ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA GENERAL

ALCALDÍA MAYOR DE BOGOTÁ - SECRETARÍA GENERAL
Rad. No.: 2-2017-23676
Fecha: 30/10/2017 12:24:49
Destino: SECRETARÍAS DE DESPACHO
Copia: N/A
Anexos: 1 FOLIO

CIRCULAR N°. 030

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

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

Asunto: **IMPLEMENTACIÓN CSIRT DE GOBIERNO.**

Los CSIRT (Computer Security Incident Response Team), son aquellos equipos que se encargan de gestionar eventos e incidentes de seguridad, entre otras cosas. Su razón de ser fundamentalmente es disminuir el impacto de una actividad maliciosa que atente contra la disponibilidad, integridad, confidencialidad de la información de la entidad.

El Ministerio TIC, en el marco de la Estrategia GEL, la implementación del Modelo de Seguridad y Privacidad de la Información, así como lo expuesto en los Conpes 3701 de 2011 y 3854 de 2016, decide poner en marcha el proyecto de implementación del CSIRT de Gobierno, el cual tendrá como objetivo el monitoreo de servicios de las entidades del estado de nivel nacional y territorial. Dicha implementación conlleva unas fases en las cuales se prestarán los primeros servicios del catálogo y se llevara a cabo el monitoreo de un primer grupo de entidades; es así como también se necesita generar capacidades de gestión de incidentes en las entidades.

Siendo así, y dada la gestión adelantada entre la Alta Consejería Distrital de TIC, y el Ministerio TIC, estamos interesados en contar con su entidad, como cabeza de sector para incluirla en el grupo de entidades que serán monitoreadas a fin de apalancar el tema de gestión de incidentes de seguridad al interior del distrito.

Por esto se requiere que la entidad verifique que cumple con los siguientes requerimientos:

- Un dispositivo perimetral que tenga la capacidad de hacer conexiones VPN Site to Site a través de IPSEC.

- Compromiso por parte de la entidad, respecto a la delegación de dos servidores públicos competentes para ser capacitados en gestión de incidentes, con el fin de ser los primeros respondientes ante un evento o un incidente en el cual se vea afectada la entidad. Dicha capacitación estará dada por los actores del convenio MinTIC – Policía Nacional.

Es de vital importancia cumplir con los requerimientos antes citados para el éxito de esta labor. Las dudas que se generen frente a este tema, serán resueltas en mesas de trabajo transversales en las cuales se definirán los servicios que serán monitoreados.

Cabe resaltar que esta actividad se pretende iniciar en conjunto con Ministerio TIC lo antes posible, por lo que requerimos de su respuesta a la mayor brevedad.

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: un (1) folio.

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

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

MINTIC

Código TRD: **330**

Bogotá, octubre 2017

MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
FECHA: 6/10/2017 HORA: 11:48:31 FOLIOS:
REGISTRO NO: **1094518**
DESTINO: USUARIOS OTI

Señor(a);
Director(a) de OTI.
La ciudad.

Asunto: **Implementación CSIRT de Gobierno.**

Un muy cordial y respetuoso saludo, como es de su conocimiento los Equipos de Respuesta a Incidentes de Seguridad Informática, denominados CSIRT (*Computer Security Incident Response Team*), son aquellos equipos que se encargan de gestionar y resolver eventos e incidentes de seguridad centrando sus acciones en disminuir el impacto de una actividad maliciosa que atente contra una entidad del estado.

El Ministerio TIC lidera la iniciativa para poner en marcha el proyecto de implementación del CSIRT de Gobierno, el cual tendrá como objetivo el monitoreo de servicios de las entidades del estado a nivel nacional y territorial. Esta implementación conlleva unas fases en las cuales se prestarán los primeros servicios del catálogo y se llevará a cabo el monitoreo de un primer grupo de entidades generando capacidades estratégicas y operativas para la gestión de los posibles incidentes.

En razón de lo anteriormente expuesto y con el fin de ser los primeros respondientes ante un evento o un incidente en el cual se participe su entidad, se requiere la verificación de cumplimiento de los siguientes requerimientos:

1. La entidad debe disponer de un dispositivo perimetral que tenga la capacidad de hacer conexiones *VPN site to site* a través de *ipsec*.
2. Delegue a dos servidores públicos competentes en seguridad informática para que reciban capacitación en gestión de incidentes. La referida capacitación será impartida por los actores del convenio MinTIC – Policía Nacional.

Agradecemos su respuesta formal a esta comunicación en el menor tiempo posible.

Atentamente,

ELIZABETH BLANDON BERMUDEZ
DIRECTORA DE GOBIERNO DIGITAL

Proyecto/Reviso:
RAFAEL LONDOÑO CARANTON
Subdirector de Estándares y Arquitectura de TI.
ANTONIO CARRILLO ROSAS
Coordinador Seguridad Digital
JULIO CESAR MANCIPE
Asesor Gobierno Digital