REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

1

GENERACIÓN CASO SIGMA

recolección de información preliminar con base en la detección o reporte de una anomalía en los componentes y/o activos de la Policía Nacional, con el fin de evidenciar si realmente es un evento o un incidente de seguridad de la información o solo se trata de una falsa alarma

2

EVALUACIÓN

.

Recolección de la evidencia

El analista de seguridad de la información clasifica la información recepcionada si en realidad incidente o evento y posterior a esto la clasifica

Triage

El caso SIGMA entra a ser evaluado mediante triage para priorizar el orden de atención entre los casos llegados

3

RESPUESTA DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Identificación de lecciones aprendidas.

El analista de Seguridad de la información identifica patrones, áreas cítricas, implementación de acciones preventivas para reducir la probabilidad de futuros incidentes, estas deben ser consignadas en el formato de atención a incidentes.

4

DOCUMENTACIÓN

El analista de seguridad de la información documentará

- 1DT-FR-0011 REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN
- Reporte de evento de Seguridad de la Información 1DT-FR-0014.