CONTROL DE CAMBIOS		
VERSIÓN[1]	**FECHA**	**DESCRIPCIÓN DE LA MODIFICACIÓN**
1	30 de agosto de 2009	Primera versión del documento
2	14 de Junio de 2011	Modificación del formato, propósito e instrucciones
3	13 de Marzo de 2013	Modificación de las instrucciones
01	28 de noviembre de 2017	Se realiza ajuste de normalización como consecuencia de la entrada en vigencia de la resolución 162 de 2017, que crea el proceso Gerencia de TIC como parte del mapa de procesos de la entidad, y en cumplimiento de lo establecido en la circular 16 del 1 de noviembre de 2017. Los lineamientos operativos descritos en este documento, corresponden íntegramente a los aprobados en la versión 3 de fecha 13 de marzo de 2013, la cual fue aprobada por Martha Patricia Jiménez Rodríguez, Subsecretaría de Planeación y Gestión como líder del proceso Gestión y Adquisición de Recursos, vigente en ese momento.

1

1. INFORMACIÓN GENERAL

Propósito del Instructivo:

Brindar soporte técnico especializado para realizar el monitoreo de la Infraestructura de Red de Datos de la Secretaria Distrital de Gobierno de manera eficiente, a través de herramientas tecnológicas y recurso humano calificado, con el fin de garantizar la disponibilidad de red de la Entidad.

Responsable:

Dirección de Planeación y Sistemas de Información

2. INSTRUCCIONES:

Para el cumplimiento del propósito del presente Instructivo, es necesario tener en cuenta los siguientes lineamientos así:

La Secretaría Distrital de Gobierno, cuenta con herramientas de monitoreo con el propósito de verificar el funcionamiento de su plataforma de red de datos. Las características a monitorear son:

- ➔ Equipos Activos (switch, Router, Firewalls),
- ➔ Consumo de ancho de banda,
- ➔ Análisis de vulnerabilidades.

Equipos Activos: Todos los enlaces son verificados en intervalos de tiempos configurables, los cuales permiten validar la disponibilidad acordado con el proveedor de servicios de conectividad. Una vez la herramienta detecta una caída de los equipos de la red WAN (routers), esta es identificada por el proveedor e informada al primer nivel del grupo de seguridad perimetral y networking.

Durante este estado, el primer nivel del grupo deberá verificar si la causa de la caída es física o de energía. Si la causa es identificada y puede ser resuelta por primer nivel, se procede a cerrar y documentar el incidente. De lo contrario, este será escalado al segundo nivel del grupo y se inicia la comunicación con el proveedor, el cual deberá verificar si la falla es de tipo configuración. Esta actividad se realiza en conjunto con el proveedor de dicho servicio, responsable de corregir la falla de tipo configuración básica, si el caso es resuelto, se procede a cerrar y documentar el incidente. De lo contrario deberá ser escalado a tercer nivel que es el proveedor del servicio de mantenimiento quienes son responsables de corregir fallas de configuración avanzada.

Consumo de Ancho de Banda

El consumo es monitoreado y comparado con los umbrales de saturación, dependiendo de dicho nivel, se genera o no la alerta que permite iniciar el proceso de validación por parte de los profesionales del grupo de Infraestructura Tecnológica encargados de dicha labor.

Análisis de Vulnerabilidades

Mensualmente se genera un análisis de vulnerabilidades de los servidores, servicios y bases de datos, con el propósito de identificar fallas de seguridad, desactualización de la plataforma, entre otros. Una vez identificada la vulnerabilidad, se reporta al grupo responsable para que el incidente sea resuelto.

3. DOCUMENTOS DEL SIG

CÓDIGO	DOCUMENTO
N/A	No aplica.