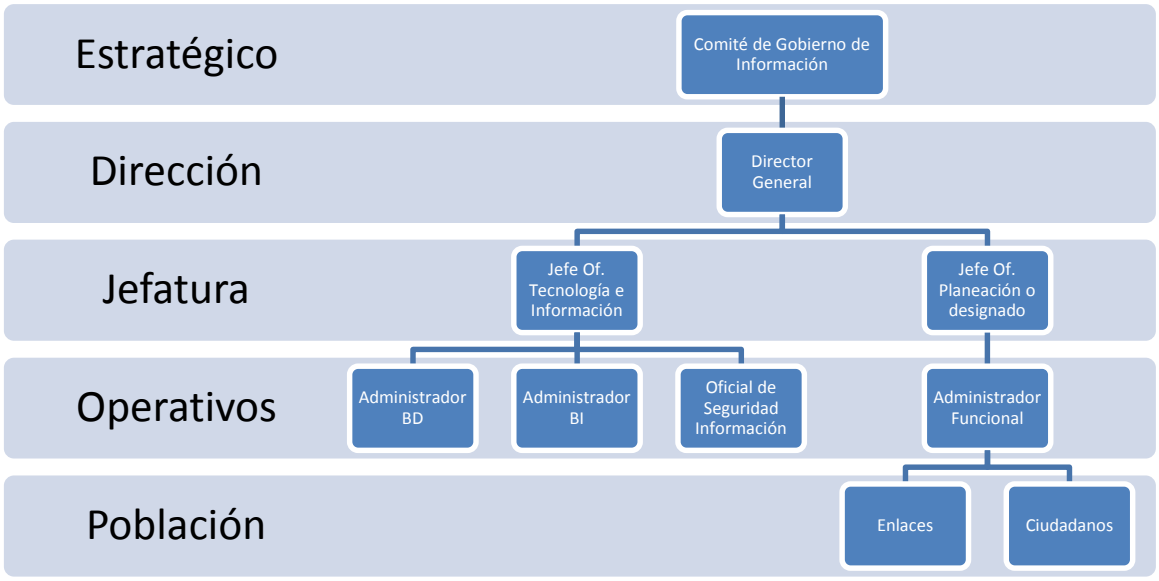


Ilustración 2 Fuente: Investigación Propia

5.2. Resultados de las encuestas

Teniendo en cuenta que la encuesta es igual para todos los usuarios y que la misma se debe desarrollar bajo las mismas condiciones, colocamos las características de la encuesta desarrollada:

5.2.1. Ficha Técnica

Nombre del proyecto: Proyecto de principio, política y lineamientos de consultas de información de la "maestra de usuarios".

Objetivo de la Encuesta: Identificar necesidades en el gobierno de datos del sistema.

Encuestadores: William Atehortua y Rafael Francisco Reyes Estudiantes de Especialización en Seguridad de la Información de la Institución Universitaria Politécnico Grancolombiano.

Fecha de realización de campo: 19 al 21 de Octubre de 2015.

Persona natural o jurídica que la realizó: William Atehortua y Rafael Francisco Reyes Estudiantes de Especialización en Seguridad de la Información de la Institución Universitaria Politécnico Grancolombiano.

Persona natural o jurídica que la encomendó: William Atehortua y Rafael Francisco Reyes Estudiantes de Especialización en Seguridad de la Información de la Institución Universitaria Politécnico Grancolombiano.

Fuente de financiación: Propia de los estudiantes.

Universo: 20 Funcionarios en diferentes instalaciones.

Grupo Objetivo: Hombres y Mujeres mayores de 18 años de edad que trabajan en la entidad y son consumidores potenciales del sistema.

Diseño Muestral: Tipo probabilístico

Marco Muestral: Base de datos de los funcionarios de la entidad.

Tamaño de la muestra: 80% de los funcionarios.

Técnica de recolección: Encuesta enviada por correo.

Cobertura Geográfica: Bogotá, Oficinas de nivel Central y Direcciones Regionales.

Cantidad de Encuestados: 16 Funcionarios

Número de Preguntas Formuladas: 15 Preguntas de respuesta cerrada.

5.2.2. Cuestionario

1. Por favor seleccione su cargo

- ( ) Jefe de oficina
- ( ) Director misional
- ( ) Director regional
- ( ) Administrador del sistema
- ( ) Analista de información
- ( ) Consultor de información

2. ¿Qué nivel de disponibilidad es necesario para los procesos que usted realiza?

- ( ) A. Alta
- ( ) B. Media
- ( ) C. Regular
- ( ) D. Ninguna

3. Por favor indique su área de responsabilidad dentro de la infraestructura.

- ( ) A. Técnico - programador/analista
- ( ) B. Negocio – analista/consultor funcional
- ( ) C. Gestión de línea de negocio - finanzas, cadena de suministro, operaciones, recursos humanos
- ( ) D. Gestión del departamento de infraestructura y soporte tecnológico

4. Su área conoce y cuenta con los acuerdos de servicios (SLA) del sistema.

- ( ) A. Si
- ( ) B. No
- ( ) C. No sabe

5. Identifica los componentes más críticos del sistema.

- ( ) A. Si
- ( ) B. No
- ( ) C. No sabe

6. Conoce el procedimiento de Administración de incidencias del sistema.

- ( ) A. Si
- ( ) B. No

- ( ) C. No sabe

7. Conoce el procedimiento de respaldo y recuperación existente para la información del sistema.

- ( ) A. Si
- ( ) B. No
- ( ) C. No sabe

8. Conoce el procedimiento de cambios de información existente sobre el sistema.

- ( ) A. Si
- ( ) B. No
- ( ) C. No sabe

9. La entidad ha definido una organización interna en términos de personas y responsabilidades con el fin de cumplir las políticas de seguridad de la información y documenta estas actividades.

- ( ) A. Si
- ( ) B. No
- ( ) C. No sabe

10. La entidad cumple con los requisitos legales, reglamentarios y contractuales con respecto al manejo de la información.

- ( ) A. Si
- ( ) B. No
- ( ) C. No sabe

11. La entidad ha definido lineamientos de trabajo a través del comité o responsable de seguridad para que sus funcionarios cumplan las políticas de seguridad y evalúa periódicamente su pertinencia.

- ( ) A. Si
- ( ) B. No
- ( ) C. No sabe

12. La entidad ha definido lineamientos en cuanto a la protección de las instalaciones físicas, equipos de cómputo y su entorno para evitar accesos no autorizados y minimizar riesgos de la información de la entidad.

- ( ) A. Si
- ( ) B. No
- ( ) C. No sabe

13. La entidad verifica de manera interna y/o a través de terceros, periódicamente sus procesos de seguridad de la información y sistemas para asegurar el cumplimiento del modelo.

- ( ) A. Si
- ( ) B. No
- ( ) C. No sabe

14. La entidad ha sido víctima de ataques informáticos el último año.

- ( ) A. Si
- ( ) B. No
- ( ) C. No sabe

15. La información consultada en el sistema arroja resultados consistentes.

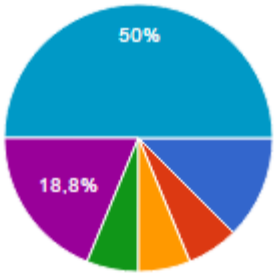
- ( ) Siempre
- ( ) Casi siempre
- ( ) A veces
- ( ) Casi nunca

La ficha técnica con la cual se llevó a cabo la encuesta está desarrollada de la siguiente manera:

5.2.3. Resultado de respuestas de la encuesta

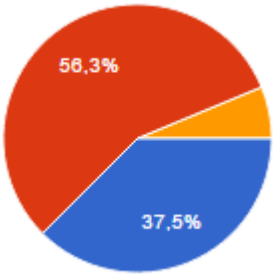
1. Por favor seleccione su cargo

Jefe de oficina	**2**	12.5%
Director misional	**1**	6.3%
Director regional	**1**	6.3%
Administrador del sistema	**1**	6.3%
Analista de información	**3**	18.8%
Consultor de información	**8**	50%



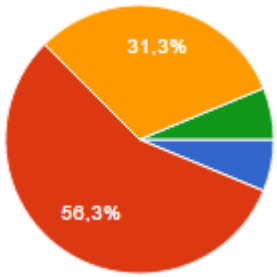
2. ¿Qué nivel de disponibilidad es necesario para los procesos que usted realiza?

A. Alta	6	37.5%
B. Media	9	56.3%
C. Regular	1	6.3%
D. Ninguna	0	0%



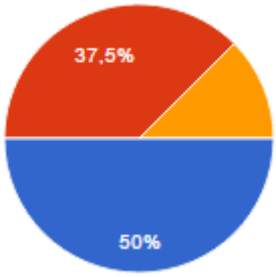
3. Por favor indique su área de responsabilidad dentro de la infraestructura.

A. Técnico - programador/analista	**1**	6.3%
B. Negocio - analista funcional	**9**	56.3%
C. Gestión de línea de negocio - finanzas, cadena de suministro, operaciones, recursos humanos	**5**	31.3%
D. Gestión del departamento de informática	**1**	6.3%



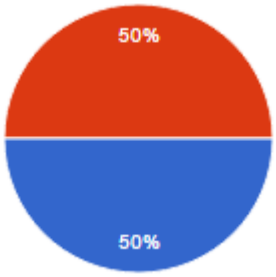
4. Su área conoce y cuenta con los acuerdos de servicios (SLA) del sistema.

A. Si	**8**	50%
B. No	**6**	37.5%
C. No sabe	**2**	12.5%



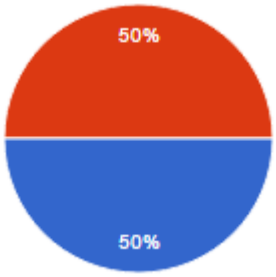
5. Identifica los componentes más críticos del sistema.

A. Si	**8**	50%
B. No	**8**	50%
C. No sabe	**0**	0%



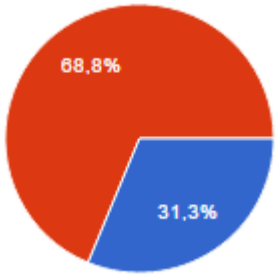
6. Conoce el procedimiento de Administración de incidencias del sistema.

A. Si	**8**	50%
B. No	**8**	50%
C. No sabe	**0**	0%



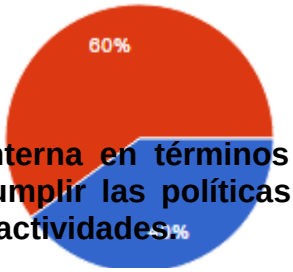
7. Conoce el procedimiento de respaldo y recuperación existente para la información del sistema.

A. Si	**5**	31.3%
B. No	**11**	68.8%
C. No sabe	**0**	0%



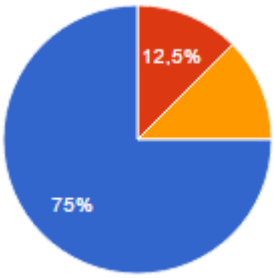
8. Conoce el procedimiento de cambios de información existente sobre el sistema.

A. Si	**6**	40%
B. No	**9**	60%
C. No sabe	**0**	0%



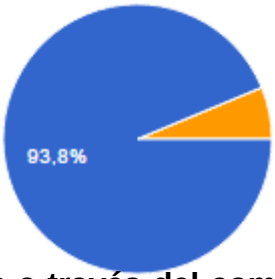
9. La entidad ha definido una organización interna en términos de personas y responsabilidades con el fin de cumplir las políticas de seguridad de la información y documenta estas actividades.

A. Si	**12**	75%
B. No	**2**	12.5%
C. No sabe	**2**	12.5%



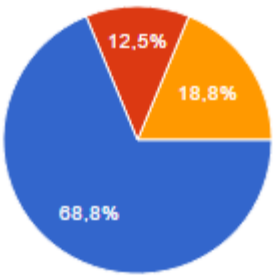
10. La entidad cumple con los requisitos legales, reglamentarios y contractuales con respecto al manejo de la información.

A. Si	**15**	93.8%
B. No	**0**	0%
C. No sabe	**1**	6.3%



11. La entidad ha definido lineamientos de trabajo a través del comité o responsable de seguridad para que sus funcionarios cumplan las políticas de seguridad y evalúa periódicamente su pertinencia.

A. Si	**11**	68.8%
B. No	**2**	12.5%
C. No sabe	**3**	18.8%

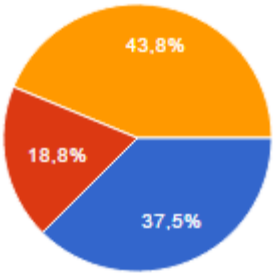


12. La entidad ha definido lineamientos en cuanto a la protección de las instalaciones físicas, equipos de cómputo y su entorno para evitar accesos no autorizados y minimizar riesgos de la información de la entidad.

A. Si	**11**	68.8%
B. No	**3**	18.8%
C. No sabe	**2**	12.5%

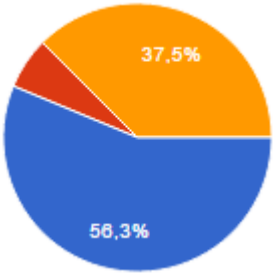
13. La entidad verifica de manera interna y/o a través de terceros, periódicamente sus procesos de seguridad de la información y sistemas para asegurar el cumplimiento del modelo.

A. Si	**6**	37.5%
B. No	**3**	18.8%
C. No sabe	**7**	43.8%



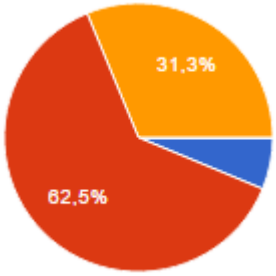
14. La entidad ha sido víctima de ataques informáticos el último año.

A. Si	**9**	56.3%
B. No	**1**	6.3%
C. No sabe	**6**	37.5%



15. La información consultada en el sistema arroja resultados consistentes.

Siempre	**1**	6.3%



Casi siempre	**10**	62.5%
A veces	**5**	31.3%
Casi nunca	**0**	0%

5.2.4. Análisis de resultados – Conclusiones de la encuesta

De acuerdo a los resultados presentados por los encuestados, podemos determinar que la mayoría de los usuarios son Consultores de la Información; es decir, la mayoría de los encuestados pertenecen al menor nivel de jerarquía de poder en el sistema pero a su vez, son los usuarios que más pueden llegar a utilizarla y tener un mejor concepto del funcionamiento del mismo.

Otro aspecto para tener en cuenta por los encuestados es que la disponibilidad de la aplicación no es importante para ellos; hay un elemento que llama la atención y es que existen usuarios no conocen los acuerdos de SLA establecidos por el Departamento para la Prosperidad Social (D.P.S.).

Un punto a atacar y del cual se puede extraer provecho para mejorar la seguridad de la información se determina en que la mitad de los usuarios encuestados pueden identificar los componentes críticos y a su vez conocen la administración de incidencias por lo que esto apoyaría la labor de levantamiento de requerimientos en el futuro; pero no todo es bueno en este aspecto, una amplia mayoría desconocen el procedimiento de respaldo y recuperación que existe en el sistema, pero debemos tener en cuenta que muchos de los usuarios encuestados son funcionales y dicho conocimiento no le es pertinente.

De acuerdo a la percepción de los encuestados, la entidad tiene definidas las políticas de seguridad de la información y cumple con los requisitos legales y reglamentarios con respecto al manejo de la información; también tienen presente que existen lineamientos para la protección de las instalaciones físicas, equipos de cómputo y su entorno; consideran que se realizan verificaciones de manera interna y/o terceros para los procesos de seguridad aunque muchos no conocen con detenimiento si esto se está llevando a cabo; a pesar, varios de los encuestados tienen conocimiento que la entidad ha sufrido ataques informáticos el último año.

Por último, dos terceras partes de los encuestados consideran que la información consultada casi siempre arroja resultados consistentes lo cual es bueno desde el punto de vista que la gran mayoría de los usuarios son funcionales y, teniendo en cuenta que conocen las debilidades que éste posee, podemos aventurarnos a decir que las mejoras son tratables y que se puede proyectar una brecha clara sin muchas dificultades.

5.3. Resultados de Definición de Brecha

La definición de brecha se llevó a cabo teniendo en cuenta el formato de autoevaluación propuesto por Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0., el cual se encuentra disponible en su anexo 4; sin embargo, aunque el formato es el resultado de la opinión de los mejores ingenieros del país y recoge valiosa información, hemos también adicionado un análisis de variables el cual nos servirá como insumo cuando se desarrollen los temas de indicadores y control.

A continuación daremos respuesta a la autoevaluación realizada en la entidad teniendo como alcance la Maestra de Usuarios:

5.3.1. Estructura Organizacional

Requisito	Cumple Si/No	Observación
La entidad cuenta con un líder de Gobierno en línea (líder GEL).	Si	
La entidad cuenta con el comité de seguridad de Gobierno en línea.	No	
La entidad cuenta con el oficial de seguridad.	Si	
La entidad cuenta con personal técnico para realizar las tareas de la seguridad de la información.	Si	El personal no es suficiente.
La entidad cuenta con una integración con otros sistemas de gestión.	Si	Sólo algunos se integran.
La entidad cuenta con apoyo y participación de planeación.	Si	
La entidad cuenta con apoyo y participación de control interno.	Si	
Los funcionarios conocen sus responsabilidades con respecto a la iniciativa de seguridad de la información de la entidad.	No	No todos los funcionarios las conocen.
Los proveedores conocen sus responsabilidades con respecto a la iniciativa de seguridad de la información de la entidad.	Si	
Los ciudadanos conocen sus responsabilidades con respecto a la iniciativa de seguridad de la información de la entidad.	No	

Tabla 2. Fuente: Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0. Anexo 4.

5.3.2. Nivel de Gestión de Seguridad de la información

Nivel	Requisito	Cumple Si/No
Plan de Seguridad Nivel Inicial	La entidad debe definir una política de seguridad que garantice la protección de la información, los datos personales y los activos de información con que cuenta. Para ello, deberá implementar las siguientes acciones:	No
	Identificar el nivel de conocimiento al interior, en temas de seguridad de la información y seguridad informática.	Si
	Definir la política de seguridad a ser implementada.	No
	Divulgar la política de seguridad al interior de la misma.	No
	Conformar un comité de seguridad o asignar las funciones de seguridad al comité GEL	No
	Identificar los activos de información en los procesos, incluyendo los activos documentales (records), de acuerdo con el análisis de procesos realizados.	Si
	Identificar los riesgos y su evaluación, en dichos procesos.	Si
	Definir el plan de acción con los controles y políticas que se implementarán para mitigar los riesgos identificados.	Si
Plan de Seguridad Nivel Básico	Con base en el análisis de procesos realizado en el nivel inicial y la política o plan de seguridad definido, la entidad inicia la ejecución de dicho plan de seguridad para implementar los controles que mitigarán los riesgos identificados, lo cual implica que la entidad presenta avances en la implementación de tales controles.	No
	De acuerdo con el plan de capacitación definido por la entidad en el nivel inicial, esta ejecuta las acciones de capacitación en seguridad, con los responsables de los controles y procesos con los cuales se inicia la ejecución del plan.	No
	La entidad inicia la documentación de políticas y procedimientos de seguridad, de acuerdo con el plan definido.	Si
Plan de	La entidad culmina la implementación de	No

Nivel	Requisito	Cumple Si/No
Seguridad Nivel Avanzado	controles definidos en el nivel inicial.	
	La entidad documenta la totalidad de políticas y procedimientos de seguridad.	No
	La entidad ejecuta las actividades de capacitación en temas de seguridad, con todos los servidores públicos.	No
	La entidad define el plan de verificación periódica de los controles, procedimientos y políticas de seguridad.	No
	La entidad reporta los avances del cumplimiento del plan.	Si
Plan de Seguridad Nivel de Mejoramiento Permanente	La entidad refuerza la divulgación de las políticas de seguridad.	No
	La entidad ejecuta los procedimientos y políticas de seguridad, de manera repetitiva.	No
	La entidad realiza la revisión periódica interna de los riesgos inicialmente detectados, políticas, procedimientos y controles.	Si
	La entidad evalúa sus políticas de seguridad e implementa acciones para mejorarlas.	No

Tabla 3 Fuente: Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0, Anexo 4.

5.3.3. Políticas, controles y métricas por estado

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
5	**POLÍTICA DE SEGURIDAD**												
5.1	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN												
5.1.1	Se tiene documento de la política de seguridad de la Información	S	Control: El documento de la política de seguridad de la información, debe ser aprobado por la dirección, y publicado y comunicado a todos los empleados y partes externas.									X	NO
5.1.2	Se hace revisión y evaluación de este documento y se promulga su lectura y aplicación	S	Control: la política de seguridad de la información debe ser revisada a intervalos planeados, o si cambios significativos ocurren, para garantizar la continuidad, sostenibilidad, efectividad y que es adecuada.									X	NO
6	**ORGANIZACIÓN SEGURIDAD**												
6.1	ORGANIZACIÓN INTERNA												
6.1.1	Compromiso de la dirección con la seguridad de la información	S	Control: La dirección debe apoyar activamente la seguridad dentro de la entidad con un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información.									X	NO
6.1.2	Coordinación de la Seguridad	S	Control: Las actividades de seguridad de la información deben ser coordinadas por los representantes de todas partes de la entidad con roles y funciones laborales pertinentes, según lo definido en la estructura institucional.									X	SI

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
6.1.3	Asignación de responsabilidades	S	Control: Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información.									X	SI
6.1.4	Proceso de Autorización a áreas de procesamiento de información	S	Control: Se debe definir e implementar un proceso de autorización de La dirección para nuevos servicios de procesamiento de información.									X	NO
6.1.5	Se realizan acuerdos de confidencialidad	S	Control: Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la entidad para la protección de la información.									X	SI
6.1.6	Contacto con las autoridades	S	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.									X	SI
6.1.7	Contacto con grupos de interés	S	Control: Contactos adecuados con grupos especiales de interés u otros foros especializados de seguridad o asociaciones profesionales deben ser implementados.									X	NO
6.1.8	Se realiza Auditoría interna	S	Control: La aproximación de la entidad a la gestión de la seguridad de la información y su implementación debe ser revisada independientemente a intervalos planeados o cuando cambios significativos ocurran en la implementación de la seguridad.		X								NO
6.2	TERCEROS												
6.2.1	Identificación de riesgos	S	Control: Los riesgos de la seguridad de la información de los procesos de negocio y sus instalaciones de procesamiento, que incluyan a terceras partes deben ser identificados y adicionalmente se deben implementar los controles apropiados antes de permitir el acceso.									X	SI

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
6.2.2	Aproximación a la seguridad al tratar con clientes	S	Control: Todos los requerimientos de seguridad deben ser atendidos antes de permitir el acceso a los clientes sobre la información o los activos de la entidad.			X				X	X	X	NO
6.2.3	Aproximación a la seguridad en acuerdos con terceros	S	Control: Los acuerdos con terceros que incluyan el acceso, procesamiento, comunicación o gestión de la información de la entidad o las instalaciones de procesamiento de información, o añadir Productos o servicios a las mismas deben cubrir todos los requerimientos de seguridad relevantes.			X				X	X	X	SI
7	**GESTIÓN DE ACTIVOS**												
7.1	RESPONSABILIDAD DE LOS ACTIVOS												
7.1.1	Inventario de activos tecnológicos y de la información	S	Control: Todos los activos deben estar claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes.									X	SI
7.1.2	Responsables de los activos tecnológicos	S	Control: Toda la información y los activos asociados con los servicios de procesamiento de información deben estar en custodia de una parte designada de la entidad.									X	SI
7.1.3	Uso aceptable de los activos tecnológicos	S	Control: Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.									X	SI
7.2	CLASIFICACIÓN DE LA INFORMACIÓN												
7.2.1	Normas para clasificación de la información	S	Control: La información debe ser calsificada en términos de su valor, requisitos legales, sensitividad y criticidad para la organización.					X			X	X	SI

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
7.2.2	Identificación y Manejo de la información	S	Control: Un conjunto de procedimientos para el etiquetado y manipulación debe ser desarrollado e implementado de acuerdo al esquema de clasificación adoptado por la entidad.					X			X	X	NO
8	**SEGURIDAD RECURSO HUMANO**												
8.1	PREVIO A LA CONTRATACIÓN												
8.1.1	Roles y responsabilidades	S	Control: Se deben definir y documentar los roles y responsabilidades de los empleados, contratistas y usuarios de terceras partes, de acuerdo con la política de seguridad de la información de la entidad.									X	SI
8.1.2	Investigación del personal que va a ser contratado	S	Control: Se deben realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a lo cual se va a tener acceso y los riesgos percibidos.									X	SI
8.1.3	Términos y condiciones laborales	S	Control: Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la entidad con relación a la seguridad de la información.									X	SI
8.2	DURANTE EL EMPLEO												

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
8.2.1	Responsabilidades de la dirección	S	Control: La dirección debe exigir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la entidad.									X	SI
8.2.2	Conciencia de la seguridad, educación y entrenamiento	S	Control: Todos los empleados de la entidad y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la entidad, según sea pertinente para sus funciones laborales.									X	NO
8.2.3	Procesos disciplinarios	S	Control: Debe existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad.									X	SI
8.3	TERMINACIÓN DEL CONTRATO O CAMBIO DE EMPLEO												
8.3.1	Responsabilidades en la terminación del contrato	S	Control: Se deben definir y asignar claramente las responsabilidades para llevar a cabo la terminación o el cambio de la contratación laboral.									X	NO
8.3.2	Devolución de activos tecnológicos	S	Control: Todos los empleados, contratistas o usuarios de terceras partes deben devolver todos los activos pertenecientes a la entidad que estén en su poder al finalizar su contratación laboral, contrato o acuerdo.									X	SI
8.3.3	Eliminación de permisos sobre los activos	S	Control: Los retiros de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se deben retirar al finalizar su contratación laboral, contrato o acuerdo o se deben ajustar después del cambio.									X	NO
9	**SEGURIDAD FÍSICA Y**												

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
	AMBIENTAL												
9.1	ÁREAS RESTRINGIDAS												
9.1.1	Perímetro de Seguridad Física	S	Control: Se deben utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información.									X	SI
9.1.2	Controles físicos de entrada	S	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.									X	SI
9.1.3	Aseguramiento de oficinas, cuartos e instalaciones	S	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.									X	SI
9.1.4	Protección contra amenazas externas y ambientales	S	Control: Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.									X	SI
9.1.5	Trabajo en áreas restringidas / seguras	S	Control: Se deben diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras. Por ejemplo, a fin de evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones y la información de la entidad; deberían definirse áreas seguras, resguardadas por un perímetro de seguridad, con barreras de seguridad y controles de acceso apropiados.									X	SI

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
9.1.6	Acceso público, envíos y áreas de carga	S	Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones, se deben controlar y si es posible, aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.									X	SI
9.2	SEGURIDAD DE COMPONENTES TECNOLÓGICOS												
9.2.1	Ubicación y protección de equipos tecnológicos	S	Control: Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado.									X	SI
9.2.2	Seguridad en el suministro de electricidad y servicios (utilities)	S	Control: Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro.									X	NO
9.2.3	Seguridad en el cableado	S	Control: El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información deben estar protegidos contra interceptaciones o daños.									X	NO
9.2.4	Mantenimiento	S	Control: Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.									X	NO
9.2.5	Seguridad de equipos fuera de las áreas seguras	S	Control: Se debe suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la entidad.									X	SI
9.2.6	Eliminación, destrucción y reutilización de equipos	S	Control: Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación.									X	SI

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
9.2.7	Extracción de activos informáticos	S	Control: Ningún equipo, información ni software se deben retirar sin autorización previa.									X	SI
10	**COMUNICACIONES Y MANEJOS OPERATIVOS**												
10.1	PROCEDIMIENTOS OPERATIVOS Y RESPONSABILIDADES												
10.1.1	Documentación de procesos operativos	S	Control: Procedimientos operativos deben ser documentados, operados y estar disponibles a todos los usuarios que los necesiten.									X	NO
10.1.2	Control de Cambios	S	Control: Los cambios a las instalaciones para el procesamiento de la información y a los sistemas, deben ser controlados.									X	NO
10.1.3	Segregación de funciones	S	Control: Las responsabilidades y las aéreas de responsabilidad deben ser segregadas para reducir las oportunidades de modificación no intencional o no autorizada, o un mal uso a las mismas.									X	NO
10.1.4	Separación de los ambientes de Desarrollo, prueba y producción	S	Control: Los ambientes de desarrollo, pruebas e instalaciones operacionales deben separarse para reducir el riesgo de acceso no autorizado o cambios al sistema operacional.									X	NO
10.2	GESTIÓN DE SERVICIOS DE TERCEROS												
10.2.1	Prestación de servicios	S	Control: Se debe garantizar que los controles de seguridad, las definiciones del servicio y los niveles de prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operados por las terceras partes.								X		SI
10.2.2	Monitoreo y revisión de servicios de terceros	S	Control: Los servicios, reportes y registros suministrados por terceras partes se deben controlar y revisar con regularidad y las								X		NO

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
			auditorías se deben llevar a cabo a intervalos regulares.										
10.2.3	Gestión de cambios a servicios de terceros	S	Control: Los cambios en la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas exigentes de seguridad de la información, en los procedimientos y los controles se deben gestionar teniendo en cuenta la importancia de los sistemas y procesos de la entidad involucrados, así como la reevaluación de los riesgos.								X		SI
10.3	PLANEAMIENTO Y ACEPTACIÓN DE SISTEMAS												
10.3.1	Gestión de la capacidad	S	Control: Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.						X				NO
10.3.2	Aceptación de sistemas	S	Control: Se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación y puesta en producción.						X				NO
10.4	PROTECCIÓN CONTRA CÓDIGO MALICIOSO Y MÓVIL												
10.4.1	Controles contra código malicioso	S	Control: Controles de detección, prevención y recuperación para la protección contra código malicioso y los procedimientos de sensibilización de los usuarios deben ser implementados.	X				X	X				SI
10.4.2	Controles contra código móvil	S	Control: Cuando el uso de código móvil esté autorizado, la configuración debe garantizar que el código móvil autorizado opera de acuerdo a lo definido claramente en la política de seguridad, y la ejecución del código móvil no autorizado debe ser prevenida.	X				X	X				SI

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
10.5	COPIAS DE SEGURIDAD												
10.5.1	Respaldo de la información.	S	Control: Se deben hacer copias de seguridad de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.					X		X	X		NO
10.6	GESTIÓN DE LA SEGURIDAD DE LA RED												
10.6.1	Controles de la Red	S	Control: Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.	X						X	X		NO
10.6.2	Seguridad de los Servicios de Red	S	Control: En cualquier acuerdo sobre los servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la entidad o se contratan externamente.	X						X	X		SI
10.7	MANIPULACIÓN EN MEDIOS												
10.7.1	Gestión de medios removibles	S	Control: Deben existir procedimientos para la gestión de medios removibles									X	NO
10.7.2	Destrucción de medios	S	Control: Los medios deben ser eliminados de manera segura y sin peligros (técnica, ambiental e industrialmente), usando procedimientos formales.									X	NO
10.7.3	Procedimientos de manejo de la información	S	Control: Los procedimientos para la manipulación y almacenamiento de información debe ser establecido para proteger la información de la divulgación no autorizada, o un mal uso.									X	NO

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
10.7.4	Seguridad de la documentación de los sistemas intercambio de información.	S	Control: La documentación del sistema debe ser protegida contra el acceso no autorizado.									X	SI
10.8	INTERCAMBIO DE INFORMACIÓN												
10.8.1	Políticas y procedimientos del intercambio de información	S	Control: Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación. Haciendo uso del manual de interoperabilidad de GEL.								X		NO
10.8.2	Acuerdos para el intercambio de información	S	Control: Se deben establecer acuerdos para el intercambio de la información y del software entre la entidad y partes externas.								X		NO
10.8.3	Medios físicos en transito	S	Control: Los medios que contienen información se deben proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la entidad.								X		SI
10.8.4	Mensajería Electrónica	S	Control: La información contenida en la mensajería electrónica debe tener la protección adecuada.								X		SI
10.8.5	Sistemas de información de la entidad	S	Control: Se deben establecer, desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información de la entidad.								X		NO
10.9	SERVICIOS DE COMERCIO ELECTRÓNICO												

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
10.9.1	Comercio Electrónico	E	Control: La información involucrada en el comercio electrónico que se transmite por las redes públicas debe estar protegida contra actividades fraudulentas, dispuestas por contratos y divulgación o modificación no autorizada.			X					X		NA
10.9.2	Transacciones en Línea	E	Control: La información involucrada en las transacciones en línea debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje.			X					X		NA
10.9.3	Información pública / disponible al público	E	Control: La integración de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no autorizada.			X					X		NA
10.10	MONITOREO												
10.10.1	Registros de Auditoría	S	Control: Se deben elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.	X	X								SI
10.10.2	Monitoreo del uso del sistema	S	Control: Se deben establecer procedimientos para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad.	X	X								SI
10.10.3	Protección de registros de monitoreo	S	Control: Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados.	X	X								SI

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
10.10.4	Registros de monitoreo de administradores y operadores	S	Control: Se debe registrar las actividades tanto del operador como del administrador del sistema.	X	X								SI
10.10.5	Registro de fallas	S	Control: Las fallas se deben registrar y analizar, y se deben tomar las acciones adecuadas.	X	X								SI
10.10.6	Sincronía / sincronización de relojes	S	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la entidad o del dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta y acordada.	X	X								SI
11	**CONTROL DE ACCESO A LA INFORMACIÓN**												
11.1	REQUERIMIENTOS DE CONTROL DE ACCESO DE ACUERDO A LAS NECESIDADES DEL NEGOCIO												
11.1.1	Política de Control de Acceso	S	Control: Se debe establecer, documentar y revisar la política de control de acceso con base en los requisitos de la entidad y de la seguridad para el acceso.				X			X	X		NO
11.2	GESTIÓN DE ACCESO DE LOS USUARIOS												
11.2.1	Registro de Usuarios	S	Control: Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.				X			X	X		SI
11.2.2	Gestión de privilegios	S	Control: Se debe restringir y controlar la asignación y el uso de privilegios.				X			X	X		NO

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
11.2.3	Gestión de Contraseñas (passwords)	S	Control: La asignación de contraseñas se debe controlar a través de un proceso formal de gestión.				X			X	X		SI
11.2.4	Revisión de los permisos asignados a los usuarios	S	Control: La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.				X			X	X		NO
11.3	RESPONSABILIDADES DE LOS USUARIOS												
11.3.1	Uso de las contraseñas	S	Control: Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas.				X				X		SI
11.3.2	Equipos desatendidos	S	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.				X				X		SI
11.3.3	Política de escritorios y pantallas limpias	S	Control: Se debe adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.				X				X		NO
11.4	CONTROL DE ACCESO A LA RED DE DATOS												
11.4.1	Políticas para el uso de los servicios de la red de datos	S	Control: Los usuarios sólo deben tener acceso a los servicios para cuyo uso están específicamente autorizados.	X			X				X		NO
11.4.2	Autenticación de usuarios para conexiones externas	S	Control: Se deben emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos.	X			X				X		NO
11.4.3	Identificación de equipos en la red	S	Control: La identificación automática de los equipos se debe considerar un medio para autenticar conexiones de equipos y ubicaciones específicas.	X			X				X		NO
11.4.4	Diagnóstico remoto y protección de la configuración de puertos	S	Control: El acceso lógico y físico a los puertos de configuración y de diagnóstico debe estar controlado.	X			X				X		NO

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
11.4.5	Separación en la redes	S	Control: En las redes se deben separar los grupos de servicios de información, usuarios y sistemas de información.	X			X				X		NO
11.4.6	Control de conexión a la red de trabajo	S	Control: Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la entidad, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control del acceso y los requisitos de aplicación de la entidad.	X			X				X		NO
11.4.7	Control de enrutamiento de red	S	Control: Se deben implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso de las aplicaciones de la entidad.	X			X				X		SI
11.5	CONTROL DE ACCESO A LOS SISTEMAS OPERATIVOS												
11.5.1	Procedimientos para inicio de sesión de las estaciones de trabajo	S	Control: El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de inicio seguro.	X			X						SI
11.5.2	Identificación y autenticación de los usuarios.	S	Control: Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.	X			X						SI
11.5.3	Sistema de gestión de contraseñas.	S	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	X			X						SI

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
11.5.4	Uso de las utilidades del sistema	S	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.	X			X						NO
11.5.5	Tiempo de la inactividad de la sesión	S	Control: Las sesiones inactivas se deben suspender después de un período definido de inactividad.	X			X						NO
11.5.6	Limitación en los periodos de tiempo de conexión a servicios y aplicaciones	S	Control: Se deben utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo.	X			X						NO
11.6	CONTROL DE ACCESO A LAS APLICACIONES												
11.6.1	Restricción de acceso a los sistemas de información	S	Control: Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.	X			X						SI
11.6.2	Aislamiento de sistemas sensibles	S	Control: Los sistemas sensibles deben tener un entorno informático dedicado (aislados).	X			X						SI
11.7	COMPUTACIÓN MÓVIL Y TELETRABAJO												
11.7.1	Computación Móvil y comunicaciones	S	Control: Se debe establecer una política formal y se debe adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.	X			X						NO
11.7.2	Teletrabajo / trabajo remoto	S	Control: Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.	X			X						NO
12	**DESARROLLO DE SOFTWARE**												

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
12.1	REQUERIMIENTOS DE SEGURIDAD PARA LOS SISTEMAS DE INFORMACIÓN												
12.1.1	Análisis y especificaciones de los requerimientos de seguridad	S	Control: Las declaraciones sobre los requisitos de la entidad para nuevos sistemas de información o mejoras a los sistemas existentes deben especificar los requisitos para los controles de seguridad.	X		X							SI
12.2	PROCESAMIENTO CORRECTO EN APLICACIONES												
12.2.1	Validación de los datos de entrada	S	Control: Los datos de entrada para las aplicaciones deben ser validados para garantizar que estos datos son correctos y apropiados.							X	X		NO
12.2.2	Control del procesamiento interno	S	Control: Validaciones deben ser incorporadas en las aplicaciones para detectar cualquier corrupción de información durante errores de procesamiento o actos deliberados.	X									NO
12.2.3	Integridad de los mensajes	S	Control: Los requerimientos para garantizar la autenticidad y proteger la integridad de los mensajes en las aplicaciones deben ser identificados, y los controles apropiados identificados e implementados.							X			NO
12.2.4	Validación de los datos de salida	S	Control: Los datos de salida de una aplicación deben ser validados para garantizar que el procesamiento de información almacenada es correcta y apropiada a las circunstancias.	X							X		NO
12.3	CONTROLES CRIPTOGRÁFICOS												

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
12.3.1	Política para el uso de controles criptográficos	S	Control: Se debe desarrollar o implementar una política sobre el uso de controles criptográficos para la protección de la información.			X						X	NO
12.3.2	Gestión de llaves	S	Control: Se debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la entidad.			X							SI
12.4	SEGURIDAD EN LOS ARCHIVOS DEL SISTEMA (SYSTEM FILES)												
12.4.1	Control del software operacional (operativo)	S	Control: Deben existir procedimientos en funcionamiento para controlar la instalación de software en los sistemas operativos.					X		X			NO
12.4.2	Protección de los datos en sistemas de prueba	S	Control: Datos de prueba deben ser seleccionados cuidadosamente, protegidos y controlados.					X		X	X		NO
12.4.3	Control de acceso a las librerías de código fuente	S	Control: El acceso al código fuente de los programas debe ser restringido.					X		X	X		SI
12.5	SEGURIDAD EN EL DESARROLLO Y EN LOS PROCESOS DE SOPORTE TÉCNICO												
12.5.1	Procedimientos para el control de cambios	S	Control: Se deben controlar la implementación de cambios utilizando procedimientos formales de control de cambios.	X									NO
12.5.2	Revisión técnica de aplicaciones después de cambios al sistema operativo	S	Control: Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la entidad.	X									NO

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
12.5.3	Restricciones a cambios en paquetes de software	S	Control: Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	X									NO
12.5.4	Fuga de información	S	Control: Se deben evitar las oportunidades para que se produzca fuga de información.	X									SI
12.5.5	Desarrollo de software por parte de Outsourcing / contratado externamente	S	Control: La entidad debe supervisar y monitorear el desarrollo de software contratado externamente.	X									NO
12.6	GESTIÓN TÉCNICA DE VULNERABILIDADES												
12.6.1	Control técnico de vulnerabilidades	S	Control: Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la entidad a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.	X									SI
13	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**												
13.1	REPORTE DE EVENTOS DE SEGURIDAD INFORMÁTICA Y DE SUS DEBILIDADES												
13.1.1	Reporte de eventos de Seguridad de la información.	S	Control: Los eventos de seguridad de la información deben ser reportados a través de los canales con la dirección tan rápido como sea posible.	X									SI

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
13.1.2	Reporte de debilidades de seguridad	S	Control: Todos los funcionarios, contratistas y terceros que utilicen los sistemas de información y servicios, se les debe requerir identificar y reportar cualquier debilidad observada o sospechosa.	X									SI
13.2	GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA Y DE SU MEJORAMIENTO												
13.2.1	Responsabilidades y procedimientos	S	Control: Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	X									SI
13.2.2	Aprendizaje a partir de los incidentes de seguridad	S	Control: Deben existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.	X									NO
13.2.3	Recolección de evidencia	S	Control: Cuando una acción de seguimiento contra una persona o entidad, después de un incidente de seguridad de la información, implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con lo establecido en la legislación vigente.	X									SI
14	**GESTIÓN DE LA CONTINUIDAD DE NEGOCIO**												

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
14.1	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO												
14.1.1	Inclusión de seguridad de la información en el proceso de administración de la continuidad del negocio	S	Control: Se debe desarrollar y mantener un proceso de gestión para la continuidad de la entidad, el cual trate los requisitos de seguridad de la información necesarios para la continuidad de la actividad de entidad.						X				SI
14.1.2	Continuidad del negocio y análisis de impacto (BIA)	S	Control: Se deben identificar los eventos que pueden ocasionar interrupciones en los procesos de la entidad junto con los riesgos identificados de dichas interrupciones, así como sus consecuencias para la seguridad de la información.						X				SI
14.1.3	Desarrollo e implementación de planes de continuidad	S	Control: Se deben desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requeridos, después de la interrupción o la falla de los procesos críticos para el negocio.						X				SI
14.1.4	Marco de planeación para la continuidad del negocio	S	Control: Se debe mantener una sola estructura de los planes de continuidad de la entidad, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento.						X				SI

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
14.1.5	Pruebas, mantenimiento y revisión de los planes de continuidad del negocio	S	Control: Los planes de continuidad de la entidad se deben someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.						X				SI
15	**CUMPLIMIENTO**												
15.1	CUMPLIMIENTO CON REQUERIMIENTOS LEGALES												
15.1.1	Identificación de leyes / legislación aplicables	S	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la entidad para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la entidad.									X	SI
15.1.2	Derechos de autor y propiedad Intelectual	S	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.									X	SI
15.1.3	Protección de los registros de la organización	S	Control: Los registros importantes se deben proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales definidos para las entidades del Estado.									X	SI
15.1.4	Protección de los datos y privacidad de la información personal	S	Control: Se debe garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.									X	NO

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
15.1.5	Prevención mal uso de los componentes tecnológicos	S	Control: Se debe disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.									X	SI
15.1.6	Regulación de controles criptográficos	S	Control: Se deben utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.			X				X	X	X	SI
15.2	REVISIÓN DE LA POLÍTICA DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO												
15.2.1	Cumplimiento de los diferentes requerimientos y controles establecidos por la política de seguridad	S	Control: Los directores deben garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y los lineamientos de seguridad.									X	SI
15.2.2	Verificación del cumplimiento técnico	S	Control: Los sistemas de información se deben verificar periódicamente para determinar el cumplimiento con los lineamientos de implementación de la seguridad.(Veracidad e integridad de la Información y que esta se encuentre disponible)									X	NO
15.3	CONSIDERACIONES RELACIONADAS CON LA AUDITORIA INTERNA												
15.3.1	Controles para auditoría del sistema	S	Control: Los requisitos y la actividades de auditoría que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.									X	NO

Num.	Nombre	Seleccionado / Excepción	Descripción / Justificación	Protección del Servicio	Registro y Auditoría	No Repudiación	Control de Acceso	Disponibilidad de la Información	Disponibilidad del Servicio	Integridad	Privacidad y Confiabilidad	Políticas Generales	Desarrollado
15.3.2	Protección de las herramientas para auditoría del sistema	S	Control: Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro.									X	NO

Tabla 4 Fuente: Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0. Anexo 4.

5.3.4. Análisis de las variables que existen en el sistema de la maestra de usuarios

VARIABLE	TIPO DE DATO	LONGITUD MÁXIMA	VALORES ESPERADOS	REGISTROS VÁLIDOS	%
FechaFinReporte	Fecha		Valor mayor o igual a 1900/01/01 y menor o igual a 2020/12/31.En formato YYYY/MM/DD	-	0,00%
FechaInicioReporte	Fecha		Valor mayor o igual a 1900/01/01 y menor o igual a 2020/12/31.En formato YYYY/MM/DD	-	0,00%
CantidadBeneficioConsolidado	Decimal	(18, 2)		-	0,00%
CantidadTutelas	Número entero		Valores mayores o iguales a 0	-	0,00%
CantidadUltimoBeneficio	Decimal	(18, 2)		-	0,00%
CicloReporte	Número entero			-	0,00%
CodigoBeneficiario	Número entero		Valores mayores o iguales a 1	-	0,00%
CodigoCorregimiento	Texto	50	Códigos de DIVIPOLA. Longitud menor o igual a 9.	-	0,00%
CodigoDepartamentoAtencion	Texto	50	Códigos de DIVIPOLA. Longitud igual a 2.	-	0,00%
CodigoDepartamentoNacimiento	Texto	50	Códigos de DIVIPOLA. Longitud igual a 2.	-	0,00%
CodigoMunicipioAtencion	Texto	50	Códigos de DIVIPOLA. Longitud igual a 5	-	0,00%
CodigoMunicipioNacimiento	Texto	50	Códigos de DIVIPOLA. Longitud igual a 5	-	0,00%
FechaInscripcionBeneficiario	Fecha			-	0,00%
FechaUltimoBeneficioAsignado	Fecha			-	0,00%
Llamada	Texto	50		-	0,00%
NombreDepartamentoAtencion	Texto	50	Departamentos de DIVIPOLA. Longitud mayor o igual a 4 y menor o igual a 60.	-	0,00%
NombreMunicipioAtencion	Texto	50	Municipios de DIVIPOLA. Longitud mayor o igual a 3 y menor o igual a 100.	-	0,00%
Parentesco	Texto	26		-	0,00%
TipoAsignacionBeneficio	Texto	50		-	0,00%
TipoBeneficio	Texto	50	MONETARIO, ESPECIE	-	0,00%

VARIABLE	TIPO DE DATO	LONGITUD MÁXIMA	VALORES ESPERADOS	REGISTROS VÁLIDOS	%
TipoPoblacion	Texto	30	DESPLAZADOS, SISBEN, TRANSICION, UNIDOS, INDIGENAS, VICTIMAS, VULNERABLE	-	0,00%
Titular	Texto	2		-	0,00%
Tutelas	Texto	2	NO, SI	-	0,00%
ValorBeneficioConsolidadoAsignado	Decimal	(18, 2)		-	0,00%
ValorUltimoBeneficioAsignado	Decimal	(18, 2)		-	0,00%
EstadoPersona	Texto	50	No definido	-	0,00%
TelefonoCelular2	Texto	20	Longitud mayor o igual a 14	2.022	0,01%
NombreDepartamentoNacimiento	Texto	50	Longitud mayor o igual a 4 y menor o igual a 60	29.952	0,14%
NombreMunicipioNacimiento	Texto	50	Longitud mayor o igual a 3 y menor o igual a 100	29.952	0,14%
EPS	Texto	50		49.654	0,24%
TipoFormacion	Texto	50		64.691	0,31%
Estrato	Número entero		Valor mayor o igual a 1 y menor o igual a 6	88.719	0,43%
TelefonoFijo2	Texto	20	Longitud mayor o igual a 14	166.391	0,80%
LugarExpedicionDocumento	Texto	28	Longitud mayor o igual a 2	187.843	0,91%
BeneficiarioSISBEN	Texto	2	NO, SI	190.587	0,92%
CondicionSexual	Texto	50		523.586	2,52%
CorreoElectronico	Texto	50	Longitud mayor o igual a 5 y menor o igual a 50. Debe contener el símbolo @.	1.408.166	6,79%
CodigoFamilia	Número entero		Valores mayores o iguales a 1	3.203.735	15,44%
Localidad	Texto	100		4.255.669	20,51%
PuntajeSISBEN	Decimal	(18, 2)	Valor mayor o igual a 1 y menor o igual a 100	6.361.631	30,66%
Pais	Texto	50	Pais de DIVIPOLA. Longitud mayor o igual a 2.	6.859.734	33,06%
IPS	Texto	150		8.789.840	42,36%
TelefonoFijo1	Texto	20	Longitud mayor o igual a 14	9.273.920	44,69%
FechaExpedicionDocumento	Fecha		Valor mayor o igual a 1900/01/01 y menor o igual a 2030/12/31.En formato YYYY/MM/DD	9.481.380	45,69%
TelefonoCelular1	Texto	20	Longitud mayor o	10.650.878	51,33%

VARIABLE	TIPO DE DATO	LONGITUD MÁXIMA	VALORES ESPERADOS	REGISTROS VÁLIDOS	%
			igual a 14		
Vereda	Texto	172		12.318.529	59,37%
Barrio	Texto	214		14.059.270	67,75%
Bancarizado	Texto	2	NO, SI	14.247.188	68,66%
SegundoNombre	Texto	34	Longitud mayor o igual a 2 y menor o igual a 20	15.410.434	74,27%
Zona	Texto	50		16.642.805	80,20%
Direccion	Texto	196	Longitud menor o igual a 100.	16.684.464	80,41%
FechaNacimiento	Fecha		Valor mayor o igual a 1900/01/01 y menor o igual a 2030/12/31.En formato YYYY/MM/DD	18.509.550	89,20%
SegundoApellido	Texto	44	Longitud mayor o igual a 2 y menor o igual a 30	19.339.223	93,20%
Genero	Texto	10	HOMBRE, MUJER, NO REPORTA	19.500.388	93,98%
NumeroDocumento	Texto	25	Longitud mayor o igual a 4 y menor o igual a 12	20.542.775	99,00%
TipoDocumento	Texto	21	RC,TI, CC, CE, AS, MS, ND, PADE, CD,NI,RN	20.545.376	99,01%
PrimerApellido	Texto	47	Longitud mayor o igual a 2 y menor o igual a 47	20.607.425	99,31%
PrimerNombre	Texto	42	Longitud mayor o igual a 2 y menor o igual a 42	20.616.056	99,35%
Discapacidad	Texto	9		20.750.350	100,00%
EstadoBeneficiario	Texto	24		20.750.350	100,00%
EstadoCivil	Texto	21	CA, DI, SO, UL, VI	20.750.350	100,00%
Etnia	Texto	42		20.750.350	100,00%
NivelEscolaridad	Texto	50		20.750.350	100,00%
RangoEdad	Texto	30	Campo Calculado	20.750.350	100,00%
UltimaFechaActualizacion	Fecha		Valor mayor o igual a 1900/01/01 y menor o igual a 2030/12/31.En formato YYYY/MM/DD	20.750.350	100,00%

Tabla 5 Fuente: Maestra de Beneficiados

Como se puede evidenciar, existen 65 variables que se pueden capturar para el análisis de información en la aplicación; la labor que se ha llevado a cabo ha sido ardua y muy positiva ya que por primera vez se puede consolidar la información de los usuarios de los programas y entidades adscritas en una sola bodega de datos para análisis.

Sin embargo, debido a la falta de política, principios y lineamientos sobre la herramienta en particular, se han presentado problemas que no han permitido que los datos se carguen de manera correcta al existir diferentes puntos de vista sobre la definición (No existente) de variables y en algunos casos, la modificación de tipos o longitudes de datos que han entorpecido el buen proceso de funcionamiento y la explotación correspondiente de los cubos.

Entre la información de los datos disponibles, sólo se puede analizar si una variable posee información o se encuentra vacía. Como podemos identificar, existen 26 variables que no se están almacenando por ninguno de los enlaces de información, por lo cual, dicha información no se ha logrado explotar; esto es el 40% de las variables en el sistema.

Un asunto más: 44 variables de información poseen menos del 50% de información disponible; esto es el 67% de las variables disponibles. Ello nos indica que sólo se está explotando el 30% de la capacidad de la información por lo cual, algunos procesos misionales se pueden ver afectados al intentar mejorar y focalizar la población atendida para la optimización de los procesos y recursos.

5.4. Plan de trabajo para reducción de brecha

Para la definición del plan de trabajo para la reducción de la brecha, tomaremos como punto inicial el cumplimiento de todos los requisitos que componen la estructura organizacional los cuales son:

- La entidad cuenta con un líder de Gobierno en línea (líder GEL).
- La entidad cuenta con el comité de seguridad de Gobierno en línea.
- La entidad cuenta con el oficial de seguridad.
- La entidad cuenta con personal técnico para realizar las tareas de la seguridad de la información.
- La entidad cuenta con una integración con otros sistemas de gestión.
- La entidad cuenta con apoyo y participación de planeación.
- La entidad cuenta con apoyo y participación de control interno.
- Los funcionarios conocen sus responsabilidades con respecto a la iniciativa de seguridad de la información de la entidad.
- Los proveedores conocen sus responsabilidades con respecto a la iniciativa de seguridad de la información de la entidad.
- Los ciudadanos conocen sus responsabilidades con respecto a la iniciativa de seguridad de la información de la entidad.

Los resultados iniciales de éste análisis se encuentran contenidos en el ítem 5.3.1. “Estructura organizacional”, por lo cual éstos no se colocarán en este apartado.

Cumplir los requisitos de la estructura organizacional es importante ya que sobre ello se puede garantizar que la entidad siempre va a poseer un responsable o doliente que se apersonará de llevar adelante y cumplir con cada uno de los Planes de Seguridad indicados en el documento de Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0 publicado por el Ministerio. De igual forma, ésta persona se encargará de estar a la vanguardia de cada uno de los avances y modificaciones que surjan sobre la Estrategia de Gobierno en Línea o sobre el Modelo de Seguridad de la Información propuesto en esta misma estrategia.

Para la reducción de la brecha desde la estructura organizacional se propone lo siguiente:

Requisito	Cumple Si/No	Acción
La entidad cuenta con un líder de Gobierno en línea (líder GEL).	Si	NA
La entidad cuenta con el comité de seguridad de Gobierno en línea.	No	Resolución de creación de Comité de seguridad (Entre sus funciones estará Gobierno en Línea).
La entidad cuenta con el oficial de seguridad.	Si	NA
La entidad cuenta con personal técnico para realizar las tareas de la seguridad de la información.	Si	Se debe realizar la gestión de CDP o solicitud de planta para estos cargos.
La entidad cuenta con una integración con otros sistemas de gestión.	Si	Se debe unificar y documentar los procesos de inter – operabilidad de datos del Sector. NIST SP 800-47
La entidad cuenta con apoyo y participación de planeación.	Si	NA
La entidad cuenta con apoyo y participación de control interno.	Si	NA
Los funcionarios conocen sus responsabilidades con respecto a la iniciativa de seguridad de la información de la entidad.	No	Empezar a desarrollar y diseñar campañas de sensibilización con la información. NIST SP 800-84
Los proveedores conocen sus responsabilidades con respecto a la iniciativa de seguridad de la información de la entidad.	Si	
Los ciudadanos conocen sus responsabilidades con respecto a la iniciativa de seguridad de la	No	Empezar a desarrollar y diseñar campañas de sensibilización con la

Requisito	Cumple Si/No	Acción
información de la entidad.		información. NIST SP 800-84

Tabla 6 Fuente: Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0. Anexo 4.

Si bien la labor de cumplir con los requisitos de estructura organizacional son importantes, también se debe apuntar a que se cumplan los requisitos de la Gestión de Seguridad para que la entidad, a través de tramos o fases, empiece a llevar a cabo acciones que conlleven al cumplimiento de los requisitos y llevar a la misma al Nivel Inicial del Plan de Seguridad propuesto por el Modelo de Seguridad de la Información.

Para la reducción de la brecha en estos aspectos se propone la realización de las siguientes actividades:

Requisito	Cumple Si/No	Acción
La entidad debe definir una política de seguridad que garantice la protección de la información, los datos personales y los activos de información con que cuenta. Para ello, deberá implementar las siguientes acciones:	No	Para el cumplimiento de éste requisito, es necesario que todos los ítems siguientes se puedan desarrollar de manera satisfactoria.
Identificar el nivel de conocimiento al interior, en temas de seguridad de la información y seguridad informática.	Si	NA
Definir la política de seguridad a ser implementada.	No	Realizar un análisis de las necesidades a cubrir y desarrollar la política de seguridad.
Divulgar la política de seguridad al interior de la misma.	No	En el momento que se encuentre lista la política de seguridad, el área de comunicaciones realizará la divulgación correspondiente.
Conformar un comité de seguridad o asignar las funciones de seguridad al comité GEL	No	Se debe realizar una **Resolución** de creación de Comité de seguridad (Entre sus funciones estará Gobierno en Línea).
Identificar los activos de información en los procesos, incluyendo los activos	Si	NA

Requisito	Cumple Si/No	Acción
documentales (records), de acuerdo con el análisis de procesos realizados.		
Identificar los riesgos y su evaluación, en dichos procesos.	Si	NA
Definir el plan de acción con los controles y políticas que se implementarán para mitigar los riesgos identificados.	Si	NA

Tabla 7 Fuente: Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0. Anexo 4.

5.5. Definición del Alcance del Sistema

Las Políticas Generales de la "Maestra de Beneficiarios" rigen para todos los funcionarios y contratistas del Departamento Administrativo para la Prosperidad Social (D.P.S.) al igual que los colaboradores de las entidades adscritas del Sector; éstas deberán ser acatadas por todas aquellas personas que en el cumplimiento de sus funciones o necesidades interactúen con los recursos y/o servicios de la "Maestra de Beneficiarios" de manera directa o indirecta.

5.6. Política de Seguridad

La Política de Seguridad de la Información es la declaración general que representa la posición de la Dirección del Departamento Administrativo para la Prosperidad Social (D.P.S.), con respecto a la protección de los activos de información (los funcionarios, la información, los procesos, las tecnologías de información incluido el hardware y el software), al apoyo, generación y publicación de sus políticas, procedimientos e instructivos.

El Departamento Administrativo para la Prosperidad Social (D.P.S.), para el cumplimiento de su misión, visión, objetivos estratégicos y apegado a su código de ética, establece la función de Seguridad de la Información de la "Maestra de Beneficiarios", con el objetivo de:

- Minimizar el riesgo en las funciones más importantes del sistema.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus beneficiarios, directivos, contratistas y funcionarios.
- Apoyar la innovación tecnológica en la operación del sistema.
- Implementar el sistema de gestión de seguridad de la información del sistema.

- Proteger los activos tecnológicos involucrados en el sistema.
- Establecer las políticas, procedimientos e instructivos del sistema que se encuentren relacionados con la seguridad de la información.
- Fortalecer la cultura de seguridad de la información del sistema en los funcionarios, contratistas, terceros, practicantes y beneficiarios del Departamento Administrativo para la Prosperidad Social (D.P.S.) al igual que en la ciudadanía.
- Garantizar la continuidad del funcionamiento del sistema frente a incidentes.

5.6.1. Alcance

Las Políticas Generales de la "Maestra de Beneficiarios" rigen para todos los funcionarios y contratistas del Departamento Administrativo para la Prosperidad Social (D.P.S.) al igual que los colaboradores de las entidades adscritas del Sector; éstas deberán ser acatadas por todas aquellas personas que en el cumplimiento de sus funciones o necesidades interactúen con los recursos y/o servicios de la "Maestra de Beneficiarios" de manera directa o indirecta.

5.6.2. Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deben adherirse en un 100% de la política.

A continuación se establecen las 13 políticas de seguridad que soportan la Gestión de Seguridad de la Información de la "Maestra de Beneficiarios":

- El Departamento Administrativo para la Prosperidad Social (D.P.S.), ha decidido definir, implementar, operar y mejorar de forma continua la Gestión de Seguridad de la Información de la "Maestra de Beneficiarios", soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

- La información almacenada tanto en los equipos de cómputo como en los servidores de la Entidad y tienen relación con la "Maestra de Beneficiarios" es propiedad del Departamento Administrativo para la Prosperidad Social (D.P.S.) y cada funcionario es responsable por proteger su integridad, confidencialidad y disponibilidad.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas, proveedores, directivos o terceros.

- El Departamento Administrativo para la Prosperidad Social (D.P.S.), protegerá la información generada, procesada o resguardada por la "Maestra de Beneficiarios", su infraestructura tecnológica y activos del

riesgo que se genera de los accesos otorgados a terceros, o como resultado de un servicio interno en outsourcing.

- El Departamento Administrativo para la Prosperidad Social (D.P.S.), protegerá la información creada, procesada, transmitida o resguardada por la “Maestra de Beneficiarios”, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- El Departamento Administrativo para la Prosperidad Social (D.P.S.), protegerá la información de la “Maestra de Beneficiarios” de las amenazas originadas por parte de funcionarios, contratistas o directivos.

- El Departamento Administrativo para la Prosperidad Social (D.P.S.), protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta los procesos de funcionamiento de la “Maestra de Beneficiarios”.

- El Departamento Administrativo para la Prosperidad Social (D.P.S.), controlará la operación de los procesos de la “Maestra de Beneficiarios” garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- El Departamento Administrativo para la Prosperidad Social (D.P.S.), implementará control de acceso a la información, sistemas y recursos de red en los cuales se involucren los procesos de funcionamiento de la “Maestra de Beneficiarios”.

- El Departamento Administrativo para la Prosperidad Social (D.P.S.), garantizará que la seguridad sea parte integral del ciclo de vida del sistema de la “Maestra de Beneficiarios”.

- El Departamento Administrativo para la Prosperidad Social (D.P.S.), garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información, una mejora efectiva del modelo de seguridad de la información de la “Maestra de Beneficiarios”.

- El Departamento Administrativo para la Prosperidad Social (D.P.S.), garantizará la disponibilidad y continuidad de la operación de la “Maestra de Beneficiarios” de acuerdo al impacto que pueden generar los eventos.

- El Departamento Administrativo para la Prosperidad Social (D.P.S.), garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

5.7. Análisis y Evaluación de Riesgos

Para determinar la probabilidad de un evento adverso futuro, las amenazas de los sistemas de TI deben ser analizadas en conjunto con las vulnerabilidades potenciales y los controles existentes en los mismos. El impacto se refiere a la magnitud del daño que podría ser causado porque las amenazas exploten una vulnerabilidad. El nivel de impacto es determinado por el impacto potencial en el logro de la misión y el valor relativo de los activos de TI que resultaren afectados.

La metodología de análisis y evaluación de riesgos está compuesta por la Identificación de Activos, Riesgo Inherente, Controles, Tratamiento, Relación Costo Beneficio (como se puede ver en el Anexo 1. Análisis y Evaluación de Riesgos).

5.8. Listado de Indicadores

CÓDIGO	1
NOMBRE DEL INDICADOR	Procesamiento de archivos.
INDICADOR	Cantidad de Archivos Procesados de acuerdo al estado del proceso del sistema de la Maestra de Beneficiarios.
EJE DE VALORACIÓN	Eficiencia.
ÁMBITO	General.
DESCRIPCIÓN	Este Indicador busca presentar la información correspondiente al Número de Archivos Correctos y el Número de Archivos Fallidos que se presentaron en el proceso de Cargue, dependiendo del periodo de tiempo y el programa o entidad seleccionado.
UNIDAD DE MEDIDA	Archivos.
TIPO DE INDICADOR	Conteo.
PERIODICIDAD	Diario.
FÓRMULA DE CÁLCULO	Sumatoria de archivos procesados con estado Correcto. Sumatoria de archivos procesados con estado Incorrecto.
NOTAS	El resultado de la información podrá ser consultado por mes, trimestre, año, entidad y programa.

CÓDIGO	2
NOMBRE DEL INDICADOR	Consulta de reportes.
INDICADOR	Cantidad de consultas efectivas realizadas a los reportes

	disponibles del sistema de la Maestra de Beneficiarios.
EJE DE VALORACIÓN	Eficiencia.
ÁMBITO	General.
DESCRIPCIÓN	Este Indicador busca presentar la información correspondiente al Número de consultas efectivas realizadas por los usuarios a los reportes disponibles del sistema dependiendo del periodo de tiempo que se haya seleccionado.
UNIDAD DE MEDIDA	Consultas.
TIPO DE INDICADOR	Conteo.
PERIODICIDAD	Mensual.
FÓRMULA DE CÁLCULO	Sumatoria de consultas realizadas a los reportes disponibles en el sistema.
NOTAS	El resultado de la información podrá ser consultado por mes, trimestre y año.

CÓDIGO	3
NOMBRE DEL INDICADOR	Procesamiento del sistema.
INDICADOR	Cantidad de tiempo que el sistema tarda en procesar una carga.
EJE DE VALORACIÓN	Eficacia.
ÁMBITO	General.
DESCRIPCIÓN	Este Indicador busca presentar la información correspondiente al tiempo invertido por el sistema para el procesamiento de un archivo de carga.
UNIDAD DE MEDIDA	Tiempo de procesamiento (HH:MM:SS).
TIPO DE INDICADOR	Suma.
PERIODICIDAD	Mensual.
FÓRMULA DE CÁLCULO	Sumatoria del tiempo invertido en el procesamiento de un archivo de carga.
NOTAS	El resultado de la información podrá ser consultado por mes, trimestre y año.

CÓDIGO	4
NOMBRE DEL INDICADOR	Oportunidad de cargue.
INDICADOR	Cantidad de días de oportunidad del cargue de los archivos del sistema Maestra de beneficiarios.
EJE DE	Eficiencia.

VALORACIÓN	
ÁMBITO	General.
DESCRIPCIÓN	Este Indicador busca evidenciar los días que cada programa emplea para el cargue de los archivos respecto a la fecha definida para la ejecución de este proceso y que pueden ser calculados en un periodo de tiempo, Entidad o Programa seleccionado. De acuerdo al resultado obtenido se puede identificar si el proceso se hace antes, durante o después del tiempo definido.
UNIDAD DE MEDIDA	Días.
TIPO DE INDICADOR	Conteo.
PERIODICIDAD	Mensual.
FÓRMULA DE CÁLCULO	Diferencia en días entre la fecha li mite de cargue y la fecha real de cargue.
NOTAS	El resultado de la información podrá ser consultado por mes, trimestre, año, entidad y programa.

CÓDIGO	5
NOMBRE DEL INDICADOR	Disponibilidad del sistema.
INDICADOR	Cantidad de tiempo en el cual el sistema se encuentra fuera de línea.
EJE DE VALORACIÓN	Eficiencia.
ÁMBITO	General.
DESCRIPCIÓN	Este Indicador busca evidenciar la cantidad de tiempo que el sistema, por diferentes aspectos no se ha encontrado disponible para la realización de las diferentes actividades de los funcionaros y la ciudadanía.
UNIDAD DE MEDIDA	Tiempo (HH:MM:SS).
TIPO DE INDICADOR	Suma.
PERIODICIDAD	Mensual.
FÓRMULA DE CÁLCULO	Sumatoria de los diferentes tiempos en los cuales el sistema no se ha encontrado disponible.
NOTAS	El resultado de la información podrá ser consultado por mes, trimestre, año, entidad y programa.

CÓDIGO	6
NOMBRE DEL INDICADOR	Integridad de la información.
INDICADOR	Cantidad de registros afectados por agentes no autorizados.

EJE DE VALORACIÓN	Eficacia.
ÁMBITO	General.
DESCRIPCIÓN	Este Indicador busca evidenciar la cantidad de registros que por diferentes factores o agentes son afectados de manera fraudulenta o no autorizada.
UNIDAD DE MEDIDA	Registros.
TIPO DE INDICADOR	Conteo.
PERIODICIDAD	Mensual.
FÓRMULA DE CÁLCULO	Conteo de cada uno de los incidentes presentados a nivel de registros del sistema.
NOTAS	El resultado de la información podrá ser consultado por mes, trimestre y año.

CÓDIGO	7
NOMBRE DEL INDICADOR	Calidad de la información (Vacios).
INDICADOR	Porcentaje de la cantidad de registros que no poseen información sobre una variable.
EJE DE VALORACIÓN	Eficacia.
ÁMBITO	Operativo.
DESCRIPCIÓN	Este Indicador busca evidenciar el porcentaje de registros que no poseen ninguna información.
UNIDAD DE MEDIDA	Porcentaje.
TIPO DE INDICADOR	Conteo.
PERIODICIDAD	Mensual.
FÓRMULA DE CÁLCULO	Cantidad de registros vacíos del campo / cantidad de registros * 100.
NOTAS	El resultado de la información podrá ser consultado por mes, trimestre y año.

CÓDIGO	8
NOMBRE DEL INDICADOR	Calidad de la información (Validez).
INDICADOR	Porcentaje de la cantidad de registros que no corresponden a la información de la variable.
EJE DE VALORACIÓN	Eficacia.
ÁMBITO	Operativo.

DESCRIPCIÓN	Este Indicador busca evidenciar el porcentaje de registros cuya información no corresponde al tipo de dato o información que se recolecta en la variable.
UNIDAD DE MEDIDA	Porcentaje.
TIPO DE INDICADOR	Conteo.
PERIODICIDAD	Mensual.
FÓRMULA DE CÁLCULO	Cantidad de registros erróneos del campo / cantidad de registros * 100.
NOTAS	El resultado de la información podrá ser consultado por mes, trimestre y año.

CÓDIGO	9
NOMBRE DEL INDICADOR	Satisfacción de los funcionarios y ciudadanía
INDICADOR	Cantidad de incidentes reportados a través de la mesa de ayuda relacionados con el sistema de la Maestra de Beneficiarios.
EJE DE VALORACIÓN	Eficacia.
ÁMBITO	Operativo.
DESCRIPCIÓN	Este Indicador busca evidenciar la cantidad de novedades que se registran por parte de los usuarios y de la ciudadanía en general en el funcionamiento del sistema de la Maestra de Beneficiarios.
UNIDAD DE MEDIDA	Incidentes.
TIPO DE INDICADOR	Conteo.
PERIODICIDAD	Diaria.
FÓRMULA DE CÁLCULO	Sumatoria de los incidentes registrados por los funcionarios o la ciudadanía.
NOTAS	El resultado de la información podrá ser consultado por mes, trimestre y año.

6. ANÁLISIS FINANCIERO

COSTOS DIRECTOS			
RECURSO	SEPTIEMBRE	OCTUBRE	VALOR TOTAL
Estudiante 1	150.000	150.000	300.000

Estudiante 2	150.000	150.000	300.000
Total	300.000	300.000	600.000
Total General	600.000		

Tabla 8 Fuente: Investigación propia

COSTOS INDIRECTOS			
RECURSO	SEPTIEMBRE	OCTUBRE	VALOR TOTAL
Transportes	20.000	30.000	50.000
Reuniones	10.000	11.000	21.000
Papelería	10.000	30.000	40.000
Internet Móvil	30.000	30.000	60.000
Energía	15.000	15.000	30.000
Gastos Administrativos	40.000	40.000	80.000
Total	125.000	156.000	281.000
Total General	281.000		

Tabla 9 Fuente: Investigación propia

7. CONCLUSIONES

La ausencia en la asignación de responsables de cada uno de los sistemas de información (La maestra de beneficiarios, Cronos, entre otros sistemas), ha permitido que los procesos en los cuales se involucra algún tratamiento

de información sean administrados de manera desorganizada y subjetiva provocando que exista diferentes consensos y falta de alineación en el uso de algunas variables en el sistema. Como se propone en el gobierno de información, es necesario que cada sistema de información (No sólo la maestra de beneficiarios) y la entidad en general defina responsables y jerarquías para cada uno y a su vez, el Comité se empodere de sus funciones con el fin de velar por el buen uso de la información cumpliendo con los criterios de seguridad de la información.

La definición de políticas, principios y lineamientos sobre el funcionamiento de la Maestra de Beneficiarios es un gran avance en la propuesta de definición de una política marco que cobije de manera integral todos los sistemas de información y éste a su vez se pueda empalmar con el sistema Integral de Gestión.

Al llevar a cabo cada uno de los procedimientos recomendados en el Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea, la entidad podrá certificarse de una manera más ágil y sencilla en la norma técnica ISO/IEC 27001 debido a que el Modelo se encuentra alineado a esta norma técnica lo cual genera el ahorro de algunos pasos en la ejecución del mismo.

En la percepción de los usuarios de la Maestra de Beneficiarios, el sistema es confiable en los datos que arroja desde los reportes disponibles, sin embargo, es evidente que un bajo porcentaje de ellos conoce los diferentes procedimientos y protocolos existentes por lo que se recomienda crear una campaña que impulse el aprestamiento y ejecución de cada uno de ellos.

Para el progreso de la entidad en el funcionamiento de la Maestra de Beneficiarios y en general para la gestión de la seguridad de la información, es indispensable que la entidad aumente de manera paulatina la cantidad de funcionarios que trabajen en el tema con el fin de responder apropiadamente a los requisitos y retos plasmados en el Modelo de Seguridad de la Información; éste es un tema importante para la organización a fin de cumplir con los objetivos propuestos por la Estrategia de Gobierno en Línea 2.0.

El sistema de la Maestra de Beneficiarios es una potente herramienta que contiene un amplio espectro de variables que pueden ser útiles para el análisis de la población atendida por la entidad pero, debido a la falta de criterios, políticas, lineamientos y principios en la carga de las variables de información; muchos programas han optado por reportar exclusivamente los datos básicos de la población haciendo que el sistema sólo sea explotado en un mínimo. La implementación del principio, política y lineamiento de la Maestra de Beneficiarios permitirá a los funcionarios tener una idea clara de qué hacer en el momento que se presenten discusiones e identificar la posición que deben adoptar cuando una decisión sea tomada.

Los indicadores de gestión de la Maestra de Beneficiarios son vitales para analizar el avance o retroceso en cada uno de los ejes de valoración. A estos indicadores se les debe realizar seguimiento de acuerdo a la ficha técnica contenida en cada indicador; se debe ser muy estricto en el análisis de los resultados entregados para no sembrar falsas expectativas y generar alertas tempranas que permitan tomar acciones para que estas apoyen en la reducción de la brecha y avance en el proyecto.

El análisis de los indicadores debe ser consultado desde un tablero de comando el cual debe permitir su análisis de acuerdo al Eje de Valoración existente, el ámbito en el cual está creado el indicador, el nombre del indicador y el resultado arrojado de acuerdo a los criterios seleccionados por el funcionario encargado de dicha función.

8. BIBLIOGRAFÍA

Administración Electrónica. (20 de Junio de 2006). *Magerit - Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I.*

Recuperado el 2015 de Octubre de 10, de http://administracionelectronica.gob.es/pae_Home#.VXMsrdJ_P_g

Departamento Administrativo de la Función Pública. (4 de Noviembre de 2011). Decreto N° 4155. *Decreto N° 4155 Por el cual se transforma la Agencia Presidencial para la Acción Social y la Cooperación Internacional, Acción Social, en Departamento Administrativo para la Prosperidad Social.* Bogotá, D.C., Colombia.

Departamento Administrativo para la Properidad Social - DPS. (1 de Julio de 2014). *Manual de Funciones y Competencias Parte 1.* Obtenido de http://www.dps.gov.co/ent/hum/SiteAssets/Paginas/manual_funciones/Manual_de_Funciones_y_Competencias_-_DPS_parte_1.pdf

Departamento Administrativo para la Prosperidad Social - DPS. (1 de Julio de 2014). *Manual de Funciones y Competencias Parte 2.* Obtenido de http://www.dps.gov.co/ent/hum/SiteAssets/Paginas/manual_funciones/Manual_de_Funciones_y_Competencias_-_DPS_parte_2.pdf

ISO. (2009). *ISO/IEC 19796-1:2005 ITLET Quality management, assurance and metrics, Part 1: General approach.* International Organization for Standardization.

Ministerio de Tecnologías de la Información y las Comunicaciones. (5 de Mayo de 2008). *Gobierno en línea 3.0.* Recuperado el 9 de Octubre de 2015, de https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0CCsQFjACahUKEwiXuuXow8DIAhUFqx4KHa7hAlc&url=http%3A%2F%2Fprograma.gobiernoenlinea.gov.co%2Fapc-aa-files%2Fe5203d1f18ecfc98d25cb0816b455615%2Fmanual3.1.pdf&usg=AFQjCNGh5

Ministerio de Tecnologías de la Información y las Comunicaciones. (Diciembre de 2011). Recuperado el 11 de Octubre de 2015, de LINEAMIENTOS PARA LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN 2.0: http://programa.gobiernoenlinea.gov.co/apc-aa-files/da4567033d075590cd3050598756222c/GEL308_IPE_Lineamientos_Seguridad.pdf

Organización Internacional de Estándares. (2005). Términos y definiciones. En ISO/IEC, *ISO/IEC 27001 Tecnología de la Información - Técnicas de Seguridad - Sistemas de gestión de la seguridad de la información - Requerimientos* (págs. 9-12).

Universidad Pedagógica y Tecnológica de Colombia. (20 de Noviembre de 2013). *Biblioteca de Documentos*. Obtenido de http://aplica.uptc.edu.co/Procesos/Documentos/Forms/AllItems.aspx

9. ANEXOS

- Anexo 1. Análisis y Evaluación de Riesgos
- Anexo 2. Cronograma