ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA GENERAL

ALCALDIA MAYOR DE BOGOTA - SECRETARIA GENERAL
Rad. No.: 2-2017-25699
Fecha: 22/11/2017 10:36:47
Destino: SECRETARIOS DE DESPACHO
Copia: N/A
Anexos: N/A

CIRCULAR N°. 036

Para: **SECRETARIOS(AS) DE DESPACHO**

De: **ALTA CONSEJERÍA DISTRITAL DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES**

Asunto: **LINEAMIENTOS DE AVANCE IMPLEMENTACION MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION**

En complemento a la Circular 001 del 13 de enero de 2017, en la cual se establece el plan de trabajo para cumplir con los porcentajes de avance requeridos en el Decreto 1078 de 2015, para las entidades de carácter territorial, es de vital importancia definir el plan de trabajo de implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, para lo que la Alta Consejería Distrital de TIC recomienda tener en cuenta los siguientes ítems a fin de avanzar en la consecución del avance esperado para el cierre del año:

FASE	ENTREGABLE	CARACTERÍSTICAS MÍNIMAS
Planificación	**1**. Política de Seguridad y Privacidad	Evaluar la Política de Seguridad de la Información de la Entidad: ✓ Si Se definen los Objetivos, Alcance de la Política. ✓ Si se encuentra alineada con la estrategia y objetivos de la entidad. ✓ Si fue debidamente aprobada y socializada al interior de la entidad por la alta dirección.
	2. Manual de Políticas	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
	3. Acto administrativo	Solicitar el Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (ó e que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección.

FASE	ENTREGABLE	CARACTERÍSTICAS MÍNIMAS
Planificación	**4**. Metodología de Gestión de Riesgos.	La entidad debe tener clara y documentada la metodología y criterios de riesgo de seguridad, aprobado por la alta Dirección que incluya: ✓ Criterios de Aceptación de Riesgos o tolerancia al riesgo que han sido informados por la alta Dirección. ✓ Criterios para realizar evaluaciones de riesgos.
	5. Análisis y evaluación de Riesgos (Aplicación de la Metodología)	Solicitar a la entidad los resultados de las evaluaciones de riesgos y establecer: ✓ Cuantas evaluaciones repetidas de riesgos se han realizado y que sus resultados sean consistentes, válidos y comparables. ✓ Que se hayan identificado los riesgos asociados con la pérdida de la confidencialidad, de integridad y de disponibilidad de la información dentro del alcance. ✓ Que se hayan identificado los dueños de los riesgos. ✓ Que se hayan analizado los riesgos es decir: - Evaluado las consecuencias (impacto) potenciales si se materializan los riesgos identificados - Evaluado la probabilidad realista de que ocurran los riesgos identificados - Determinado los niveles de riesgo. ✓ Que se hayan evaluado los riesgos es decir: - Comparado los resultados del análisis de riesgos con los criterios definidos - Priorizado los riesgos analizados para el tratamiento de riesgos.

FASE	ENTREGABLE	CARACTERÍSTICAS MÍNIMAS
Planificación	**6**. Plan de Tratamiento de Riesgos	El plan de tratamiento de riesgos y la declaración de aplicabilidad, entre otros cumplirá con : ✓ Selección de opciones apropiadas para tratar los riesgos, teniendo en cuenta los resultados de la evaluación de riesgos. ✓ Determinar todos los controles necesarios para implementar las opciones escogidas para el tratamiento de riesgos. ✓ Comparación de los controles determinados en el plan de tratamiento con los del Anexo A y verifique que no se han omitidos controles, si estos han sido omitidos se debe reflejar en la declaración de aplicabilidad. ✓ Revisar la Declaración de Aplicabilidad que tenga los controles necesarios y la justificación de las exclusiones, ya sea que se implementen o no y la justificación para las exclusiones de los controles del Anexo A, y que haya sido revisado y aprobado por la alta Dirección. ✓ Revisar que el plan de tratamiento de riesgos haya sido revisado y aprobado por la alta Dirección. ✓ Revisar que exista una aceptación de los riesgos residuales por parte de los dueños de los riesgos. El anexo A, donde se mencionan los controles para la implementación de seguridad de acuerdo con el Estándar ISO 27001 puede ser consultado en la pagina del MinTIC www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf
	7.Inventario de activos de información	Es necesario que en la entidad se comprometan a realizar el Inventario de activos de Información, revisado y aprobado por la alta Dirección y de este validar : ✓ Ultima vez que se actualizó. ✓ Mencionar la importancia del activo. ✓ Señalar el propietario del activo Dicha clasificación debe estar alineado con la Ley 1712 de 2014 medio de la cual se crea la Ley de Transparencia

FASE	ENTREGABLE	CARACTERÍSTICAS MÍNIMAS
Planificación	**8**. Plan de Comunicaciones	Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo. Se debe tener evidencia probatoria de este cumplimiento.
	9. Inventario de Activos IpV6	El Plan de diagnóstico de la Entidad contendrá mínimo los siguientes componentes: ✓ Inventario de TI (Hardware y software) ✓ Informe de la Infraestructura de red de comunicaciones ✓ Recomendaciones para adquisición de elementos de comunicaciones , cómputo y almacenamiento con el cumplimiento de IPv6 ✓ Plan de direccionamiento en IPv6 ✓ Plan de manejo de excepciones Se debe tener en cuenta la Resolución 2710 de 2017, por la cual se establecen los lineamientos para la adopción del protocolo IPv6 y que puede ser consultado en la pagina del MinTIC http://mintic.gov.co/portal/604/w3-article-61000.html
Implementación	**1**. Planificación y Control Operacional	Es importante que en la entidad se cuente con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.
	2. Implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad	Verificar que los compromisos de avance en el plan de tratamiento de riesgos y el grado de cumplimiento de los mismos y genere un dato con el porcentaje de avance.
	3. Plan de transición IpV4 a Ipv6	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de seguridad y privacidad de la información e infraestructura de red de comunicaciones

		(IPv4/IPv6), revisado y aprobado por la alta dirección. Se debe tener en cuenta la Resolución 2710 de 2017, por la cual se establecen los lineamientos para la adopción del protocolo IPv6 y que puede ser consultado en la pagina del MinTIC http://mintic.gov.co/portal/604/w3-article-61000.html
	4. Indicadores de Gestión	Es importante que en la entidad se cuente con los Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.

Por tanto, la Alta Consejería TIC, acorde con sus funciones establecidas en el Decreto 425 de 2016 en su Artículo 8. Funciones de la Oficina de Alta Consejería Distrital de Tecnologías de Información y Comunicaciones –TIC–. Entre otras las de Asesorar a los sectores y entidades del Distrito Capital en la formulación de los planes, programas y proyectos institucionales relacionados con la implementación de la política distrital en TIC y articular las diferentes instancias involucradas en la ejecución de los mismos., estará atenta a recibir vía email al correo estrategiagelbogota@alcaldiabogota.gov.co y con copia a mpnino@alcaldiabogota.gov.co, el avance frente a la etapa de planificación y los planes para la etapa de implementación, de acuerdo con las recomendaciones anteriormente mencionadas y según la hoja de ruta propuesta.

La Fecha de entrega de dicha información tiene como plazo máximo el 15 de Diciembre del año 2017. La hoja de ruta se adjunta como anexo a dicha circular.

De antemano agradecemos su respuesta a esta circular y su decisión de participar en este ejercicio que redunda en el fortalecimiento de la gestión en las entidades distritales.

Cordialmente,

SERGIO MARTÍNEZ MEDINA
Alto Consejero Distrital de TIC

Anexos: 1 Folio
Proyectó: María del Pilar Niño Campos.
Revisó: Iván Mauricio Hernández Lanao

ACCIONES						HERRAMIENTAS
1.		Definición del Líder Oficial Seguridad de la informacion y empoderamiento				
	1,1	Definición de responsabilidades				Guía No 4. Roles_responsabilidades
2.		Garantizar el compromiso de la alta dirección				
3.		Determinar la política y alcances de la seguridad de la información				Guia No 2. Politica_General
	3.1	Objetivos y metas lo más concretos posible en materia de seguridad.				
4.		Definir estado actual de al información		4X.	Definir estado de madures de los controles existentes	Diligenciamiento de la herramienta de Diagnostico de Mintic
	4.1	Determinación de Procesos y Procedimientos		4X.1	Determinación de Procesos y Procedimientos	
5.		Definir el método para evaluar los riesgos				
	5.1	Recursos a utilizar y activos a evaluar				Guia No 5. Gestion_Clasificacion de los activos
	5.2	Definir acciones y objetivos para gestionar los riesgos				Guia No 7. Gestion_Riesgos
	5.3	Identificar, analizar y evaluar los riesgos				Guia No 8. Controles_Seguridad
	5.4	Indicadores de Gestion				Guia No. 9. Indicadores_Gestion_Seguridad
6		Análisis de vulnerabilidades				Guía No 1. Metodologia_pruebas_efectividad
7		Procedimientos de seguridad y privacidad de la información.				Guia No 3. Procedimiento_de_Seguridad
8		Integración del mspi, con el sistema de gestión documental de la entidad.				Guia No 6. Gestion_Documental
9		Plan de comunicaciones.				Guía No 14. Plan_comunicacion_sensibilizacion
10		Medición de indicadores de gestión				Guía No 19. Indicadores_Gestion_Seguridad
11		Plan de transición de ipv4 a ipv6.				Guia No 20. Transicion_IPv4_IPv6 / Guía No 19 . Aseguramiento del Protocolo IPv6.
12		Auditoría interna, revisión del proceso y mejoras				Guia No 15. Guía de Auditoría. /Guía No 16. evaluaciondesempeno / Guía No 17 .Mejora Continua