# **Plan de implementación para el Modelo de Seguridad y Privacidad de la Información**

**en la Secretaría Distrital de Planeación**

## **DIRECCIÓN DE SISTEMAS DE INFORMACIÓN**

## **ABRIL DE 2018**

**“Básicamente no existe una bala de plata para los problemas de seguridad que pueda tener una entidad. Una evaluación de seguridad si bien es cierto es útil como primera fase, no es efectiva en evaluaciones más profundas que requiera una entidad para mejorar sus niveles de seguridad en todas las áreas; esta es una razón de que la seguridad es un proceso, no un producto.”**

**Metodología Pruebas de Efectividad**. **MinTIC. Versión 1.0**

**INTRODUCCIÓN**

El Plan de implementación para el Modelo de Seguridad y Privacidad de la Información, MSPI, es la respuesta activa a la fase de planeación en la que se define el alcance, las políticas, las acciones y el apoyo de la dirección; la publicación, difusión y apropiación por parte de los responsables de los activos de información.

Con las acciones de implementación no solo se identifican y clasifican los activos (inventario de activos de información) sobre los cuales se aplican diferentes controles para preservar la confidencialidad, integridad y disponibilidad de la información, sino que se evalúan los riesgos, amenazas, vulnerabilidades, se establecen responsables de la seguridad y se hacen las primeras mediciones. Vienen luego los indicadores, la valoración de los resultados y la mejora continua.

Si bien la SDP presenta avances en la fase de implementación, el ciclo PHVA exige desarrollar estrategias concretas para su sostenibilidad, teniendo en cuenta factores externos como cambios en la normatividad, en las dinámicas de la organización, en la infraestructura tecnológica, en los servicios y naturalmente la disponibilidad de los recursos.

También se debe tener en cuenta acciones de mejora propuestas en las auditorías internas del Modelo de Seguridad y Privacidad de la Información de la SDP, lo que indica que la construcción de los principios de seguridad de la información tiene ya una trayectoria importante que se debe considerar y valorar.

1. **OBJETIVO**

El Objetivo principal del Plan de implementación para el Modelo de Seguridad y Privacidad de la Información es definir las acciones que debe asumir la SDP para preservar la integridad, confidencialidad y disponibilidad de la información; las prioridades de ejecución, los recursos necesarios para llevarlas a cabo y el seguimiento para verificar la eficacia del mismo.

Como resultado, la SDP debe contar con un proceso de seguridad que garantice la efectividad de los controles definidos para la custodia de los activos, que vele porque la información sea correcta y completa, esté siempre a disposición del cumplimiento de las metas de la institución, esté respaldada y sea utilizada sólo por aquellos que tienen autorización para hacerlo.

1. **ACTIVIDADES**
   1. **Asignación de Roles y Responsabilidades (2018)**

Está asociada con la definición de los actores responsables en su actuar y función de la seguridad de la información en la entidad de acuerdo con el documento **A-LE-009 ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN DE LA SDP**, cuya asignación no sólo generará las dinámicas propias de un proceso, sino que ampliará la cobertura de la seguridad sobre todos los activos de información en la entidad.

**Se identifican responsabilidades en las siguientes áreas:**

Dirección de Sistemas  
Dirección de Planeación  
Dirección de Recursos Físicos y Gestión Documental  
Dirección de Gestión Contractual  
Dirección de Gestión Humana  
Dirección de Servicio al Ciudadano  
Oficina de Control Interno y CID   
Subsecretaría Jurídica

**Responsables de la coordinación de la ejecución del Plan de Acción para implementar el Modelo de Seguridad y Privacidad de la Información :**

Dirección de Sistemas  
Dirección de Planeación  
Dirección de Recursos Físicos y Gestión Documental  
Dirección de Gestión Contractual  
Dirección de Gestión Humana  
Dirección de Servicio al Ciudadano  
Oficina de Control Interno y CID   
Subsecretaría Jurídica

**Producto:**

**Documento A-LE-009 ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN DE LA SDP, actualizado de acuerdo con la Resolución 1508 de 2017 y** [**la Guía 4 - Roles y responsabilidades del MinTIC**](http://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf)

**Duración: 1 mes  
Fecha de Entrega: 30/07/2018**

* 1. **Definición del Estado Actual de la Información (2018)**

En esta etapa la entidad debe recopilar la información necesaria para obtener un panorama general sobre los activos de información, su clasificación, herramientas tecnológicas disponibles para garantizar la seguridad y realizar seguimientos de auditoría, tratamiento y prácticas de seguridad, cultura institucional, incidencia sobre clientes internos y externos.

Como herramienta metodológica se hará uso de la **Matriz de Autoevaluación** elaborada y propuesta por el MInTIC para su aplicación en todas las entidades públicas para el subsistema de Seguridad de la Información.

Esta actividad se complementa con la revisión y actualización del inventario de activos de información de la entidad, como una jornada de participación general.

La información obtenida permitirá identificar los activos de información críticos de la entidad, generalmente asociados con los procesos misionales y de apoyo para establecer prioridad y mayor énfasis en el control para la seguridad de dicha información.

El grupo de personas que hace la recolección de información, debe reconocer el organigrama de la entidad, mapa de procesos, política de seguridad, manual de políticas, metodología de riesgos, identificación de riesgos, planes de gestión de riesgos, entre otros. Esta información es la base para la identificación de la brecha de seguridad que tiene la entidad.

También se deben identificar aquí los grupos de interés al interior de la entidad, como lo es control interno, tecnología, recursos humanos, calidad, comunicaciones, GEL, servicio al ciudadano, líderes de procesos.

**Responsable de la generación de la autoevaluación de la seguridad de la información**Dirección de Sistemas – Oficial de Seguridad

**Producto: Documento de autoevaluación del MSPI de acuerdo con la herramienta del MinTIC  
Duración: 2 Meses  
Fecha de entrega: 30/07/2018**

* 1. **Actualización, clasificación y valoración de los activos de Información**

Esta actividad implica identificar e incluir en el inventario de activos de información todos aquellos elementos que aportan información y tienen valor para la institución. La SDP cuenta con un inventario de información oficial cuya información fue recaudada en el año 2016.   
Sobre esta base se hará un proceso de identificación de nuevos elementos, la clasificación de los activos críticos y sensibles para la entidad, la valoración cuantitativa y cualitativa de los mismos. Definir y clasificar los activos de la entidad, evaluando su criticidad, sus posibles vulnerabilidades técnicas, operacionales y de gestión.

**Responsables:  
Coordinación de la actualización del inventario de activos de información de la SDP:**

Dirección de Planeación   
Dirección de Sistemas -Oficial de Seguridad  
Dirección de Recursos Físicos y Gestión Documental  
Responsables de los Procesos **Ejecución:**Toda la entidad a través de los responsables de los procesos que involucran los activos de información.  
  
**Producto:** Inventario de Activos de Información Actualizado y aprobado  
**Duración: 1 Mes  
Fecha de Entrega: 30/08/2018**

* 1. **Integración del MSPI con el Sistema de Gestión Documental de la entidad**

La seguridad de la información institucional contempla activos con componente informático (digitales) y activos de información en físico o disposición en papel. Por lo tanto, la Dirección de Recursos Físicos y Gestión Documental está llamada a aportar las características propias de la gestión de seguridad de los documentos a cargo e integrarse a este objetivo a través de las políticas, procedimientos, controles, indicadores y planes de mejoramiento aplicables al MSPI adoptado por la SDP.

**Responsables Coordinación y Ejecución:**Dirección de Sistemas –Oficial de Seguridad  
Dirección de Planeación – Líder GEL  
Dirección de Recursos Físicos y Gestión Documental

**Producto:**   
Inclusión de los activos de información físicos en las políticas, procedimientos, controles, indicadores y planes de mejoramiento aplicables al MSPI adoptado por la SDP.

**Duración: 2 Meses  
Fecha de Entrega: 30/10/2018**

* 1. **Aplicar el método definido por la entidad para identificar, analizar y asignar los riesgos**

Luego de la clasificación de los activos, la identificación del estado actual y su valoración de criticidad, es necesario revisar los riesgos asociados a la seguridad de la información de acuerdo con la metodología definida por la entidad definida en los documentos **E-LE-030 POLÍTICA DE ADMINSTRACIÓN DEL RIESGO; E-IN-005 INSTRUCTIVO PARA LA GESTIÓN DEL RIESGO; M-FO-042 MATRIZ DE ANÁLISIS, IDENTIFICACIÓN, Y ASIGNACIÓN DE RIESGOS; A-LE-303 MAPA DE RIESGOS DEL PROCESO SOPORTE TECNOLOGICO** y los asociados a la evaluación del riesgo definidos por la entidad

En este análisis se tendrá en cuenta lo siguiente:

* + 1. Activos a evaluar y estrategia de cobertura
    2. Análisis y valoración de riesgos
    3. Análisis de Vulnerabilidades
    4. Identificación de amenazas
    5. Tratamiento de riesgos. Elaboración de planes de mitigación

**Responsables de la valoración e identificación de riesgos a los activos de información:  
  
Coordinación:**Dirección de Sistemas  
Dirección de Recursos Físicos y Gestión Documental  
Dirección de Planeación  
Responsables de los Procesos  
 **Ejecución:**Toda la entidad a través de los responsables de los procesos y de los activos de información

**Producto:**   
Identificación de riesgos, vulnerabilidades y amenazas de seguridad de la información para cada activo de información registrado en el inventario.  
**Duración: 1 Mes  
Fecha de Entrega: 30/11/2018**

* 1. **Efectividad de Controles Vs Análisis de Riesgos**

En esta actividad se adelantan las verificaciones de los controles establecidos, de acuerdo con el resultado del análisis de riesgos obtenido en la actividad anterior. Las pruebas se basan en evidencias y documentación de los controles implementados y están orientadas a revisar la estructura de seguridad en la entidad con miras a generar, ajustar o crear nuevos controles que mitiguen la materialización de un riesgo.

**Responsables de la Evaluación:**

Dirección de Sistemas –Oficial de Seguridad  
Dirección de Planeación – Líder GEL  
Dirección de Recursos Físicos y Gestión Documental  
  
**Responsables de la Ejecución de Controles y Medición:**   
Toda la entidad a través de los responsables de los procesos y de los activos de información   
  
**Producto:**Listado de controles implementados (Definición, seguimiento, medición)

* 1. **Revisión de la madurez y eficiencia de los controles vigentes y Actualización de la Declaración de Aplicabilidad de Controles**

La SDP cuenta con el documento **A-LE-334 DECLARACION DE APLICABILIDAD DEL SGSI** en el que se establecen los controles de seguridad que aplican a la entidad, sobre los que se debe llevar una medición de efectividad. Dicha medición incluye llevar un registro de cada control, valorar su alcance, efectividad y el costo de realizarlo.

Además, es necesario evaluar estos controles de acuerdo con el grado de madurez que espera alcanzar la entidad en términos de seguridad de la información, los recursos disponibles (tecnológicos y humanos) y las limitaciones existentes incluyendo la consideración de requerimientos legales y regulatorios.

Por lo tanto, se debe considerar actualizar el alcance de la Declaración de Aplicabilidad del MSPI en la SDP y en consecuencia, la actualización de los controles a aplicar.

La actividad demanda revisar los controles que actualmente están documentados, revaluarlos y definir los controles pendientes de acuerdo con la declaración de aplicabilidad vigente.

Como resultado de la revisión de los controles a la luz de los riesgos, las vulnerabilidades, los costos y el alcance, es probable que se implementen los controles mediante otras técnicas, se eliminen algunos y se complementen algunas acciones de control ya existentes.

En este aspecto se realizarán dos actividades así:

* + 1. **Realización de Pruebas y Análisis de vulnerabilidad**

Las pruebas de vulnerabilidad son técnicas empleadas para comprobar la seguridad de una entidad. Para obtener un resultado objetivo, las pruebas de vulnerabilidad se realizan por medio de servicios de consultoría especializados que utilizan metodologías y herramientas informáticas a través de las cuales se concretan de manera controlada pruebas de hacking, ingeniería social, identificación de vulnerabilidades de aplicaciones, servicios web, pruebas de acceso, entre otros con el fin de sustentar qué tan robusto es un control o tan informada y capacitados está el recurso humano con relación a la información a su cargo.

Es importante tener en cuenta que estas pruebas no tienen como objetivo identificar solamente una vulnerabilidad sobre un sistema específico o algún sistema desactualizado, sino que la meta principal es identificar los riesgos de seguridad de la información a través de los controles evaluados a través de las pruebas, para así tomar las medidas proactivas/preventivas para mitigar los riesgos encontrados.

**Responsables en el diseño de las pruebas:**

Dirección de Sistemas  
Dirección de Planeación  
Dirección de Recursos Físicos y Gestión Documental  
Dirección de Gestión Contractual  
Dirección de Gestión Humana  
Dirección de Servicio al Ciudadano  
Oficina de Control Interno y CID   
Subsecretaría Jurídica

**Responsables en la ejecución de las pruebas:**

Subsecretaría de Información y Estudios Estratégicos  
Dirección de Sistemas – Oficial de Seguridad  
Dirección de Recursos Físicos y Gestión Documental

**Producto:**

Documento con los resultados obtenidos en las pruebas de seguridad para tener soportes de las labores realizadas, su impacto en términos de seguridad y a la vez la respectiva justificación de las acciones preventivas – correctivas que se propongan como consecuencia de los mismos.

Incluir la siguiente información:

* Listado de pruebas aplicadas en la categoría de técnicas y administrativas
* Identificación del entorno.
  + Ambiente técnico
  + Ambiente de cultura organizacional
* Identificación y categorización de cada tipo de vulnerabilidad
* La amenaza a la seguridad que se expone
* La causa del problema de seguridad
* La técnica de prueba usada para encontrarla
* La remediación de la vulnerabilidad
* Estado institucional frente a las mejores prácticas.
* La calificación de riesgo de la vulnerabilidad (alta, media, baja). ubicando los activos que mayor riesgo pueden traer a la organización con base al criterio del ejecutor de la prueba de efectividad de los controles.

Se requiere que estas pruebas midan además la efectividad de un sistema de monitoreo o detección, es decir, si se están realizando actividades de escaneo, ataques, infiltración, alteración de la información y que exista una respuesta eficaz.

* + 1. **Evaluación de la Declaración de Aplicabilidad**

Documento que define, justifica y argumenta los controles de la ISO 27001 que la SDP asume para implementación en su MSPI.

**Responsables:**  
Dirección de Sistemas – Oficial de Seguridad  
Dirección de Recursos Físicos y Gestión Documental  
Dirección de Planeación

**Producto:  
Declaración de Aplicabilidad actualizada  
Duración: 1 mes  
Fecha de entrega: 15/12/2018**

* 1. **Definición de Indicadores de Gestión**

Esta acción contempla la construcción de indicadores que permitan tener una medición de la efectividad de los controles vigentes frente a la presencia de incidentes de seguridad, el conocimiento de los funcionarios, contratistas y terceros de las políticas y lineamientos de TI y  
el avance de la entidad en la implementación del MSPI.

**Responsables de la definición de indicadores:**Dirección de Planeación  
Subsecretaría de Información y Estudios Estratégicos  
Dirección de Sistemas – Oficial de Seguridad  
Dirección de Gestión de Recursos Físicos y Gestión Documental

**Responsables de la aplicación de indicadores:**Todos los dueños de los procesos y activos de información a los que les aplique controles de seguridad de la información  
**Producto:  
Batería de Indicadores para el MSPI**

* 1. **Definición e implementación del Plan de Comunicaciones**

Un programa efectivo de sensibilización, capacitación y comunicación en seguridad de la información debe explicar de manera apropiada las reglas de comportamiento adecuadas para el uso de los sistemas y la información, que generalmente están plasmadas en las políticas y procedimientos de seguridad de la información que la Entidad requiere sean cumplidos por parte de todos los usuarios del sistema.

Cualquier incumplimiento a las políticas, debe llevar a la imposición de una sanción, siempre y cuando el usuario haya sido adecuadamente capacitado e informado sobre todo el contenido de seguridad correspondiente a su rol y responsabilidades.

Esta acción se focaliza sobre el componente humano de la entidad, con el fin de alcanzar no sólo la comunicación del mensaje sino la apropiación y concientización sobre la importancia de asumir la seguridad de la información en la vida personal, profesional y laboral como una práctica social.

**Responsable de la elaboración e implementación del Plan de Comunicación y Sensibilización del MSPI:**Dirección de Sistemas – Oficial de Seguridad  
Apoyo en la Implementación: Oficina de Comunicaciones

**Producto:**   
**Plan de Comunicación y Sensibilización del MSPI aprobado y en ejecución  
Duración: 12 meses  
Fecha de entrega: De enero a diciembre de 2018**

* 1. **Registro y tratamiento de bases de datos personales**

De acuerdo con la Ley 1581 de 2012 todas las entidades de naturaleza pública o privada están llamadas a cumplir con los principios y disposiciones aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento, especialmente en procesos de recolección, almacenamiento, uso, circulación o supresión.

Adicionalmente, la Directiva 002 del 6 de febrero de 2018 emitida por la Secretaría Jurídica Distrital, exhorta a todas las entidades del Distrito Capital a expedir la respectiva política de tratamiento de datos personales con el fin de garantizar a los titulares los derechos constitucionales que le asisten en términos de información, actualización, rectificación, clasificación, publicación y administración bajo condiciones de seguridad y privacidad definidas por la Ley.

En dicho procedimiento están involucradas dependencias como la Dirección de Planeación, Dirección de Gestión Humana, la Dirección de Atención al Ciudadano y todas aquellas que captan y administran información personal en el ámbito de la gestión institucional.

El resultado será la definición e implementación de una política institucional de tratamiento de datos ajustada a la normatividad vigente, que incluya herramientas tecnológicas que faciliten el seguimiento, auditoría y verificación.

El inventario de las bases de datos personales incluye la obtención de la siguiente información:

1. Cantidad de bases de datos con información personal.
2. Cantidad de titulares por cada base de datos.
3. Información detallada de los canales o medios que se tienen previstos para atender las peticiones y reclamos de los titulares.
4. Tipos de datos personales contenidos en cada base de datos a los que se realiza Tratamiento, como: datos de identificación, ubicación, socioeconómicos, sensibles u otros.
5. Ubicación de las bases de datos.
6. Los datos de identificación y ubicación de los Encargados del tratamiento.
7. Medidas de seguridad y/o controles implementados en la base de datos para minimizar los riesgos de un uso no adecuado de los datos personales tratados.
8. Conocer si se cuenta con la autorización de los titulares de los datos contenidos en las bases de datos.
9. Forma de obtención de los datos (directamente del titular o mediante terceros).
10. Si se ha realizado transferencia o transmisión internacional de los datos personales contenidos en la base de datos.
11. Si se ha realizado cesión de la base de datos.

Fuente: <http://www.sic.gov.co/preguntas-frecuentes-rnbd>

**Responsables de la definición y aplicación de la estrategia para el Registro y Tratamiento de Datos Personales**  
Dirección de Planeación  
Dirección de SistemasDirecciones Responsables del tratamiento de la información personal contenida en las bases de datos.

**Responsables de la ejecución del tratamiento de datos**

Dirección de Servicio al Ciudadano  
Dirección de Gestión Humana  
Dirección de Recursos Físicos y Gestión Documental  
Dirección de Gestión Contractual  
Dirección de Sisbén  
Dirección de Estratificación  
Dirección de Análisis y Conceptos Jurídicos  
Y todas aquellas áreas que se identifiquen posteriormente con el tratamiento de datos personales

**Producto:**Bases de Datos Personales registradas en la SIC  
Procedimiento Tratamiento de Datos personales actualizado e implementado.

**Duración: 3 meses  
Fecha de entrega: 30/11/2018**

Nota: La responsabilidad de la coordinación puede variar de acuerdo con la respuesta a un concepto solicitado a la Secretaría Jurídica de la Alcaldía de Bogotá.

* 1. **Medición de Indicadores de Gestión**

Una vez establecidos los períodos de medición para los controles de seguridad de los activos, se alimentan los indicadores de gestión y se realiza la presentación de los resultados a la Dirección.  
Estos resultados son la base para medir internamente los avances en la seguridad de la información y la evidencia para la activación de mejoras y afinación de controles.

**Responsables de la Consolidación de Información**Dirección de Planeación  
Subsecretaría de Información y Estudios Estratégicos  
Dirección de Sistemas – Oficial de Seguridad  
Dirección de Recursos Físicos y Gestión Documental

**Responsables de alimentar los indicadores:**Toda la entidad a través de los responsables de los procesos y de los activos de información

**Producto:**   
Informe de medición de indicadores de gestión de la seguridad de la información

* 1. **Plan de Transición IPV4 a IPV6**

La transición de protocolo IP versión 4 a la versión 6 es un imperativo global. Las entidades públicas tienen la obligación de adelantar las acciones de capacitación, desarrollo, pruebas e implementación y aseguramiento para proveer no sólo el acceso la información institucional, sino el funcionamiento e interacción de todos sus recursos.   
La SDP ya adelantó la etapa de diagnóstico y caracterización. Le siguen las fases de:

* Plan de Transición
* Implementación de Tecnologías
* Monitorización
* Testing Funcional
* Configuración y soporte
* Aseguramiento de entornos
* Estrategia de apagado IPv4.

Es de anotar que, si bien el plazo establecido por el MinTIC para realizar a la transición completa a IPv6 es hasta el 2020, en dicho período se deben realizar acciones que afectan a todos los activos de información digitales que incluyen: actualizaciones en aplicaciones, servidores, computadores personales, dispositivos electrónicos, servicios web, servicios de rede, repositorios y bases de datos, lo que genera un impacto importante en la entidad.

Dichos esfuerzos van acompañados generalmente de altas inversiones y riesgos, algunos no previstos, que pueden llevar a acciones y tiempos adicionales, por lo que es recomendable manejar esta acción como un proyecto independiente, pero ajustado y alineado con el MSPI.

**Responsables:**Dirección de Sistemas – Equipo de Infraestructura

**Producto:**Plan de Transición y de Implementación aprobado

* 1. **Auditoría interna, revisión del proceso y mejoras**

Una vez cumplido el ciclo de actividades de implementación del MSPI es necesario realizar la auditoría interna por una autoridad de control (Oficina de Control interno de la SDP) que garantice la aplicación de normas y estándares para la seguridad de la información.

La auditoría interna es la preparación para auditorías de entes de control o autoridades de certificación de calidad en sus diferentes aspectos.

Las no conformidades o recomendaciones de la auditoría interna serán tomadas como los aspectos a mejorar sobre los cuales se deben enfocar las acciones inmediatas.

Algunas actividades pueden adelantarse se manera simultánea y/o independiente, como es el caso de la definición e implementación del plan de comunicaciones; el registro y tratamiento de bases de datos personales y el plan de transición IPV4 a IPV6.

Para las demás se sugiere seguir el orden establecido con el fin de obtener resultados objetivos, con acciones sustentadas en evaluaciones y acciones que han sido objeto de medición.

**Responsables:**

Oficina de Control Interno  
Dirección de Sistemas – Oficial de Seguridad  
Dirección de Recursos Físicos y Gestión Documental

1. **RECURSOS**

La implementación del MSPI está sujeto a diferentes tipos de recursos para su implementación

* 1. **Recursos Humanos:** Orientados a generar de manera transversal en la entidad acciones de capacitación y sensibilización; identificación de activos de información con sus riesgos, amenazas y vulnerabilidades; identificación de controles; aplicación de controles; evaluación y seguimiento de controles; medición; reporte, activación e implementación de planes de mejoramiento.
  2. **Recursos Tecnológicos:** Son herramientas tecnológicas cuya función es cerrar las posibles vulnerabilidades en la plataforma informática de la entidad. Estas herramientas son específicas y están orientadas a brindar seguridad o generar reportes en activos como la red de comunicaciones, los servidores, el correo electrónico, aplicaciones, servicios web e incluso archivos específicos.

En principio, se debe realizar una evaluación técnica de la funcionalidad actual de la plataforma tecnológica de la SDP, las debilidades, posibles fallas, desactualizaciones o vulnerabilidades identificadas, así como una evaluación del estado del arte en seguridad tecnológica para plantear un esquema de seguridad acorde a las necesidades y recursos institucionales.

Algunas herramientas están orientadas a la seguridad de la infraestructura informática son:

Proxi para control de acceso o navegación

Filtrado de contenido

DLP (Data Lost Prevention) para instalación en equipos de cómputo.

IPS (Intrusion Prevention System) minimiza eficazmente una amplia gama de ataques de red. Sistemas inteligentes utilizados para identificar, clasificar y detener o bloquear con precisión el tráfico malicioso en tiempo real.

NAC (Network Access Control): Tecnología que permite controlar de forma granular qué dispositivos pueden acceder a la red, permitiendo establecer políticas de gestión de los dispositivos, tanto fijos como móviles.

Seguridad para el correo electrónico: con herramientas de filtrado, spam, antivirus, antimalware y cifrado.

Firewall para bases de datos o archivos

Es de anotar que algunas de estas herramientas pueden cumplir varias funciones de seguridad, dependiendo del objetivo y la ubicación específica en el entorno informático. Por ello, esta evaluación se debe realizar de manera coordinada con los encargados de la infraestructura y operación informática de la entidad.

Para todos los casos las herramientas deben contar con opciones de reporte que garanticen la trazabilidad y auditoria de las políticas de seguridad definida en dispositivos de hardware o software

* 1. **Recursos Comunicacionales:** La seguridad de la información está asociado a la actuación cotidiana de su recurso humano en la gestión de la información de acuerdo con las políticas y lineamientos definidos por la entidad.

Por lo tanto, la consolidación de la cultura de la seguridad es un proceso permanente que debe apoyarse en recursos comunicacionales, de sensibilización y concienciación en todos y cada uno de sus funcionarios, contratistas, proveedores y partes interesadas.

Por lo tanto es obligatorio la activación de campañas de información y sensibilización a través de medios de comunicación internos como intranet y correo electrónico, las cuales se deben complementar con actividades vivenciales de participación activa como dinámicas, concursos, talleres, conmemoración de fechas especiales que generen recordación e interiorización práctica de la seguridad de la información.  
Naturalmente algunas actividades requieren de recursos adicionales a los relacionados con las funciones de algunos cargos.

* 1. **Consultorías**Algunas actividades de la implementación del MSPI desbordan la capacidad de gestión institucional, debido a que pertenecen a un ámbito específico y la entidad no cuenta con las herramientas técnicas y el recurso humano especializado para adelantar dichas acciones con los resultados esperados. Por esta razón se recomienda la contratación de consultorías previamente definidas en su alcance, calidad y resultados esperados.

Este es el caso para:

* **Plan de Transición IPV4 a IPV6** en sus diferentes etapas. Es de anotar que los ajustes a desarrollos, aplicativos o elementos de hardware no están incluidos en el alcance de la consultoría.
* **Acompañamiento en el proceso de pruebas y análisis** con énfasis en hacking ético controlado, ingeniería social, análisis de efectividad en los servicios de red, eficiencia en servicios web y administración de aplicaciones, entre otros.
* **Servicios comunicacionales de participación** y experiencias prácticas, que pueden estar asociados con talleres, conferencias de expertos para usuarios y dinámicas vivenciales.

* 1. **Recursos para formación y capacitación**

La seguridad asociada a la información requiere de permanente actualización, debido a que las amenazas se renuevan cada cierto ciclo, y tanto la industria del software como la del hardware liberan periódicamente actualizaciones en sus productos. También las organizaciones deben actualizar sus políticas y conocimientos sobre los nuevos riesgos, vulnerabilidades y debilidades a los que se enfrentan en razón de los intereses internos o externos para acceder de manera anónima e intencional al recurso público de la información.  
En este sentido, se requiere disponer de recursos para que los servidores de la SDP accedan a espacios de capacitación técnicos y prácticos y tengan posibilidades frente a ofertas del Estado a través del MinTIC.   
La formación debe extenderse a funcionarios de todas las dependencias, especialmente a aquellos que tienen roles y responsabilidades en la seguridad de la información en la SDP.

1. **CRONOGRAMA**

De acuerdo con el plazo establecido por el MinTIC, en el 2018 todas las entidades públicas de orden nacional y territorial deben contar con el MSPI implementado en el 100% siguiendo las sugerencias y las guías desarrolladas por ese ministerio.

En la última evaluación de diagnóstico realizada entre febrero y marzo de 2018, la entidad se posiciona en un nivel de cumplimiento del 30%, lo que indica un nivel de criticidad en la implementación del modelo.

Si bien las actividades aquí descritas implican un orden en su desarrollo, pues los resultados de una son el insumo de la siguiente, es posible realizar algunas de manera independiente y paralela dada su criticidad. Otras deben estar presentes de forma permanente, como es el caso de la comunicación y sensibilización.

No obstante, el cumplimiento de las metas depende del compromiso de la alta dirección, de la eficacia de los responsables en el cumplimiento de sus roles, de la disposición de los recursos planteados y de la evaluación permanente de los controles.

Bajo estas condiciones se expresa el cronograma de la siguiente forma:



**BIBLIOGRAFÍA**

* **Estándar ISO 27001:2013**
* **Modelo de Seguridad y Privacidad de la Información. MinTIC. Versión 3.0.2**
* **Diseño e implementación de una estrategia de seguridad de la información. Guía Técnica. MinTIC. Versión 1.0**
* **Metodología Pruebas de Efectividad. MinTIC. Versión 1.0**
* **Implementación de la Estrategia del Modelo de Seguridad y Privacidad de la Información de las Entidades Distritales. Alta Consejería Distrital de TIC.** [**www.ticbogota.gov.co**](http://www.ticbogota.gov.co)