SUPERINTENDENCIA FINANCIERA DE COLOMBIA

CARTA CIRCULAR 65 DE 2019
(Octubre 02)

Señores
REPRESENTANTES LEGALES, MIEMBROS DE JUNTA DIRECTIVA, REVISORES FISCALES, OFICIALES DE CUMPLIMIENTO, FUNCIONARIOS RESPONSABLES Y CONTRALOR NORMATIVO DE LAS ENTIDADES SUPERVISADAS.

Referencia: Mecanismos que fortalecen la colaboración en la gestión de incidentes cibernéticos

Apreciados señores:

Con el propósito de continuar fortaleciendo la gestión de la seguridad de la información y la ciberseguridad de las entidades vigiladas, esta Superintendencia pone a su disposición la siguiente información:

1. El Gobierno Nacional cuenta con el Centro de Capacidades para la Ciberseguridad de Colombia (C4), dotado con el primer laboratorio para el análisis de malware, que identifica el código malicioso, formula recomendaciones para su tratamiento y recuperación, adelanta investigaciones, realiza análisis forense y reporta alertas, servicios que pueden ser de ayuda en caso de materializarse un incidente cibernético. Adicionalmente, el C4 cuenta con una gran base de datos de llaves de ciframiento y el apoyo técnico de expertos del Centro Europeo Contra el Cibercrimen (EC3) de Europol (Oficina Europea de Policía) que le podrían permitir descifrar los archivos infectados por un ataque de *ransomware* (secuestro de datos) sin tener que aceptar las pretensiones del ciberdelincuente.

   Los servicios mencionados se prestan sin ningún costo. Para mayor información se pueden comunicar con el centro cibernético policial en el teléfono 5159727, en la ciudad de Bogotá, e ingresar la información correspondiente al caso en el siguiente enlace:

   https://caivirtual.policia.gov.co/contenido/#contactenos

   En desarrollo de esta iniciativa de colaboración el C4 está recopilando llaves de descifrado que pudieran servirle a otras organizaciones, por lo tanto, si su entidad cuenta con algunas de ellas, puede remitirlas al correo electrónico

caivirtual@policia.gov.co con el asunto [NO MORE RANSOMWARE COLOMBIA] y de esta manera contribuir a esta campaña o, puede contactar a los responsables de administrar dichas llaves en el teléfono indicado anteriormente.

2. La iniciativa internacional de Europol denominada "*No More Ransom*", que tiene como objetivo principal compartir conocimiento y educar a los usuarios sobre la manera como se pueden prevenir los ataques de ransomware, cuenta con varias herramientas gratis de descifrado para distintos tipos de malware. En el sitio web https://www.nomoreransom.org podrá consultar información al respecto, en la pestaña denominada "*Herramientas de descifrado"*.

Cordialmente,

MIGUEL ÁNGEL VILLALOBOS HERNÁNDEZ
Superintendente Delegado para Riesgos Operativos
530000