PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Departamento Administrativo de la Defensoría del Espacio Público

2019

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

LISTA DE TABLAS

1 INTRODUCCIÓN

La nueva Política de Gobierno Digital tiene el objetivo de desarrollar un enfoque integral que permita obtener, por medio del uso y aprovechamiento de las tecnologías de la información, un valor público mediante la articulación entre el Estado y la Sociedad generando mayor competitividad, innovación y proactividad.

La Política de gobierno digital está conformada por dos (2) componentes denominados, TIC para el Estado y TIC para la Sociedad, ambos encargados de orientar la implementación de esta política, además de tres (3) habilitadores transversales que facilitan su desarrollo, llamados: Seguridad y Privacidad, Arquitectura de Tecnologías de la Información-TI y Servicios Ciudadanos Digitales, para desarrollar los cinco (5) propósitos definidos en la política, como son: Servicios Digitales, Procesos Internos Seguros y Eficientes, Decisiones Basadas en Datos, Empoderamiento Ciudadano y Desarrollo de territorios y Ciudades Inteligentes que cuya finalidad es generar valor con entornos de confianza digital.

En este plan se hace referencia del habilitador **Seguridad y Privacidad** por lo cual es necesario hablar del **Modelo de Seguridad y Privacidad de la Información** que hace parte de la antigua estrategia Gobierno en Línea – **GEL.** En este modelo se propone un conjunto de guías prácticas que contribuyen a mitigar los riesgos asociados a la seguridad de la información, así como velar por la preservación de la confidencialidad, integridad y disponibilidad de los activos de información con los que cuenta la Entidad. En tal sentido, la seguridad de la información actúa como eje transversal e integral para el desarrollo de objetivos y metas propuestas a través de estructuras de relaciones y procesos organizacionales que velan por la protección de la información de la entidad.

2 OBJETIVO

Establecer la estrategia para la definición e implementación de políticas, controles, lineamientos, procedimientos y buenas prácticas que contribuyan con la preservación de la disponibilidad, integridad y confidencialidad de los activos de información del Departamento Administrativo de la Defensoría del Espacio Público-DADEP que favorezcan una cultura organizacional, eficiente y eficaz en la gestión de la seguridad de la información, transparencia, protección de datos personales y acceso a la información pública cumpliendo con la normativa vigente en la materia.

2.1 Objetivos específicos

- Definir la estrategia para gestionar los riesgos de seguridad de la información asociados a los activos de información del Departamento Administrativo de la Defensoría del Espacio Público-DADEP.
- Establecer los procedimientos, controles y buenas prácticas para la gestión eventos e incidentes que afecten la integridad, confidencialidad e integridad de los activos de información de la entidad.
- Definir políticas y controles que contribuyan con la seguridad de la información de la entidad.
- Identificar acciones de mejora que faciliten el intercambio de información pública de forma segura.
- Sensibilizar el talento humano para la gestión eficiente y eficaz en seguridad de la información.

3 ALCANCE

El Plan de Seguridad y Privacidad de la Información inicia con la definición y adopción de la política de seguridad de la información, la clasificación de los activos de información críticos que hacen parte de los procesos, la identificación y tratamiento de los riesgos de seguridad de la información y finaliza con la definición de procedimientos, controles además de buenas prácticas de seguridad de la información que permitan proteger los activos de información del Departamento Administrativo de la Defensoría del Espacio Público-DADEP.

4 DEFINICIONES Y SIGLAS

4.1 DEFINICIONES

Para la adecuada gestión de la seguridad de la información se debe manejar con propiedad los siguientes términos:

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

- **Activo [Según ISO 27000]:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- **Amenaza [Según ISO 27000]:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- **Análisis de Riesgo [Según ISO 27000]:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

- **Auditoría [Según ISO 27000]:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria.

- **Autorización [Ley 1581 de 2012, art 3]:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

- **Ciberseguridad [CONPES 3701:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

- **Ciberespacio [Resolución CRC 2258 de 2009]:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.

- **Control [Según ISO 27000]:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Datos Abiertos [Ley 1712 de 2014, art 6**]: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

- **Declaración de aplicabilidad [Según ISO 27000]:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

- **Framework:** Marco de trabajo con lineamientos, conceptos y prácticas que sirve como referencia para tratar un tema específico.

- **Gestión de incidentes de seguridad de la información [Según ISO 27000]:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

- **Impacto [Según ISO 27000]:** El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

- **Información Pública Clasificada [Ley 1712 de 2014, art 6]:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.

- **Información Pública Reservada [Ley 1712 de 2014, art 6]:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.

- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **Plan de tratamiento de riesgos [Según ISO 27000]:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

- **Riesgo [Según ISO 27000]:** 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 consecuencias.

- **Riesgo Residual [Según ISO 27000]:** El riesgo que permanece tras el tratamiento del riesgo.

- **Seguridad de la información [Según ISO 27000]:** Preservación de la confidencialidad, integridad, y disponibilidad de la información.

- **Sistema de Gestión de Seguridad de la Información SGSI [Según ISO 27000]:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

- **Vulnerabilidad [Según ISO 27000]:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

4.2 SIGLAS

- **DADEP:** Departamento Administrativo de la Defensoría del Espacio Público.
- **TI**: Tecnologías de la información.
- **MINTIC:** Ministerio de Tecnologías de la Información y las Comunicaciones.
- **MSPI**: Modelo de seguridad y privacidad de la información.
- **ISO:** Organización Internacional de Estandarización
- **NIST:** Instituto Nacional de Estándares y Tecnología.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **SI:** Seguridad de la Información.
- **PETI:** Plan Estratégico de Tecnologías de la información.

5 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

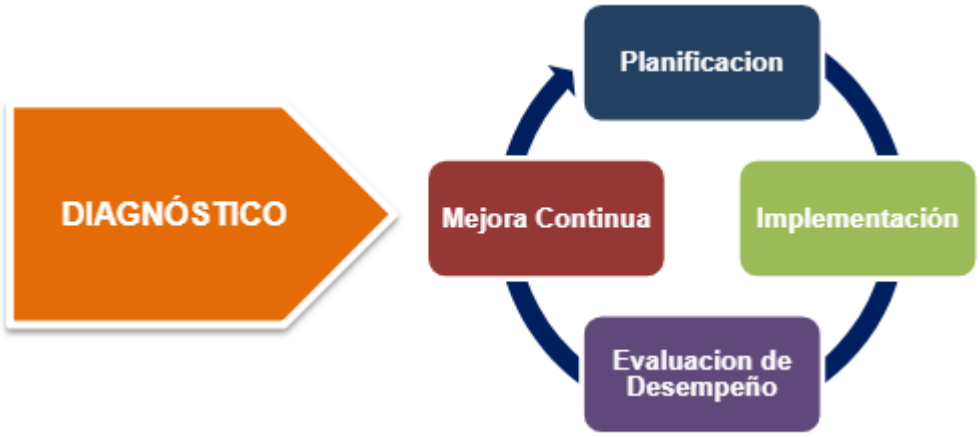
El Departamento Administrativo de la Defensoría del Espacio Público - DADEP, para dar cumplimiento a lo establecido en el Decreto 1078 del 26 de mayo de 2015 del MinTIC: por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, inicio la implementación del Modelo de Seguridad y Privacidad de la Información-**MSPI** desde al año 2016 donde los avances más relevantes hasta la fecha son: el compromiso de la alta dirección, la definición y adopción de la Política de Seguridad de la Información e implementación del manual de gestión de seguridad de la información en el cual se contempla controles para mitigar los riesgos asociados los activos de información.

Con la transformación de la Estrategia de Gobierno en Línea a política de Gobierno Digital, obliga a la entidad a resolver nuevos retos encaminados hacia la implementación de cada uno de los componentes, habilitadores y el logro de los propósitos que hacen parte de la nueva política "Gobierno Digital".

Como respuesta a los requerimientos de la política digital y a lo establecido el decreto 1008 del 14 de junio de 2018 de MinTIC : **"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" el DADEP, va a desarrollar el habilitador seguridad y privacidad de la información utilizando la metodología definida por el MinTIC en las guías para la implementación del modelo de seguridad y privacidad de la información-MSPI que establece cinco fases a través de un ciclo de operación con objetivos, metas y actividades que a continuación se describen:

Ilustración 1. Ciclo de Operación



Fuente. Guía Modelo de Seguridad y Privacidad de la Información – MinTIC

La ilustración 1 propone un ciclo de operación el cual inicia a partir de un diagnóstico y cuatro fases con las acciones encargadas de gestionar la protección de los activos de información, los riesgos asociados a los activos y finalmente dar cumplimiento a requisitos de Ley; para esto, a continuación se describen actividades y avances por cada una de las fases necesarias para la implementación del Modelo de Seguridad y Privacidad de la Información.

5.1 FASE DE DIAGNOSTICO

El ciclo de operación para la implementación del Modelo de Seguridad y Privacidad de la Información inicia con la identificación de un diagnóstico preliminar, a partir del cual se logra determinar el nivel de madurez y cumplimiento actual acerca de la gestión de la seguridad de la información realizada al interior del DADEP. Para esto, se utilizó el instrumento diseñado por el MinTIC denominado Instrumento de Identificación de la Línea Base de Seguridad, el cual tiene como propósito evaluar la efectividad de los controles establecidos en el anexo A del estándar internacional ISO 27001 versión 2013. Medir el porcentaje de avance del modelo de operación (PHVA) que permite la mejora continua de cada una de las fases que hacen parte del ciclo de operación del MSPI y finalmente, identificar el nivel de madurez actual sobre los controles y la gestión de riesgos orientados hacia la Ciberseguridad tomando como referente el estándar NIST 800-53, obteniendo los siguientes resultandos:

Evaluación de efectividad de controles - ISO 27001:2013 anexo A.

El anexo A del estándar internacional ISO 27001 versión 2013 especifica 14 dominios, 35 objetivos de control y un total de 114 controles propuestos para la mitigar los riesgos y realizar una adecuada gestión de la seguridad de la información.

En razón a lo anterior, los resultados obtenidos en el instrumento de diagnóstico permiten inferir que se encuentran gestionados de acuerdo a la escala de evaluación los controles relacionados con los dominios de *políticas de seguridad de la información, seguridad de los recursos humanos, control de acceso, seguridad física y del entorno y seguridad de las operaciones*, dado que se realiza monitoreo y medición al cumplimiento de los procedimientos. No obstante, los dominios de *organización de la seguridad de la información, gestión de activos, seguridad de las comunicaciones, adquisición desarrollo y mantenimiento y por último cumplimiento* contemplan aspectos de seguridad en los cuales existe un avance significativo, pero resulta importante en estos controles lograr identificar cuando el control no se aplica oportunamente o la forma en que se aplica el control no es la más precisa e indicada.

Es evidente entonces, que la entidad debe orientar sus esfuerzos para fortalecer los controles relacionados con los dominios de *relación con los proveedores, aspectos de la seguridad de la información,* que a pesar de contar con algunos procedimientos, no se encuentran debidamente estandarizados, documentados y formalizados.

Ilustración 2 Dominios ISO 27001:2013

NOTA: Esta información no se publica ya que puede generar riesgo para la entidad.

Fuente: Instrumento de Evaluación MSPI 2018

La ilustración 2 refleja el estado actual o nivel de madurez de acuerdo a la escala de evaluación en que se encuentran los dominios del anexo A del estándar ISO 27001:2013 implementados al interior de la entidad, arrojando en su gran mayoría que se encuentran de forma gestionada y efectiva, pero que hay que mejorar los demás dominios a fin de implementar controles adecuados.

5.1.1 Avance ciclo de funcionamiento del modelo de operación (PHVA)

Se conoce como PHVA al ciclo de cuatro (4) fases definidas como Planear, Hacer, Verificar y Actuar, que de manera sistémica operan en función de lograr el mejoramiento continuo acerca de los productos o servicios que ofrecen las distintas organizaciones. Para tal fin, la entidad luego de aplicar el formato *Instrumento de Identificación de la Línea Base De Seguridad* logra determinar el nivel de cumplimiento del ciclo definido dentro del MSPI de la siguiente manera:

- Fase de Planificación: La entidad ha definido un marco de seguridad y privacidad de la información dado que actualmente cuenta con: la política de seguridad y de la información, manual de políticas de seguridad de la información, una serie de procedimientos generales de seguridad, posee un inventario de activos de la información y se tiene documento con la metodología, análisis, evaluación y tratamiento de riesgos. Sin embargo resulta importante desarrollar la documentación acerca de procedimientos detallados de seguridad de la información, establecer los roles y responsabilidades de SI, definir el plan de comunicación y sensibilización de SI, realizar la declaración de aplicabilidad,

plan de diagnóstico de IPV4 a IPV6 así como fortalecer e implementar el programa de gestión de riesgos de la información de la entidad.

- Fase de Implementación: En esta fase la entidad ha realizado avances acerca el tratamiento de riesgos, aunque se hace evidente llevar a cabo el plan de tratamiento de riesgos de Seguridad de la información, además definir y aplicar indicadores y métricas acerca de la gestión de la seguridad y privacidad de la información.

- Fase de Evaluación de Desempeño: Actualmente el DADEP cuenta con un plan de auditorías y un plan de seguimiento, no obstante el nivel de desarrollo de las etapas anteriores limita los resultados de la evaluación del desempeño en cuanto a la gestión de la seguridad de la información.

- Fase de Mejora Continúa: Sobre esta fase resulta importante que la entidad avance aún más en las metas y resultados de las fases anteriores de modo que se defina un plan de mejoramiento y un plan para la comunicación de resultados de la gestión e implementación del MSPI.

Tabla 1. Nivel de avance de implementación del MSPI

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2015	Planificación	18%	40%
2016	Implementación	5%	20%
2017	Evaluación de desempeño	4%	20%
2018	Mejora continua	4%	20%
TOTAL		31%	100%

Fuente. Instrumento medición MINTIC

En la tabla anterior se observa el porcentaje de avance logrado por el DADEP, en donde el resultado obtenido es producto del desarrollo e implementación del Modelo de Seguridad y Privacidad de la Información.

5.1.2 Desempeño de mejores prácticas en Ciberseguridad (NIST)

El Instituto Nacional de Estándares y Tecnología conocido por las siglas NIST es una agencia de los Estados Unidos que promueve innovación y competencias en diversos campos de aplicación por medio de mediciones, estándares y tecnologías.

De acuerdo con NIST, en el año 2014 la agencia emitió el marco de trabajo "NIST Cybersecurity Framework" que contempla directrices, prácticas y estándares para gestionar de manera adecuada la infraestructura critica de las organizaciones permitiendo una adecuada gestión de los riesgos de seguridad cibernética. El framework se encuentra estructurado con funciones, categorías, subcategorías y referencias informativas que le permiten al DADEP realizar una adecuada la gestión de la Ciberseguridad en cada una de las funciones de la siguiente manera:

5.1.2.1 Identificar

Esta función requiere el desarrollo y comprensión organizacional de la importancia de los activos de información para priorizar esfuerzos en la administración y gestión de los riesgos de Ciberseguridad.

Las categorías que hacen parte de esta función el Framework las denomina como:

- Gestión de activos
- Gobernanza
- Ambiente de negocios
- Evaluación de riesgos
- Estrategia de gestión de riesgos

En este sentido, la entidad actualmente ha identificado la infraestructura considerada como crítica, sin embargo resulta importante priorizar la gestión y clasificación de activos de información, en especial con aquella información que hace parte de la misionalidad y con los objetivos estratégicos, que permita realizar una apropiada evaluación de riesgos y posibles amenazas de Ciberseguridad.

5.1.2.2 Proteger

En esta función se desarrollan e implementan medidas de protección que permitan proteger la integridad, confidencialidad y disponibilidad de los datos, información, sistemas de información y servicios tecnológicos. Adicionalmente, esta función debe medir la capacidad de los recursos frente a eventos e incidentes de Ciberseguridad, por lo tanto resulta importante llevar una adecuada gestión en las siguientes categorías:

- Control de acceso
- Capacitación y sensibilización
- Seguridad datos
- Procesos y procedimientos de protección de la información
- Mantenimiento
- Tecnología de protección

Sobre esta función se hace necesario que el DADEP fortalezca actividades, controles, procesos y procedimientos de seguridad cibernética de forma continua permitiendo así alcanzar niveles de protección adecuados sobre los activos críticos de la entidad y de esta forma lograr reducir el nivel de exposición al riesgo que se enfrentan.

5.1.2.3 Detectar

En la detección se emplean mecanismos de prevención y detección oportuna acerca de eventos e incidentes de seguridad de la información que puedan afectar las infraestructuras tecnológicas y demás activos críticos para la entidad y para ello, son contempladas las siguientes categorías:

- Anomalías y eventos.
- Monitoreo continuo de la seguridad.
- Procesos de detección.

La entidad cuenta una política de niveles de acceso y autorización a los sistemas de información y posee algunos recursos que apoyan la identificación de anomalías y eventos, es necesario contar con herramientas tecnológicas de seguridad como: talento humano capacitado, procesos estandarizados entre otros, que de manera articulada detecten oportunamente riesgos, amenazas, eventos e incidentes.

5.1.2.4 Responder

La función de responder se encarga de llevar a cabo el despliegue de procesos, procedimientos, recursos tecnológicos y talento humano para responder ante la materialización de eventos de seguridad cibernética con el propósito de lograr un impacto bajo sobre los activos de información de las organizaciones. Para esto, es necesario adoptar las siguientes categorías:

- Planes de respuesta a eventos e incidentes.
- Comunicaciones.
- Análisis.
- Mitigación.
- Mejoras (Procesos, Tecnología, Talento Humano).

El DADEP ha trabajado en la definición de algunas actividades para la respuesta a incidentes de seguridad cibernética, se puede considerar que los procesos y procedimientos son Ad Hoc ya que no hay actividades que sigan un orden especifico, indicadores de gestión más precisos, así como roles y responsabilidades. Por tanto es necesario trabajar en ello para facilitar la respuesta y atención a incidentes.

5.1.2.5 Recuperarse

En esta función las actividades están asociadas para que las organizaciones cuenten con un plan de contingencia, plan de recuperación de desastres y plan de continuidad de negocio para retornar a la operación y funcionamiento normal luego de un incidente con el objetivo de reducir el impacto. Por lo tanto, es necesario contemplar las siguientes categorías:

- Planes de recuperación.
- Mejoras.
- Comunicaciones

Actualmente existen en la entidad algunos procedimientos no estandarizados y documentados, tan solo se depende en gran medida de la experticia, conocimientos y formación del talento humano. Por lo que se evidencia un problemática inmediata que atender a nivel general sobre cada una de las funciones que contribuyan a la gestión de la seguridad y privacidad de la información.

Ilustración 3 FRAMEWORK CIBERSEGURIDAD NIST

NOTA: Esta información no se publica ya que puede generar riesgo para la entidad.

Fuente: Instrumento de Evaluación MSPI 2018

5.2 FASE DE PLANIFICACIÓN

Durante el año 2018 y con el propósito de avanzar en la implementación del Modelo de Seguridad y Privacidad de la Información, la entidad logró avances significativos que fueron liderados desde la oficina de Sistemas con el apoyo y colaboración de otras dependencias que permitieron alcanzar el 76 % de las actividades definidas dentro del plan de seguridad y privacidad de la información que se propuso.

Dentro de los logros más significativos se encuentran:

- La publicación y adopción de la política de seguridad de la información y el manual de gestión de seguridad de la información
- Identificación de vulnerabilidades sobre los sistemas de información.
- Establecer documento de roles y responsabilidades de seguridad de la información.
- Levantamiento de inventario y clasificación de los activos de información.
- Definición del Plan de Gestión de Riesgos de Seguridad Digital.
- Diseño y socialización del Plan de Sensibilización y Concientización de Seguridad de la Información.
- Establecer procedimientos de seguridad de la información.
- Definición de la guía para la gestión de incidentes de seguridad de la información
- Diagnóstico y plan de implementación y transición del protocolo de comunicaciones IPV4 a IPV6

Adicionalmente, se empezó a trabajar en la identificación de riesgos de seguridad digital con los procesos misionales de la entidad que permita mitigar el nivel de riesgos de exposición al que se enfrentan los activos de información.

Ver plan de trabajo anexo 1

5.3 FASE DE IMPLEMENTACIÓN

En esta fase se lleva a cabo la implementación de la fase de planificación realizada, en donde es necesario sean ejecutadas las actividades descritas a continuación:

- Implementar del plan de tratamiento de riesgos de seguridad de la información.
- Implementar de controles de seguridad y privacidad de la información
- Realizar la declaración de aplicabilidad.
- Establecer indicadores de gestión.
- Implementar plan de transición de IPV4 a IPV6.
- Gestionar la respuesta a incidentes de seguridad de la información.

Ver plan de trabajo anexo 1

5.4 FASE DE EVALUACIÓN DE DESEMPEÑO

En la fase de evaluación de desempeño se realiza seguimiento y monitoreo al MSPI tomando de referencia los indicadores y métricas estratégicas, de gerencia y operativas que apoyen la posterior toma de decisiones sobre el MSPI por lo cual es necesario contemplar lo siguiente:

- Realizar plan de seguimiento y revisión de la efectividad de la implementación del MSPI.
- Realizar plan de ejecución de auditorías.
- Medir la efectividad de los controles y políticas definidas
- Revisar los niveles de riesgos.
- Actualizar los planes entorno a la seguridad de la información.

Ver plan de trabajo anexo 1

5.5 FASE DE MEJORA CONTINUA

En esta fase se consolidan los resultados de la fase anterior que sirven de insumo para elaborar el plan de mejoramiento continuo contemplando las acciones correctivas y preventivas adecuadas que contribuyan a la eficacia del MSPI, para lo cual es necesario realizar las siguientes actividades:

- **Desarrollar plan de mejora continua:** Durante la vigencia del plan de seguridad y privacidad de la información se gestionaran las acciones correctivas y preventivas producto de los seguimientos y revisiones a la implementación y las auditorias programadas dentro del plan de auditoria de Control Interno.

- **Gestión de las comunicaciones de este plan:**

La adecuada administración de las comunicaciones, permitirán fortalecer las estrategias para lograr una efectiva comunicación interna y externa de manera transversal, mejorando la gestión en temas de seguridad y privacidad de la información.

La estrategia de comunicaciones del Plan de Seguridad y Privacidad de la Información se traducirá en

un plan de difusión a ser ejecutado durante el período de duración del proyecto, teniendo en cuenta los siguientes elementos:

Información a comunicar: La comunicación contendrá detalles de: avances en las actividades programadas, resultados de los seguimientos al plan, comunicación de atención a incidentes, tips de buenas prácticas de seguridad en la información implementadas en el DADEP y su periodicidad se realizará de acuerdo a los avances y las necesidad identificadas por el área de Sistemas o la Dirección de la entidad.

Audiencia identificada: De acuerdo a los objetivos propuestos en el plan, en la audiencia objetivo se describe de la siguiente manera:

Público Interno: Son los servidores que trabajan en la entidad ya sea en calidad de funcionarios de carrera administrativa, libre nombramiento, provisionales, así como los contratistas, y que desarrollan su labor dentro o fuera de las instalaciones del DADEP.

Ciudadanía en General: Cualquier ciudadano habitante del Distrito Capital que desee obtener cualquier tipo de información pública referente a la seguridad y privacidad de la información.

Actores Políticos o entes externos: Concejales, ediles, representantes políticos de la ciudadanía con poder de decisión, así como las demás entidades con funciones de vigilancia y control de gestión de las entidades públicas.

Mensaje y medios de comunicación: Los mensajes a transmitir se adecuarán a los distintos grupos que forman la audiencia, mediante comunicaciones escritas, página web, reuniones, carteleras internas, web interna, Audios y correos institucionales, Redes sociales, correos internos, audios, carteleras y anuncios en vivo por medio del sistema de sonido, Vocerías institucionales, plataformas digitales de la entidad.

6 METODOLOGÍA A IMPLEMENTAR

El Departamento Administrativo para la Defensoría del Espacio Público – **DADEP** adoptará el ciclo de vida PHVA que a través de la mejorar continua logre la implementación total del Modelo de Seguridad y Privacidad de la Información propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones - **MinTIC**.

7 MATRIZ RACI

La matriz RACI permite realizar un mapeo de los roles y responsabilidades asociadas a cada actividad definida que hace parte del plan de seguridad y privacidad de la información. Allí se describe quién hace parte dentro del desarrollo de la actividad y con qué nivel de participación.

En la tabla 2 se definen las responsabilidades asociadas a cada uno de los roles haciendo uso de la matriz

RACI en donde la letra A corresponde al responsable de que la actividad se cumpla, la letra R es el encargado de realizar la actividad, la letra C corresponde a quién posee información o conocimiento que sirve como insumo para llevar a cabo la actividad y por último la letra I corresponde a quién se debe informar el estado o avance del desarrollo de la actividad.

Ilustración 4 Matriz RACI

Tabla 2. Matriz de Responsabilidades

FASE	ACTIVIDAD	Rol					
		Director	Oficial de Seguridad de la Información	Responsable del Proceso	Jefe de Oficina de Sistemas	Gestor de Riesgos	Subdirector SAF
Planeación	Establecer Política de Seguridad de la Información	A	R	I	C		
	Establecer manual de gestión de Seguridad de la Información	A	R	I	C		
	Actualizar el manual de seguridad de la información		A/R	I	C		
	Actualizar la política de seguridad de la información del DADEP		A/R	I	C		
	Validar seguridad en aplicaciones de la Entidad		A/R		R	I	
	Establecer roles y responsabilidades de seguridad de la información	I	A/R	I	I		
	Definir instrumento para el levantamiento y clasificación de activos de información	I	A/R	I	C		I
	Realizar levantamiento y clasificación de activos de información	A	R	R	R		I
	Establecer contexto de los riesgos de seguridad de la información	I	A/R	C		R	
	Identificar riesgos de seguridad de la información	I	A/R	R	R	R	R
	Realizar análisis de riesgos de seguridad de la información	I	A/R	C		R	
	Realizar evaluación de los riesgos de seguridad de la información	I	A/R	C		R	
	Establecer declaración de aplicabilidad	I	A/R	C	C	I	
	Diseñar el programa de sensibilización y capacitación	I	A/R		R	C	R
	Diseñar el plan de sensibilización y capacitación de sensibilización y capacitación en seguridad de la información	I	A/R		C	I	C
	Definir herramientas para el programa de sensibilización y capacitación en seguridad de la información	C	A/R		R		R
	Implementar el programa de sensibilización y capacitación en seguridad de la información		A/R		R		R
	Establecer y documentar procedimientos de seguridad de la información	I	A/R	I	R	I	I
	Definir guía para la gestión de eventos e incidentes de seguridad de la información	I	A/R	I	C		
Implementación	Implementar plan de tratamiento de riesgos de seguridad de la información	I	A/R	C		R	
	Establecer el plan de contingencias de los sistemas de información y servicios de TI	I	R	C	A/R	C	
	Definir componentes para la continuidad del negocio	C	R	C	C	A/R	
	Realizar análisis de impacto del negocio		R	R		A/R	
	Implementar transición Protocolo IPV4 - IPV6	C	C	I	A/R	I	

Fuente: Elaboración Propia

8 RECURSOS

El origen de los recursos que harán parte del diseño e implementación del plan de seguridad y privacidad de la información, provienen del proyecto de inversión *Fortalecimiento de la plataforma tecnológica del DADEP* y a su vez se articula con el modelo de gestión de TI definido en el actual Plan Estratégico de Tecnologías de la Información – PETI 2016 -2020 de la entidad.

9 PLAN DE TRABAJO

Las actividades definidas en el plan de seguridad y privacidad de la información que dan alcance conforme al Plan Distrital de Desarrollo 2016 -2020 "Bogotá Mejor para Todos" se encuentran en el Anexo publicado a continuación:

Proyectó: Carlos Rojas Villamil

Elaboró: Carlos Rojas Villamil

Revisó: Luis Fernando Arango Vargas, Isaías Sánchez Rivera.

Aprobó: Julio Alexander Hernández Martínez

Código de archivo:

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE MODIFICACIÓN**
2	06/02/2019	Se realizó ajustes en el contenido del plan, así como en el logro de las actividades realizadas durante el año 2018 y en el plan de trabajo para la vigencia 2019.

PLAN DE TRABAJO MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN																															
FASE	ACTIVIDAD	2016	2017	2018												2019												MEDICION Y SEGUIMIENTO		
				Feb	MAr	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun	Jul	Agos	Sep	Oct	Nov	Dic	Indicador	Medición por	Medición - Avance -FASE
PLANIFICACION	Establecer Política de Seguridad de la Información																										Actividades ejecutadas / Actividades Prgrmadas	1	75.79%
	Establecer manual de gestión de Seguridad de la Información																											1	
	Actualizar el manual de seguridad de la información																											1	
	Actualizar la política de seguridad de la información del DADEP																											1	
	Validar seguridad en aplicaciones de la Entidad																											1	
	Establecer roles y responsabilidades al interior del DADEP																											1	
	Definir guía e instrumento para el levantamiento y clasificación de activos de																											1	
	Realizar levantamiento y clasificación de activos de información																											1	
	Establecer contexto de los riesgos de seguridad de la información																											1	
	Identificar riesgos de seguridad de la información																											0.1	
	Realizar análisis de riesgos de seguridad de la información																											0	
	Realizar evaluación de los riesgos de seguridad de la información																											0	
	Establecer declaración de aplicabilidad																											0	
	Diseñar el programa de sensibilización y capacitación																											1	
	Diseñar el plan de sensibilización y capacitación de sensibilización y capacitación en seguridad de la información																											1	
	Definir herramientas para el programa de sensibilización y capacitación en seguridad de																											1	
	Implementar el programa de sensibilización y capacitación en seguridad de la información																											0.3	
	Establecer y documentar procedimientos de seguridad de la información																											1	
	Definir guía para la gestión de eventos e incidentes de seguridad de la información																											1	
IMPLEMENTACION	Implementar plan de tratamiento de riesgos de seguridad de la información																										Actividades ejecutadas / Actividades Prgrmadas	0	6.00%
	Establecer el plan de contingencias de los sistemas de información y servicios de TI																											0.3	
	Definir componentes para la continuidad del negocio																											0	
	Realizar análisis de impacto del negocio																											0	
	Implementar transición Protocolo IPV4 - IPV6																											0	
EVALUACIÓN DE DESEMPEÑO	Realizar plan de seguimiento y revisión de la efectividad de la implementación del MSPI.																										Actividades ejecutadas / Actividades Prgrmadas	0	8.00%
	Ejecución de auditorías																											0.4	
	Medir la efectividad de los controles y políticas definidas																											0	
	Revisar los niveles de riesgos.																											0	
	Actualizar los planes entorno a la seguridad de la información																											0	
MEJORA CONTINUA	Desarrollar plan de mejora continua																										Actividades ejecutadas / Actividades Prgrmadas	0.1	15.00%
	Gestionar las comunicaciones																											0.2	