PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL ÁREA METROPOLITANA DE BUCARAMANGA

Bucaramanga 21 de diciembre de 2018

CONTENIDO

1. Introducción……..……3
2. Objetivo General……..……..…4
2.1 Objetivo Especifico……..……...4
3. Programa estratégico……..……4
4. Objetivo del plan……4
5. Justificación……5
6. Alcance del plan……6
7. Marco de referencia……...7
8. Definiciones ……8
9. Documentos referencia……..……11
10. Normatividad ……..……11
11. Plan general de seguridad de la información……..……16
12. Metodología para la implementación del proyecto……..……17
13. Ejemplo de implantación del ciclo PDCA……..……18
14. Metas……..……19
15. Fase etapa previa a la implementación……..……..……19
16. Directrices, fases y lineamientos a seguir para la implementación del modelo de seguridad y privacidad de la información……20
17. Modelo de madurez……22
18. Tabla de modelo de madurez……...23
19. Características de control de objetivos……24
20. Descripción del plan……..25

1. INTRODUCCIÓN

El Área Metropolitana de Bucaramanga AMB como entidad Pública busca afrontar los diferentes retos con una infraestructura moderna, robusta y segura. Que sea competitiva en el nuevo mundo digital, que avanza día a día.

Conscientes de los grandes desafíos que existen en la realidad en temas de seguridad de la información y con los grandes ataques cibernéticos de los últimos años, se hace imperante la realización e implementación de un plan de acción con el fin de prevenir y mitigar cualquier tipo de incidente que pueda afectar a la entidad.

Con ello se busca promover la implementación y ejecución de buena prácticas de seguridad y privacidad de la información, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información del Ministerio de las TIC.

2. OBJETIVO GENERAL

Convertir al Área Metropolitana de Bucaramanga AMB en una entidad moderna, segura y transparente para lo cual se realizarán trabajos de planificación, orientación y desarrollo de políticas que nos lleven a contar con disponibilidad, integridad y confidencialidad de todos los activos de información con los que cuenta la entidad.

2.1. OBJETIVOS ESPECIFICOS

- Dar lineamientos para la implementación del modelo de seguridad y privacidad de la información.
- Promover el uso de mejores prácticas de seguridad de la información
- Contribuir a mejorar los procesos de intercambio de información publica
- Implementar las mejores prácticas para la construcción de una política de privacidad respetuosa de los datos personales.
- Optimizar la gestión de la información al interior de la entidad
- Crear conciencia en todos los funcionarios y contratistas de la importancia del cumplimiento de unas políticas de seguridad de la información.

3. PROGRAMA ESTRATEGICO

Convertir al Área Metropolitana de Bucaramanga AMB en una entidad moderna, segura y transparente.

Mejora continua de la infraestructura TI e implementación de las Políticas de Seguridad y Privacidad de la información.

4. OBJETIVO DEL PLAN

Identificar y dar prioridad a todas las actividades contempladas en el modelo de seguridad y privacidad de la información y que se realizaran en la vigencia 2018 – 2020, alineados con la Política de Gobierno Digital (Estrategia de MINTIC)

5. JUSTIFICACIÓN

En el mundo moderno para toda organización ha venido cobrando mayor importancia el valor que se le asigna a la información. Esta representa hoy en día uno de los pilares fundamentales en la estructura de cualquier organización. Para el área metropolitana de Bucaramanga no es ajena esta realidad; por lo tanto, todo lo referente con la seguridad en la información es una de las preocupaciones más grandes que puede llegar a tener la entidad, ya que se refiere a garantizar la calidad, disponibilidad, veracidad y confidencialidad de su activo más valioso: la información. La información es un activo que, como otros activos comerciales importantes, es vital para el negocio de una organización y en consecuencia se requiere que sea protegido adecuadamente. Esto es especialmente importante en el sector de las entidades estatales que cada vez más busca tener a los ciudadanos acceso a la información de forma inmediata y minimizar la tramitología haciendo que la gran parte de los tramites se puedan hacer en línea.

Como resultado de esta creciente interconectividad, el que denominamos como uno de los más preciados activos; la información, ahora está expuesta a un sin número de amenazas y vulnerabilidades. Hoy día las organizaciones que manejen sistemas de información han visto la necesidad del aseguramiento de la información, generando políticas y controles, buscando garantizar la estabilidad y confiabilidad de la información.

Es importante aclarar que este proyecto está encaminado en establecer unas bases que permitan establecer los lineamientos que se aplicaran poco a poco buscando avanzar en la consecución del objetivo principal que es el establecimiento de un Plan de Seguridad Informática que parta desde las copias de seguridad, su protección, integralidad, restricción de acceso y demás elementos a tener en cuenta.

Los principales beneficiarios son en primera medida la Alta Dirección, ya que se ofrecerá disponibilidad y veracidad en la información que se usa para la toma de decisiones. Por otra parte, los usuarios finales del sistema de información que alimentan y requieren de agilidad y seguridad al momento de ingresar información que puede o no ser pública, a través de los servicios tecnológicos de la entidad.

6. ALCANCE DEL PLAN

El alcance del presente plan comprende todas las actividades que permitan dar cumplimiento al 100% de los componentes definidos en el Modelo de Seguridad y Privacidad de la Información acompañado de la implementación de controles establecidos por el estándar ISO 27001:2013 y la normatividad vigente aplicable.

Por tal razón, los funcionarios, contratistas y terceros que interactúen con los activos de información de la entidad, deberán tener conocimiento y cumplir con las políticas, procesos y procedimientos que hacen parte del SGSI, en donde por sobre todo se protejan los principios de confidencialidad, integridad y disponibilidad de la información.

7. MARCO DE REFERENCIA

Durante la última década las entidades públicas han intensificado sus esfuerzos en realizar acciones cuyo fin sea el mejorar la eficiencia y efectividad de su gestión tomando como punto de partida la reducción de costos tanto operativos como administrativos en busca de un mejor aprovechamiento de sus recursos.

para lograr ese objetivo se realizan tareas como: optimizar sus procesos misionales, evaluar y actualizar los procesos y políticas de adquisición en la entidad, automatización de procesos manuales, hacer más agiles los procesos de su sistema integrado de gestión, entre otros. Esto se realiza a partir de los lineamientos de la Política **Gobierno en Línea** establecidos por el **Gobierno Nacional** por medio del **Ministerio de las TICS** y lo que hoy se denomina **Gobierno Digital**. Dichos lineamientos establecen los componentes normativos sobre los cuales debe enmarcarse la ejecución de todos estos objetivos.

Teniendo como fin el mejoramiento de estos procesos se hace indispensable utilizar las tecnologías de información de acuerdo a las necesidades de la entidad, tomando como base la misión y la visión acompañadas de los planes estratégicos que la alta dirección quiere implementar en la Entidad.

El Plan Estratégico de Tecnología de Información y comunicación (PETIC) hace referencia al conjunto de políticas tecnológicas e informáticas que la Oficina de Sistemas de entidad proyecte y lidere las cuales tendrán que estar encaminadas al cumplimiento de la misión, visión y planes estratégicos que tenga el área metropolitana de Bucaramanga como entidad. Si tenemos en cuenta que el objetivo principal de las oficinas de los tics es el mejoramiento y optimización de los procesos de las áreas misionales por tal razón el área de las tecnologías debe ir siempre de la mano de la misión de cada organización y trabajar simultánea y transversalmente para el cumplimiento de las metas propuestas. Dentro de estas podemos evidenciar las de mayor preocupación como lo son dispositivos **NAS** para el almacenamiento de copias de seguridad, definir políticas institucionales de seguridad de la información para lo cual se tomará como punto de partida el documento informe sobre seguridad informática que realizo la empresa INTEGRASOF buscando que la entidad este a nivel en el cumplimiento de las normativas para las entidades del sector público.

8. DEFINICIONES

MPSI	Modelo de Seguridad y Privacidad de la Información
SGSI	Sistema de Gestión de Seguridad de la información

***Activo:** cualquier cosa que tiene valor para la organización. [NTC 5411-1:2006]

***Información:** La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente.

***Riesgo:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones. (ISO Guía 73:2002)

***Riesgo residual:** nivel restante de riesgo después del tratamiento del riesgo. [Guía ISO/IEC 73:2002]

***Aceptación del riesgo:** decisión de asumir un riesgo. [Guía ISO/IEC 73:2002]

***Análisis de riesgo:** uso sistemático de la información para identificar las fuentes y estimar el riesgo. [Guía ISO/IEC 73:2002]

***Gestión del riesgo:** actividades coordinadas para dirigir y controlar una organización en relación con el riesgo. [Guía ISO/IEC 73:2002]

***Evaluación del riesgo:** proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo. [Guía ISO/IEC 73:2002]

***Amenaza:** causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.

***Amenaza informática**: la aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado (Ministerio de Defensa de Colombia).

***Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. [NTC 5411-1:2006]

***Declaración de aplicabilidad:** documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la organización. NOTA Los objetivos de control y los controles se basan en los resultados y conclusiones de los procesos de valoración y tratamiento de riesgos, requisitos legales o reglamentarios,

obligaciones contractuales y los requisitos del negocio de la organización en cuanto a la seguridad de la información.

***Disponibilidad:** propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [NTC 5411-1:2006] NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001

***Evento de seguridad de la información**: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. [ISO/IEC TR 18044:2004]

***Incidente de seguridad de la información:** un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. [ISO/IEC TR 18044:2004]

***Integridad:** propiedad de salvaguardar la exactitud y estado completo de los activos. [NTC 5411-1:2006]

Integridad: la propiedad de salvaguardar la exactitud y complejidad de la información. • Inventario de activos: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organizac

***Seguridad de la información:** preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad. [NTC-ISO/IEC 17799:2006]

***Sistema de gestión de la seguridad de la información SGSI:** parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001 4 NOTA El sistema de gestión incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.

***Habeas data:** derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

***Datos abiertos:** son datos primarios o sin procesar puestos a disposición de cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

*__Datos biométricos:__ parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (huella digital o voz).

*__Datos personales sensibles:__ se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

*__Dato privado:__ es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. *__Dato público:__ es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

*__Dato semiprivado:__ es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

__*Titular de la información:__ es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.

*__Responsable del tratamiento__: persona natural o jurídica. Pública o privada. Que por sí misma o en asocio con otros. Decida sobre la base de datos y/o el Tratamiento de los datos.

__*Tratamiento del riesgo:__ proceso de selección e implementación de medidas para modificar el riesgo. [Guía ISO/IEC 73:2002] NOTA En la presente norma el término “control” se usa como sinónimo de “medida”.

__*Valoración del riesgo:__ proceso global de análisis y evaluación del riesgo. [Guía ISO/IEC 73:2002]

*__Trazabilidad:__ cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

*__Vulnerabilidad:__ debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000.es, 2012).

9. DOCUMENTOS DE REFERENCIA

MPSI Modelo de Seguridad y Privacidad de la Información del Ministerios de las TIC

ISO 27001:2013 Norma internacional emitida por la Organización Internacional de Normalización (ISO) sobre gestión de seguridad de la información.

ISO 22301:2012 Norma internacional emitida por la Organización Internacional de Normalización (ISO) sobre gestión de continuidad del negocio

LEY 1581:2012 Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 1008 de 2018 Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

Decreto 1078 de 2015 Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones

10. NORMATIVIDAD

LEGISLACIÓN	***TEMA***	***REFERENCIA***
En el Decreto Nacional 2573 de 2014	Estrategia de Gobierno en Línea de la República de Colombia	El Decreto establece los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones
LEY 1712 DE 2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública	Hace referencia, principalmente, al artículo 74 de la Constitución Nacional en el cual se establece que “Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley”. El objeto de la ley es “regular el derecho de acceso a la información pública, los procedimientos para el

		ejercicio y garantía del derecho y las excepciones a la publicidad de información"
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones	El decreto tiene por objeto regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información, y constituye el marco general de la protección del ejercicio del derecho de acceso a la información pública en Colombia.
Decreto 2609 de 2012 (hoy incorporado al Decreto Único 1080 de 2015	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado	Sobre la Gestión de Documentos indica que las normas del decreto se aplicarán a cualquier tipo de información producida y/o recibida por las entidades públicas, sus dependencias y servidores públicos, y en general por cualquier persona que desarrolle actividades inherentes a la función de dicha entidad o que hayan sido delegados por esta, independientemente del soporte y medio de registro (análogo o digital) en que se produzcan, y que se conservan en: a) Documentos de Administración de documentos. b) Archivos institucionales (físicos y electrónicos). c) Sistemas de Información Corporativos. d) Sistemas de Trabajo Colaborativo. e) Sistemas de en la nube. Archivo (físicos y electrónicos). f) Sistemas de Mensajería Electrónica. g) Portales, Intranet y Extranet. h) Sistemas de Bases de Datos. i)Disco duros, servidores, discos o medios portables, cintas o medios de video y audio (análogo o digital), etc.

		j) Cintas y medios de soporte (back up o contingencia). k) Uso de tecnologías
Decreto 886 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, en lo relativo al Registro Nacional de bases de datos.	Serán objeto de inscripción en el Registro Nacional de Bases de Datos, "las bases de datos que contengan datos personales cuyo Tratamiento automatizado o manual se realice por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él, en este último caso, siempre que al Responsable del Tratamiento o al Encargado del Tratamiento le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales. Lo anterior sin perjuicio de las excepciones previstas en el artículo 2° de la Ley 1581 de 2012".
Ley 1581/12	Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales	Hace referencia, en particular, al artículo 15 de la Constitución Nacional, según el cual "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. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución…". La ley tiene por

		objeto "desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma"
Ley 1273/09	Por medio de la cual se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones	"De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos".
CONPES 3701 de 2011	Lineamientos de política para ciberseguridad y Ciberdefensa	Busca generar lineamientos de política en ciberseguridad y ciberdefensa encaminados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.
Ley 1266/08	Por la cual se dictan 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	Se regula el manejo de la información para "todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada".

	proveniente de terceros países	
Ley 594/00	Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones	La presente ley "tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado". Y "comprende a la administración pública en sus diferentes niveles, las entidades privadas que cumplen funciones públicas y los demás organismos regulados por la presente ley".
La Ley 850/03 establece en su artículo 9º	Principio de Transparencia	"A fin de garantizar el ejercicio de los derechos, deberes, instrumentos y procedimientos consagrados en esta ley, la gestión del Estado y de las veedurías deberán asegurar el libre acceso de todas las personas a la información y documentación relativa a las actividades de interés colectivo de conformidad con lo dispuesto en esta ley y en las normas vigentes sobre la materia"

11. PLAN GENERAL DE SEGURIDAD DE LA INFORMACION

Para el Área Metropolitana de Bucaramanga El Plan de seguridad es un documento de suma importancia en el cual se describe en detalle cual es el compromiso de la entidad y hasta donde desea llegar en aras de tener los más altos estándares en seguridad informática.

Con el cumplimiento de los objetivos y el cronograma establecido en este Plan se espera llegar a los más bajos niveles de riesgo que signifiquen perdida o daños; producto de usuarios malintencionados, ciberataques, amenazas y demás tipo de riesgos cuyo objetivo sea el desestabilizar los procesos y el óptimo funcionamiento de la entidad. en donde los procesos informáticos son en gran medida la base para el cumplimiento de sus horizontes misionales.

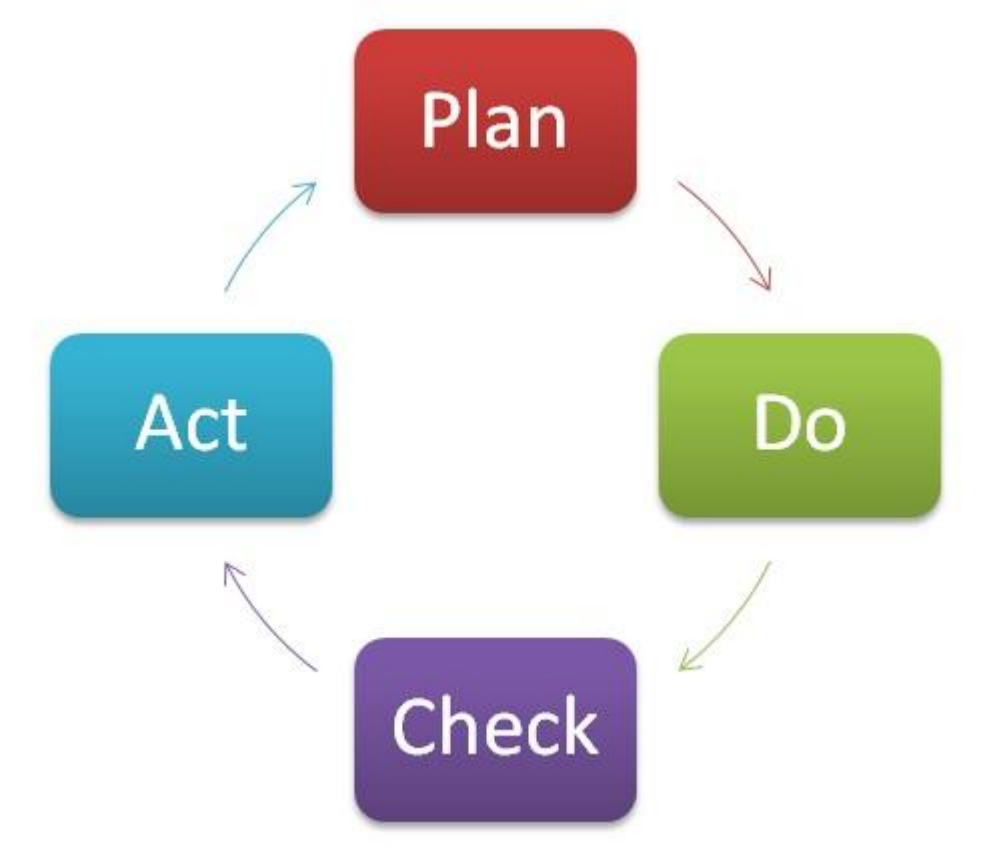
El área metropolitana de Bucaramanga y su oficina de tics deben establecer protocolos de seguridad que estén encaminados a proteger su mayor activo “la información” y blindar sus características de integridad, disponibilidad y confidencialidad, Haciendo uso de prácticas y políticas institucionales que tengan como fin el cumplimiento de sus planes estratégicos sin dejar de lado la normatividad que rige en la actualidad.

Es así como el área metropolitana de Bucaramanga trabajara arduamente velando por que se dé un correcto y adecuado manejo en la gestión del riesgo, implementación de nuevas prácticas en el buen uso de los activos de información y la mejora continua de los niveles de competencia del personal con el que cuenta la oficina de recurso humano.

El éxito de estos planes de seguridad depende en gran medida del compromiso depositado por los directivos de la entidad y una participación activa y consiente de parte de los funcionarios, contratistas y terceros, los cuales tendrán que entrelazar y compartir esfuerzos para lograr los objetivos establecidos aquí siguiendo las directrices dadas como políticas de seguridad de la información y una continua autoevaluación que permita el mejoramiento de los procesos y procedimientos que se aplican como respuesta ante los incidentes de seguridad informática

METODOLOGÍA PARA LA IMPLEMENTACION DEL PROYECTO

Para la implementación del proyecto el área metropolitana de Bucaramanga usara el modelo ciclo **PHVA** como metodología del modelo de mejora continua. El phva es el sistema mas usado en el mundo para el desarrollo de dichos modelos.



PDCA Cycle: Plan, Do, Check, Act.
Ciclo PHVA: Planificar, Hacer, Verificar, Actuar.

En esta metodología se utilizan cuatro pasos o procesos fundamentales que deben seguirse al pie de la letra para así poder alcanzar mejoras continuas en los procesos de calidad, esas mejoras nos deberán representar: (disminución de fallos, aumento de la eficacia y eficiencia, solución de problemas, previsión y eliminación de riesgos potenciales…) dicho proceso debe realizarse de forma cíclica de tal manera que tan pronto se cumpla un ciclo este vuelva a repetirse buscando mejorar en cada ciclo.

1. **Planificar (Plan):** Se revisarán los procesos que la organización determine pueden ser optimizados y se determinara los objetivos a cumplir. Para poder establecer esos procesos a mejorar se podrán conformar grupos de trabajo, indagar sobre las percepciones de los trabajadores, y tratar de modernizar o actualizar las tecnologías que utilice la entidad en la actualidad.

2. **Hacer (Do):** En esta etapa se realizan los cambios a los procesos propuestos estos cambios deben realizarse en un ambiente de pruebas hasta estar seguros del correcto funcionamiento y así poder ser aplicados en toda la organización.

3. **Controlar o Verificar (Check):** Luego de ser realizados los cambios que buscan optimizar los procesos se dará un tiempo para que se realicen las pruebas necesarias que permitan establecer si dichos cambios en efecto produjeron un cambio positivo en aras del cumplimiento de las metas establecidas.

4. **Actuar (Act):** Tan pronto se concluya el tiempo destinado para hacer pruebas se realiza un análisis pormenorizado de los resultados obtenidos y se establecen unas tablas comparativas del antes y el después de la implementación de los cambios en el ambiente de pruebas. Si los resultados fueron positivos se debe establecer la forma de implementarlos de manera definitiva en el menor tiempo posible causando el menor traumatismo, por el contrario, si los resultados no son los esperados se debe considerar desistir de la idea o buscar mejorarlos e iniciar nuevamente el ciclo en busca de la mejora continua.

EJEMPLO DE IMPLANTACIÓN DEL CICLO PHVA

En Colombia el departamento de Santander es altamente reconocido por el desarrollo que tiene la industria del calzado; es así como una de estas grandes fábricas en busca del mejoramiento de sus procesos de producción decide aplicar un sistema de mejora continuo y para ello establecen basarse en el ciclo PHVA; la aplicación de dicho sistema se da de la siguiente manera:

1- se realiza un análisis para evaluar las posibles mejoras bien sea por que han sido detectadas fallas o por que los empleados han propuestos cambios para mejora de los procesos de producción o porque en el mercado están

disponibles nuevas máquinas que mejorarían los tiempos, las cantidades y los costos en los procesos de producción.

2- Se evalúan las mejoras propuestas y el impacto que estas generarían en la fábrica, se escogen las que se consideran funcionaran mejor y se decide implantarlas en un ambiente de pruebas.

3- Después de realizadas una serie de pruebas con los cambios propuestos se verifica que los mismos hallan funcionado correctamente obteniendo los resultados esperados; si esos resultados no son los esperados se modificara lo propuesto en busca de tener un cambio satisfactorio según lo proyectado.
4- Para finalizar si los resultados obtenidos son los esperados serán implementados de forma definitiva en toda la línea de producción de la fábrica y una vez finalizado este proceso de mejoras el área de producción será más eficiente, productivo y rentable. Aun cuando los resultados hayan sido satisfactorios este ciclo debe aplicarse nuevamente buscando siempre la excelencia y la optimización continua.

14. METAS

- 70% de avance en la implementación del MSPI

15. FASE- ETAPA PREVIA A LA IMPLEMENTACIÓN

Nos encontramos en la ETAPA PREVIA A LA IMPLEMENTACIÓN:

- Se realizó diagnóstico para conocer el estado actual del AMB
- Se identificó el nivel de madurez Nivel 1 Nivel inicial
- Se da inicio al proceso de levantamiento de información

16. DIRECTRICES FASES Y LINEAMIENTOS A SEGUIR PARA LA IMPLEMENTACION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

PROCESO DE ALINEACION DEL SGSI Y EL MODELO PHVA	
DIRECTRIZ 1: IDENTIFICACION DEL MODELO DE MADUREZ SI	
FASE 1 PREPARACION	*Planeación de jornadas de capacitación. *Creación del equipo que liderara el proyecto.
FASE 2. Evaluación del estado actual y determinar falencias.	*Formular y realizar sondeos sobre percepción de niveles de seguridad. *Establecer en nivel de madurez en que se encuentra la entidad realizando una autoevaluación sobre nuestros sistemas de seguridad. *Definición de Brechas: -Analizar la estructura organizacional de la entidad. -Revisión por niveles de madurez de acuerdo a los requisitos del manual de GEL. -Revisión de controles de SI (Existentes y ausentes). -Definir el estado actual de SI de la entidad. -Definición del plan o cronograma a seguir para disminuir la brecha y alinearse con el nivel de madurez adecuado.
FASE 3. Alineación con el Sistema de Gestión de Seguridad de la Información SGSI.	*Ejecución del Programa para la reducción de la brecha.

PLANEAR	
DIRECTRIZ 2: LLEVAR A LA ENTIDAD A UN NIVEL DE MADUREZ INICIAL EN SEGURIDAD.	
FASE 1. Actividades Lineamientos Nivel Inicial	*Obtener soporte de la Dirección de la entidad. *Identificar legislación y normatividad aplicable. *Definir el alcance del SGSI “SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN”. *Definir la Política de la Seguridad de la información. *Realizar el análisis dedel riesgo: -Definir la aproximación para la Gestión del Riesgo. -Realizar la identificación de Activos. -Identificar los riesgos. -Analizar el riesgo en contexto de los objetivos de la entidad y partes interesadas. *Selección de controles. *Plan de Tratamiento del riesgo. *Generar el DDA - Declaración de aplicabilidad.

HACER	
DIRECTRIZ 3: LLEVAR A LA ENTIDAD A UN NIVEL DE MADUREZ BÁSICO EN SEGURIDAD.	
FASE 1. Actividades Lineamientos Nivel Basico.	*Implementar el plan de tratamiento del riesgo. *Documentar los controles del SGSI: -Definir métricas y medidas para medir el desempeño del SGSI. *Implementar políticas y controles de seguridad de la fase de planeación. *Implementar los planes de concientización y entrenamiento. *Establecer y gestionar la operación del SGSI y sus recursos. *Implementar la infraestructura de respuesta a incidentes.

VERIFICAR	
DIRECTRIZ 4: LLEVAR A LA ENTIDAD A UN NIVEL DE MADUREZ AVANZADO EN SEGURIDAD.	
FASE 1. Actividades Lineamientos Nivel Avanzado.	*Ejecutar plan operacional. *Revisiones regulares de eficacia: -Monitorear y revisar políticas, estándares, procedimientos y prácticas. -Revisar la eficacia de las operaciones de seguridad usando métricas y mediciones. *Revisar el nivel del riesgo residual. *Realizar Auditorías internas. *Realizar Auditorías externas. *Revisión de la dirección del SGSI. *Registro del impacto en el SGSI.

ACTUAR	
DIRECTRIZ 5: LLEVAR A LA ENTIDAD A UN NIVEL DE MADUREZ DE MEJORAMIENTO PERMANENTE EN SEGURIDAD.	
FASE 1. Actividades Lineamientos Nivel Mejoramiento Permanente.	*Implementar las mejoras identificadas y aprobadas al SGSI en un nuevo ciclo. *Tomar medidas preventivas y correctivas. *Aplicar las lecciones aprendidas. *Comunicar los resultados. *Proceso continuo y Gestión auto sostenible del modelo de las entidades: -Revisión de Política de Seguridad. -Verificación del alcance del conjunto de políticas en la entidad. -Revisión de los activos de información de la entidad. -Revisión del riesgo residual. -Recopilación y análisis de los indicadores del modelo. -Análisis de estadísticas de incidentes de seguridad de la información en entidades del Estado. -Implementación de los ajustes.

17. MODELO DE MADUREZ

Modelo de Madurez Nivel 2. INICIAL

El AMB reconoce la necesidad de implementar el MSPI, para definir las políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre la seguridad de la información que presenta actualmente.

Se han identificado mediante un diagnóstico de seguridad informática y privacidad de la información las debilidades presentadas por el AMB

Actualmente los incidentes de seguridad se tratan de forma reactiva.

Con posterioridad a la revisión en el cumplimiento de las directrices y lineamientos, se debe realizar una verificación detallada del nivel de madurez del CGSI “Componente de Gestión de Seguridad de la Información”

Dicha revisión deberá llevarse a cabo siguiendo los parámetros establecidos por el MINTIC como se describe en el siguiente cuadro sobre el modelo de madurez:

18. TABLA MODELO DE MADUREZ

(según modelo de seguridad y privacidad de la información del MINTIC vive digital)

Tabla 6 – Características de los Niveles de Madurez

Nivel	Descripción
Inexistente	• Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo no están alineados a un Modelo de Seguridad. • No se reconoce la información como un activo importante para su misión y objetivos estratégicos. • No se tiene conciencia de la importancia de la seguridad de la información en la entidad.
Inicial	• Se han identificado las debilidades en la seguridad de la información. • Los incidentes de seguridad de la información se tratan de forma reactiva. • Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.
Repetible	• Se identifican en forma general los activos de información. • Se clasifican los activos de información. • Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información. • Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión. • La entidad cuenta con un plan de diagnóstico para IPv6.
Definido	• La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información. • La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información. • La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas. • La Entidad tiene procedimientos formales de seguridad de la Información • La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información. • La Entidad ha realizado un inventario de activos de información aplicando una metodología. • La Entidad trata riesgos de seguridad de la información a través de una metodología. • Se implementa el plan de tratamiento de riesgos. • La entidad cuenta con un plan de transición de IPv4 a IPv6.
Administrado	• Se revisa y monitorea periódicamente los activos de información de la Entidad. • Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información. • Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro. • La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6.
Optimizado	• En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización. • Se utilizan indicadores de efectividad para establecer si la entidad encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales. • La entidad genera tráfico en IPv6.

19. CARACTERISTICAS DE CONTROL DE OBJETIVOS.

Enseguida realizaremos un breve recuento de los aspectos que más tendremos en cuenta en nuestro proyecto y que hacen parte de la norma ISO/IEC 27001:2013, que ha sido definida por el Área Metropolitana de Bucaramanga como estándar para la implementación y mantenimiento del CGSI.

- **Gestión de Activos:**
Detalla los elementos de la Organización (servidores, PCs, medios magnéticos, información impresa, documentos, etc.), que deben ser considerados para establecer un mecanismo de seguridad que permita garantizar un nivel adecuado de protección.

- **Políticas de seguridad de la Información:**
Establece la necesidad de definir un conjunto de políticas aplicadas a todas las actividades relacionadas con la gestión de la seguridad de la información dentro de la Organización, con el propósito de proteger la misma contra las amenazas presentes en el entorno.

- **Seguridad de las operaciones:**
Define las políticas, procedimientos y responsabilidades para asegurar la correcta operación de las instalaciones de procesamiento de información.

- **Seguridad física y ambiental:**
Responde a la necesidad de proteger las áreas, los equipos y los controles generales. El objetivo principal es la prevención de accesos no autorizados a las instalaciones de la Organización, con especial atención a todos los sitios en los cuales se procesa información (centros de cómputo, PC de usuarios críticos, equipos de los proveedores de servicios, etc.), y áreas en las cuales se recibe o se almacena información (magnética o impresa) sensitiva (fax, áreas de envío y recepción de documentos, archivadores, etc.), minimizando riesgos por pérdidas de información, hurto, daño de equipos y evitando la interrupción de las actividades productivas.

- **Seguridad de las comunicaciones:**
Define las políticas y procedimientos para asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información.

- **Seguridad del Recurso Humano:**
Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y confidencialidad de la información que manejan.

-**Control de acceso:**
Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para protegerlos contra los abusos internos e intrusos externos. Asimismo, establece los diferentes tipos de accesos o privilegios a los recursos informáticos (sistema operativo, aplicaciones, correo electrónico, Internet, comunicaciones, conexiones remotas, etc.) que requiere cada empleado de la Organización y el personal externo que brinda servicios, en concordancia con sus responsabilidades.

- **Gestión de Incidentes de Seguridad:**
Establece la necesidad de desarrollar una metodología eficiente para la generación, monitoreo y seguimiento de eventos e incidentes de seguridad.

-**Cumplimiento:**
Imparte instrucciones a las organizaciones para que verifiquen si el cumplimiento con la norma técnica ISO/IEC 27002:2013, concuerda con otras leyes, reglamentos, normatividad y obligaciones contractuales o cualquier requerimiento de seguridad, tales como propiedad intelectual, auditorías, contrato de servicios, entre otros.

20. DESCRIPCIÓN DEL PLAN

ACTIVIDAD	TAREA A DESARROLLAR PARA EL PLAN	RESPONSABLE	FECHA INICIO	FECHA INICIALIZACIÓN
Diagnostico Riesgos de Seguridad de la información AMB	Realizar un Diagnóstico del estado actual	Ing. Fredy Varela ,	30/07/2018	15/11/2018
Actualizar el inventario básico de activos (software y hardware)	Actualizar el inventario actual de todos los activos de TIC de software y hardware	Ing. Fredy Varela,	10/01/2019	17/01/2019 SE ADJUNTA LA TABLA CON EL INVENTARIO
Crear y/o actualizar políticas relacionadas con el cumplimiento del Modelo de Seguridad y Privacidad de la Información	Elaborar y/o actualizar políticas según el modelo de Seguridad y Privacidad de la Información.	Ing. Fredy Varela	1/08/2018	29/03/2019 Fecha tentativa que nos permite realizar esta actividad en el primer trimestre
Crear y/o actualizar procedimientos	Elaborar los procedimientos	Ing. Fredy Varela	1/08/2018	Si no se siene la meta propuesta

para la clasificación de la información	para clasificar la información			seria el primer semestre de 2019 , Si ya se tiene se coloca fecha de finalización y se adjunta documento a carpeta de anexos
Implementar la Ley 1581:2012 sobre protección de datos personales	Implementar la política de y requisitos de le ley de protección de datos personales	Ing. Fredy Varela	FECHA INICIO CONTRATO	FECHA FINALIZACIÒN CONTRATO Anexar soportes resultado de dicho contrato a anexos del presente plan
Socialización políticas de Seguridad y Privacidad de la Información	Elaborar e implementar el cronograma de socialización de Políticas	Ing. Fredy Varela	2/01/2019	30/06/2019 esta debe ir posterior a la entrega del documento de las políticas con su correspondiente resolución.
Seguridad Recurso Humano.	Inducción y/o jornadas de capacitación y concientización sobre seguridad de la información	Ing. Fredy Varela Recursos Humanos	Durante todo el año 2019, ingreso del personal y jornadas de re inducción	Durante todo el año 2019, ingreso del personal y jornadas de re inducción
Elaboración del Manual de roles y responsabilidad	Elaborar para su posterior presentación ante la Dirección del AMB	Ing. Fredy Varela	15/10/2018	26/10/2018 Se anexa como documento soporte para plan de riesgos y plan se seguridad.
Implementar manual de Roles	Implementar el Manual de roles de la entidad		Primer semestre 2019	Primer semestre 2019
Presentación manual de Roles y responsabilidades	Presentación ante la Dirección de la entidad para aprobación	Ing. Fredy Varela	2/01/2019	29/03/2019 se propone esta fecha pero puede realizarse en el primer semestre de 2019

Clasificación de los riesgos hallados en el Diagnostico	Elaborar tabla de clasificación Según: Tipo, Amenaza y Origen	Ing. Fredy Varela	2/01/2019	29/03/2019 Fecha propuesta
Elaborar documento de registro de vulnerabilidades y controles existentes	Elaborar registro de las afectaciones recibidas y las acciones tomadas para su control	Ing. Fredy Varela	2/01/2019	31/12/2019 Fecha propuesta, pero se debe iniciar su registro desde el primer día de 2019
Listado de consecuencias de las afectaciones recibidas y de las posibles a recibir	Elaborar documento donde se registren las consecuencia recibidas	Ing. Fredy Varela	2/01/2019	29/03/2019 Fecha propuesta, pero se debe iniciar su registro desde el primer día de 2019
Evaluación del Riesgo	Documento de evaluación cualitativa del Riesgo	Ing. Fredy Varela	01/04/2019	30/05/2019 Fecha propuesta
Documentación acciones de Mitigación realizadas por la entidad	Registro de acciones de Mitigación de riesgos	Ing. Fredy Varela	2/01/2019	31/12/2019 Se debe diligenciar desde el primer día 2019 como soportes y registro de esta actividad
Implementación de Rack de Comunicaciones tipo gabinete para Servidores y equipos de telecomunicaciones	Instalar Rcks tipo gabinete donde se ubiquen los servidores y equipos de comunicaciones	Ing. Fredy Varela	1/04/2019	28/06/2019
Establecer zona de TICs, o Cuarto de Comunicaciones.	Establecer zona de TICs, donde se ubique los principales racks de comunicaciones y se tenga un control de acceso	Ing. Fredy Varela Dirección	2/01/2019	29/03/2019

Personal	Aumentar personal área de TICS según manual de roles con el fin de llevar a cabo el presente plan	Ing. Fredy Varela Dirección	Segundo semestre 2019	Segundo semestre 2019
Procedimiento de mantenimiento de equipos.	Documento donde se establece el procedimiento de mantenimiento y cronograma	Ing. Fredy Varela	Primer semestre 2019	Primer semestre 2019
Segmentación de Red	Segmentación de la red en VLANS	Ing. Fredy	Segundo semestre 2019	Segundo semestre 2019
Definición de Presupuesto	Definir Presupuesto de Ti para implementación del SGSi	Ing. Fredy Varela	2/01/2019	29/03/2019 Fecha propuesta

Elaboro: Sergio Andrés Lizarazo Quiroga
Ingeniero en Telecomunicaciones
Contratista SPI

William Oswaldo Barrera León
Ingeniero de Sistemas
Contratista SAF

Reviso: Fredy Neil Varela Lemus
Profesional Universitario AMB

Aprobó: