1. Objetivo.

Establecer las acciones necesarias que permitan 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, sede central y sedes asociadas.

2. Alcance.

El procedimiento inicia con la identificación de un incidente, continúa con la detección y análisis, contención, erradicación y finaliza con la recuperación o solución del incidente. El procedimiento aplica para todas las áreas de la Gobernación de Nariño en la sede central y sedes asociadas.

3. Definiciones.

Activo de Información: Es todo aquello que representa valor para la Gobernación de Nariño, hardware, software, información, servicios y personas.
Amenaza: Posibilidad de ocurrencia de cualquier tipo de evento que puede producir un daño grave a un sistema o activo de información. Una amenaza puede suceder o no.
Atención de incidentes de seguridad: Procesos y tecnologías disponibles en la Gobernación de Nariño para detectar y resolver los incidentes de seguridad de acuerdo con los procedimientos establecidos.
Confidencialidad: Principio fundamental de la seguridad de la información que garantiza el necesario nivel de secreto de la información y de su tratamiento, para prevenir su divulgación no autorizada.
Contención de un incidente: Son todas aquellas actividades encaminadas a reducir el impacto inmediato de un incidente de seguridad de la información.
CSIRT Gobierno: Equipo de Respuesta a Incidentes de Seguridad. brinda acompañamiento y apoyo a las entidades del estado, a través de su portafolio de servicios, con el fin de mejorar los procesos de seguridad de la infraestructura tecnológica, la gestión de los incidentes cibernéticos y generación de conciencia en seguridad digital.
Detección de incidentes de seguridad: Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información.
Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando sea requerida por un individuo, entidad o procesos autorizados.
Evento: Ocurrencia o cambio de un conjunto particular de circunstancias.
Incidentes Seguridad de la Información: Es un evento adverso que atenta contra los principios fundamentales de la seguridad como son: la disponibilidad, confidencialidad e integridad, así mismo es alguna violación o inminente amenaza de violación de una política de seguridad de la información.
Integridad: Propiedad de la información relativa a su exactitud y completitud.
Mesa de Servicios: Es un conjunto de servicios que ofrece la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral.
Recolección y análisis de evidencia digital: Toma, preservación, documentación y análisis de evidencia cuando sea requerida.
Riesgo de seguridad informática: Es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o eliminar.
Vulnerabilidad: Debilidad del hardware o software (sistemas, equipos de cómputo, servidores, sistema operativo, sistemas de información, aplicaciones, redes), que puede ser aprovechado con el fin de ocasionar daño o extraer información confidencial y datos personales.

4. Desarrollo del documento.

4.1 Condiciones y/o políticas específicas de operación

4.1.1 Los posibles incidentes de seguridad y/o eventos se reportarán por medio de la Mesa de Ayuda y/o formulario de reporte de incidentes de seguridad establecidos por la Secretaría TIC, diligenciando la información correspondiente y adjuntando evidencias del posible incidente como capturas de pantalla, correos electrónicos, registro fotográfico, video, etc.

4.1.2 Criterios para considerarse incidente:

a. Pérdida o daño de información física o digital.
b. Fuga y/o robo de información física o digital.
c. Modificación no autorizada de la información.
d. Suplantación de identidad.
e. Acceso no autorizado.
f. Pérdida o alteración de registros de base de datos.
g. Pérdida de un activo de información.
h. Código malicioso “malware, ransomware”.
i. Denegación del servicio.
j. Ciberataque.
k. Uso indebido de imagen institucional.
l. Suspensión de algún servicio de tecnología.

4.2 Descripción de Actividades

No	Actividad	Descripción de la actividad	Documento de trabajo	Responsable
1	Reportar incidentes	Reportar los presuntos incidentes de seguridad de la información a través del sistema Mesa de Ayuda y/o formulario de reporte de incidentes de seguridad, teniendo en cuenta lo descrito en el numeral 4.1.1. Mesa de Ayuda: https://soportetic.narino.gov.co/app/dashboard/inicial	Registro en la Mesa de Ayuda, en el Formulario Reporte de Incidentes de Seguridad	Funcionarios Contratistas Proveedores
2	Validar el incidente reportado	Recibido el reporte del posible Incidente o del evento de seguridad, el equipo técnico para la gestión de incidentes debe establecer si cumple con alguno de los criterios para ser considerado un incidente, definidos en el numeral 4.1.2.	Formato Reporte de incidentes de seguridad digital	Personal de soporte encargado de la gestión de incidentes en la Secretaría TIC

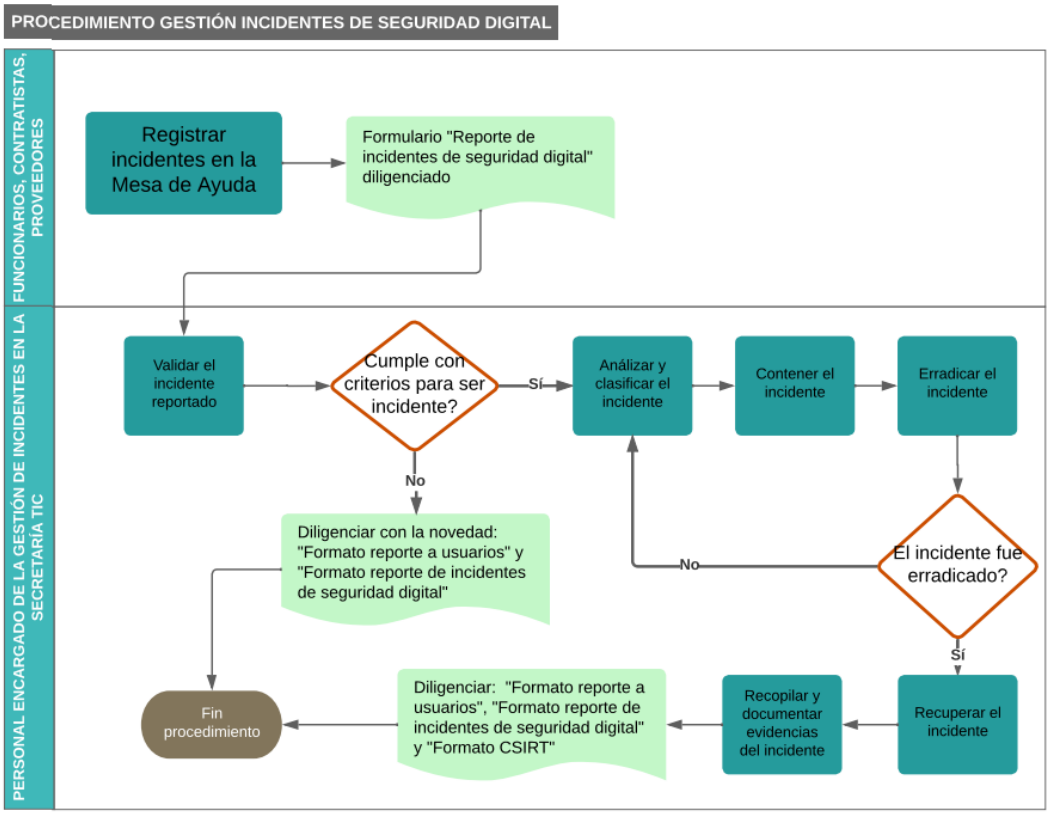
		¿Cumple con criterios para ser incidente? **SI:** Pase a la actividad **3** **NO:** Termina el procedimiento registrando la novedad en el formato establecido en la Mesa de Ayuda.		
3	Analizar y Clasificar el incidente	El equipo Técnico encargado de la gestión de incidentes en la Secretaría TIC, recopila y analiza toda la información disponible del incidente, respaldándose en la categorización del riesgo en los activos de información y clasifica el criterio de incidente afectado (numeral 4.1.2) y establece la criticidad del incidente según la severidad: - **Alto Impacto**: Afecta activos de información de impacto catastrófico y mayor, que influyen con los objetivos misionales de la Gobernación. Se incluyen aquellos incidentes que afectan la reputación y el buen nombre o involucren aspectos legales. - **Medio Impacto**: Afecta activos de información de impacto moderado, que influye en los objetivos de un proceso determinado. - **Bajo Impacto**: Afecta activos de información de impacto menor, que no influyen en ningún objetivo. Deben ser monitoreados.	Formato Reporte de incidentes de seguridad digital	Personal de soporte encargado de la gestión de incidentes en la Secretaría TIC
4	Contener el incidente	El Equipo Técnico responsable de la gestión de incidentes en la Secretaría TIC, aplicará estrategias definidas para evitar la propagación del incidente y disminuir los daños que pueda ocasionar teniendo como base toda la información recolectada en la actividad 3. Entre las estrategias, se tienen: ● Bloqueo de cuentas de usuarios. ● Apagado del sistema para accesos no autorizados.	Formato Reporte de incidentes de seguridad digital	Personal encargado de la gestión de incidentes en la Secretaría TIC

		● Desconexión de la red del equipo afectado con código malicioso. ● Detener procesos sospechosos. ● Bloqueo de puertos ● Aislar sistemas afectados en una subred segura ● Aplicar restricciones temporales en accesos ● Monitorear los sistemas comprometidos		
5	Erradicar el incidente	Después de que el incidente ha sido contenido se debe realizar las siguientes acciones con el fin de erradicar el incidente: ● Identificar la causa raíz del incidente para identificar vulnerabilidades, malware y error humano, que permitieron el ataque. ● Eliminar cualquier rastro del incidente: limpiar malware, cerrar brechas de seguridad, aplicar parches o actualizaciones, eliminar archivos sospechosos. ● Verificar la integridad de la información (bases de datos, aplicaciones, etc.). ● Realizar copia de seguridad de la información si fuera necesario. ● Reinstalar software legítimo si fue comprometido. ● Restaurar la configuración de seguridad en los sistemas afectados. ● Instalar parches de seguridad y actualizar software, sistemas operativos y dispositivos de red. ● Verificar que todos los sistemas tengan las últimas versiones de sus aplicaciones críticas y seguridad. **¿El incidente fue erradicado?** **SI**: Pase a la actividad 6 **NO**: Vaya a actividad 3	Formato Reporte de incidentes de seguridad digital	Personal encargado de la gestión de incidentes en la Secretaría TIC
6	Recuperar el Incidente	Una vez erradicado el incidente, se procede a la recuperación a través de:	Formato Reporte de incidentes de seguridad digital	Personal encargado de la gestión de incidentes en la

		● Reconectar de forma gradual los dispositivos afectados a la red tras realizar evaluaciones de seguridad exhaustivas para confirmar que ya no representan un riesgo. ● Recuperar datos críticos y configuraciones de sistemas usando copias de seguridad previas al incidente. Verificar la existencia de copias de seguridad previas al incidente, su integridad y accesibilidad. ● Si se cuenta con copias de seguridad oportunas, íntegras y accesibles, se procede a restaurarlas. ● Si no se cuenta con copias de seguridad oportunas, íntegras y accesibles se procede a determinar una copia que pueda ser utilizada, y se realiza la restauración. ● Se determina el tipo y volumen de información que tuvo pérdida para determinar el impacto en uno o varios procesos de la entidad. ● Implementar un monitoreo intensivo en los sistemas restaurados para detectar cualquier comportamiento anómalo, intentos de acceso o signos de persistencia de amenazas. ● Realizar pruebas exhaustivas de funcionamiento y seguridad en los sistemas recuperados para confirmar que operan correctamente y cumplen con los estándares de seguridad. ● Establecer nuevas reglas tanto en firewall como el antivirus si es necesario		Secretaría TIC
7	Recopilar y documentar evidencias del incidente	Recopilar y documentar todos los detalles del incidente con el fin de: ● Reportar a los usuarios afectados, la severidad e impacto del incidente de seguridad, y las medidas aplicadas para su contención y restauración. ● Registrar en base de conocimiento de TIC. ● Reportar a CSIRT a través de	Formato Reporte a Usuarios Formato Reporte de incidentes de seguridad digital Formato CSIRT	Personal encargado de la gestión de incidentes en la Secretaría TIC

		formulario establecido por MinTIC y enviar al correo csirtgob@mintic.gov.co. • Socializar las lecciones aprendidas con equipo de soporte de incidentes de la Secretaría TIC..	diligenciado Correos electrónicos enviados	

5. Diagrama de flujo



6. Documentos y registros relacionados

Política General de Seguridad y Privacidad de la Información V02
Matriz Inventario de Activos de Información

7. Anexos

Anexo 1. Formato Reporte de Incidentes de seguridad digital
Anexo 2. Formato Reporte a Usuarios
Anexo 3. Formato Reporte a "CSIRT"

8. Control de cambios

Versión	Fecha de versión	Descripción del cambio	Responsable
01	26/12/2024	Creación del documento	Jonathan Huertas Secretario TIC, Innovación y Gobierno Abierto

9. Responsable

El responsable de este documento es el(la) Secretario(a) TIC, Innovación y Gobierno Abierto quien debe revisarlo, y si es necesario actualizarlo.

10. Revisión, aprobación y verificación.

Revisión:	Aprobación:	Verificación:
Jonathan Huertas Secretario TIC, Innovación y Gobierno Abierto	Jonathan Huertas Secretario TIC, Innovación y Gobierno Abierto	Lized Anabel López Erazo Secretaria de Planeación