Bogotá, 4 de mayo de 2021

Alerta de seguridad

Asunto: **Alerta sobre difusión de amenazas de ataques cibernéticos**

Esta información se deriva de la Activación PMU CIBER por parte de 07 entidades gubernamentales (• Presidencia de la República (Csirt Presidencia) • Ministerio de Defensa (ColCERT) • Ministerio de Comunicaciones (CSIRT Gobierno) • Fiscalía General de la Nación • Fuerzas Militares (CCOCI) • Policía Nacional (Centro Cibernético, DIPOL, DIPRO, POLFA, CSIRT PONAL) • Dirección Nacional de Inteligencia), en el marco del desarrollo de las protestas sociales que se están llevando a cabo desde el 28 de abril de 2021.

Se han identificado en algunas redes sociales publicaciones que incitan a ejecutar ataques a las entidades públicas con el fin de afectar la confidencialidad e integridad de la información relacionada con los datos personales de los ciudadanos que son tratados en las diferentes entidades, por lo cual se ha establecido un estado de alerta para prevenir la materialización de esta amenaza.

Por lo anterior, es importante identificar posibles vectores de ataque y/o solicitar bloqueo o borrado de estos mensajes, o cuentas y estar en constante monitoreo de servicios.

Se recomienda denunciar en redes sociales estas publicaciones con el fin de que estas puedan ser baneadas y así evitar su propagación.

Aconsejamos tener en cuenta las siguientes recomendaciones:

1. Robustecer los protocolos de seguridad de los sistemas de información con el fin de contrarrestar situaciones que pongan en riesgo la disponibilidad, la integridad y la confidencialidad de la información.

2. Aumentar monitoreos a todos los sistemas de información y operación.

3. Revisar las políticas de backup de los sistemas críticos y realizar las pruebas sobre estos backup, con el fin de comprobar que serán funcionales para recuperarse ante un incidente

4. Realizar bloqueos de peticiones sospechosas, establecer umbrales máximos (números de peticiones, tiempo, recurrencia, ubicación geográfica)

5. Implementar doble factor de autenticacion sobre la infraestructura de TI y sistemas críticos especialmente expuestos en Internet.

6. Realizar un monitoreo constante de las acciones realizadas con los usuarios con rol de administrador y super administrador sobre la infraestructura de TI y sistemas críticos especialmente expuestos en Internet.

7. Realizar procedimientos de hardening y revisar el uso e instalación de las últimas versiones y parches de seguridad.

8. Realizar análisis de vulnerabilidades y pruebas de seguridad sobre los activos de información críticos.

9. Revisar los procedimientos de continuidad de la operación y realizar simulacros de situaciones reales, para evaluar la idoneidad y puntos de mejora.

Por último, contar con una Estrategia de Seguridad Digital y su correspondiente procedimiento de Gestión de Incidentes que contemple este tipo de ataques lineados con el Plan de Seguridad de la Información.

POR FAVOR, EN CASO DE ESTAR REALIZANDO ALGÚN MANTENIMIENTO EN LOS PORTALES WEB, se recomienda habilitar un banner indicando que se encuentran efectuando dicho mantenimiento.

En caso de ser necesario puede comunicarse con CSIRT Gobierno por medio de los siguientes canales:

Csirtgob@mintic.gov.co **+1 5159728 o 018000910742 opción 4.**