Gobernación de NARIÑO | Secretaría TIC Innovación y Gobierno Abierto

CIRCULAR No. STIC-004-2025

DE: Secretaría TIC, Innovación y Gobierno Abierto

PARA: Funcionarios y Contratistas Gobernación de Nariño

ASUNTO: Socialización Procedimiento Gestión de Incidentes de Seguridad Digital

FECHA: 11 de marzo de 2025

En el marco de la Política de seguridad y privacidad de la Información, la Secretaría TIC socializa el PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL, que tiene como propósito identificar, analizar, contener, erradicar y prevenir incidentes de seguridad relacionados con la pérdida de Confidencialidad, Integridad y Disponibilidad de la información en la Gobernación de Nariño.

Un Incidente de Seguridad Digital, es un evento adverso, acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de un activo de información, que constituye una amenaza de violación de una política de seguridad de la información, y que puede tener impacto en la operación normal de la entidad afectando el funcionamiento de las redes, sistemas y demás recursos tecnológicos, así como la pérdida de disponibilidad, integridad y confidencialidad de la información.

Por lo anterior, se requiere que los funcionarios y contratistas de la Gobernación de Nariño, reporten la ocurrencia de incidentes de seguridad digital a la Secretaría TIC, con el fin de que se realice el procedimiento necesario para su contención y erradicación según sea el caso.

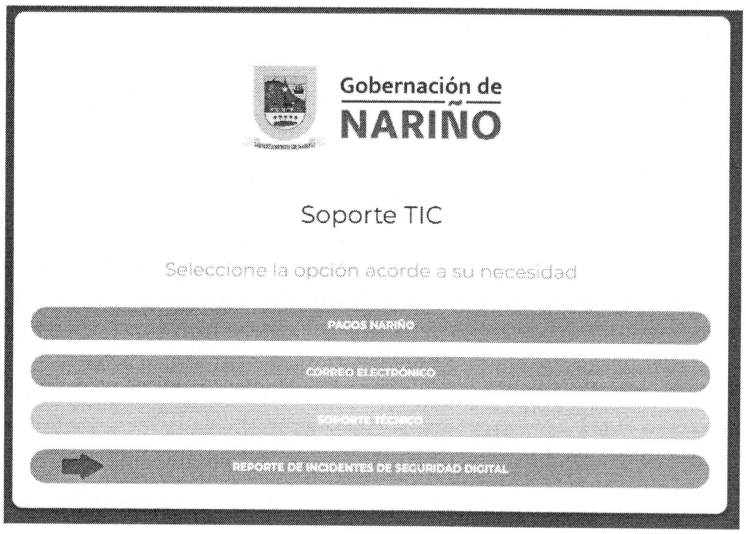
Para el reporte de incidentes se debe diligenciar el Formulario dispuesto en la Intranet, en el menú SOS TIC / REPORTE DE INCIDENTES DE SEGURIDAD DIGITAL:

https://docs.google.com/forms/d/e/1FAIpQLSfIKWcqPjcn63dMtX5tfDdUzpDM2xgHRCcWIpMKhnjse7yscw/viewform?vc=0&c=0&w=1&flr=0

Tener en cuenta la identificación de los siguientes eventos que se consideran incidentes de seguridad digital para su reporte a TIC:

1. Correos electrónicos desconocidos y sospechosos.
2. Premiación engañosa, oferta de premios, concursos en los que nuca te inscribiste, suelen ser intento de fraude.
3. Anuncios inesperados, anuncios emergentes o pop-ups fuera de lo común, incluso cuando no estás navegando en internet.
4. Páginas de inicio Modificadas, si el navegador redirige a sitios web desconocidos o cambian la página de inicio sin su consentimiento.
5. Programas o archivos bloqueados, algunos virus pueden bloquear el acceso al antivirus o programas de seguridad para evitar ser detectados.
6. Fuga, pérdida o robo de información digital.

7. Información cifrada o dañada.
8. Cambio de extensión en archivos.
9. Modificación no autorizada de la información.
10. Suplantación de identidad.
11. Acceso no autorizado a sistemas e información.
12. Pérdida o alteración de registros de base de datos.
13. Pérdida de un activo de información (servidor, equipo de cómputo, dispositivo de red, unidades de almacenamiento).
14. Uso indebido de imagen institucional.
15. Denegación del servicio (suspensión de algún servicio de tecnología).
16. Rendimiento lento del equipo de cómputo.
17. Actividad de red extraña, conexión a internet más lenta de lo normal.
18. Secuestro de información y cobro por rescate.
19. Alertas en software antivirus.
20. Alertas en equipos firewall de seguridad.
21. Caída de servidores.
22. Uso indebido de permisos por parte de usuarios en los sistemas de información.
23. Aumento inusual en el tráfico de la red.
24. Existencia de programas y archivos desconocidos.



JONNATHAN HUERTAS SALAS
Secretario TIC, Innovación y Gobierno Abierto
Gobernación de Nariño

Proyectó: Patricia Martínez Solarte
Profesional Universitaria SecTIC