1. OBJETIVO

Gestionar los incidentes de seguridad de la información identificando, analizando, evaluando y solucionándolos cuando ocurran en los diferentes procesos y cargos, para luego ser consolidados y crear así, una base de conocimiento que permita su prevención, mejorar su atención y gestión en la Cooperativa.

2. ALCANCE

El funcionario inicia con la identificación del incidente de seguridad para posteriormente realizar el reporte a la subgerencia TIC por medio de la plataforma tecnológica Milldesk para su debido análisis, plan de acción, seguimiento y documentación.

3. RESPONSABLES

3.1. Comité del Seguridad de la Información.
3.2. Subgerencia TIC.
3.3. Dirección SIAR.
3.4. Oficial de Seguridad de la información .
3.5. Funcionario.

4. REQUISITOS LEGALES Y DOCUMENTALES

4.1. Plan de Continuidad del Negocio
4.2. Manual del Sistema de Gestion de Seguridad de la Información

5. TÉRMINOS Y DEFINICIONES

5.1. Riesgo Operativo: Es la posibilidad de incurrir en pérdidas por deficiencias, fallas, ausencias o inadecuaciones en:

a) Los procesos,
b) El recurso humano,
c) La tecnología,
d) La infraestructura física;
e) Por la ocurrencia de acontecimientos externos.

5.2 Evento de riesgo operativo: Son situaciones que generan impactos no deseados en COONFIE asociados al riesgo operativo.

5.3 Incidente de Seguridad de la información: Es la materialización de una serie de eventos de seguridad de la información inesperados o no deseados que comprometen las operaciones de la entidad.

5.4 Gestion de Incidentes: Describe las acciones necesarias que realiza una organización para analizar, identificar y corregir problemas mientras toma medidas que pueden evitar futuros incidentes.

6. DISPOSICIONES GENERALES

6.1. Si al evaluar el evento de riesgo operativo, se concluye que no es un incidente de Seguridad de la información, se deberá seguir con normalidad la gestión de un evento de riesgo operativo, como lo indica el procedimiento PO-RI-08 Reporte y Gestion de Eventos de Riesgo Operativo.

6.2. Los reportes de los incidentes de seguridad se podrán realizar vía telefónica o correo corporativo, entendiendo la urgencia y prioridad de un evento de este tipo. Una vez se realice el análisis y se tome el control sobre este, el funcionario quien comunicó el evento de seguridad debe escalarlo por la mesa de ayuda para su debido registro y soporte.

6.3. Si el incidente de seguridad de la información ha sucedido con anterioridad en la Cooperativa, se deberá buscar en la Bitácora FO-TI-XX el formato que consolida la gestión hecha sobre ese incidente.

6.4 Si el incidente de seguridad reportado compromete la base de datos, el oficial de seguridad de la información

debe reportarlo al oficial de protección de datos personales.

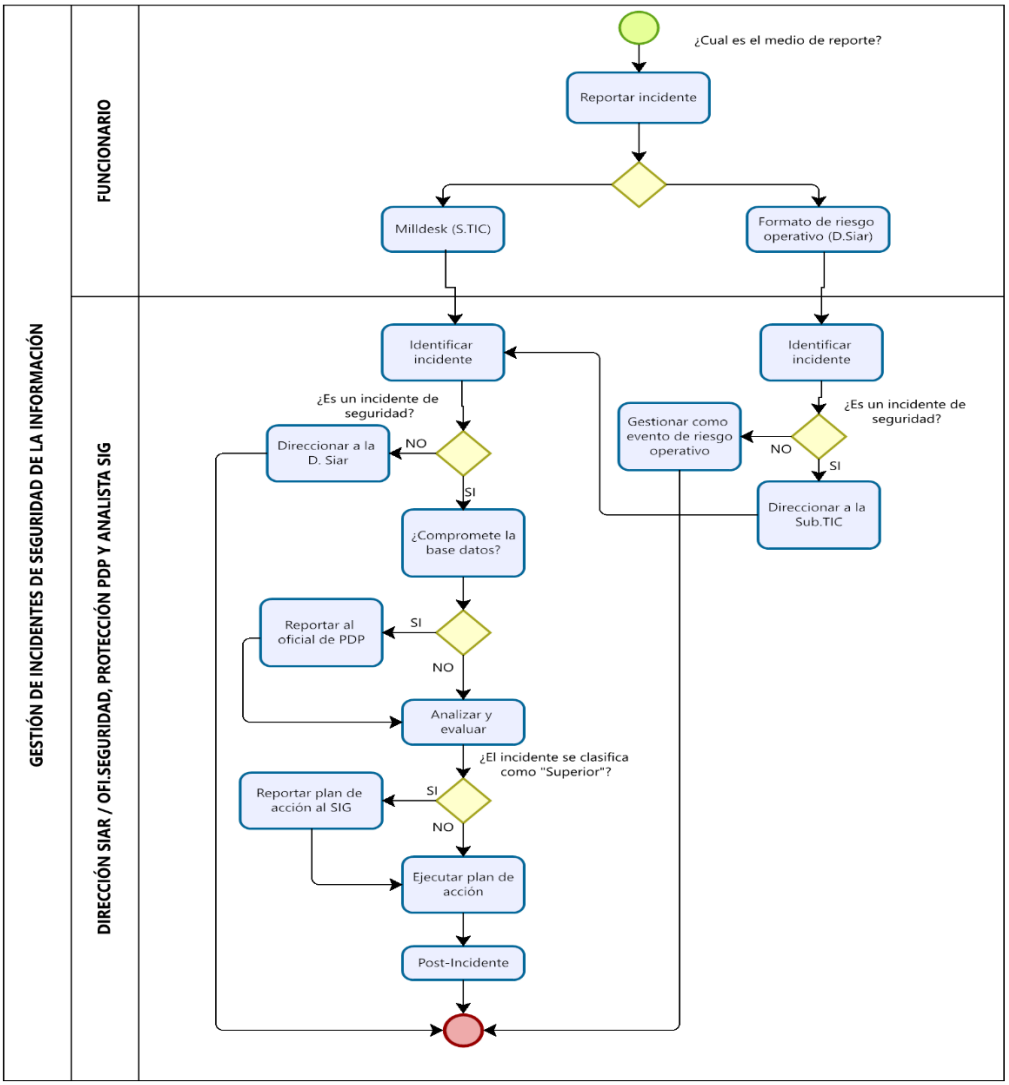
6.5 Si el incidente al ser evaluado, su nivel de criticidad o de Impacto es clasificado como 'Superior', el oficial de seguridad de la información deberá reportar al analista SIG el plan de mejoramiento para su seguimiento en la matriz MT-GI-03 Plan de Mejoramiento del SIG.

6.6 Si el incidente al ser evaluado, su nivel de criticidad o de Impacto es 'Alto' o Superior, se deberá citar al Comité de Seguridad de la información para revisar el caso y tomar las respectivas medidas para ejecutar el plan de acción.

6.7 Cada trimestre, el Oficial de Seguridad de la información, deberá reportar al Comité de Seguridad de la información un informe detallado de los nuevos incidentes.

6.8 La gestión del incidente que comprende la etapa de identificación, análisis y evaluación, plan de acción y post-incidente deben ser registradas en el formato **FO-TI-25**

7. DIAGRAMA DE FLUJO



8. DESCRIPCIÓN DE ACTIVIDADES

No.	Actividad	Descripción de la actividad	Responsable	Registro
1	Reportar Evento de Seguridad de la información	El funcionario reporta el incidente de seguridad a la dirección del Siar o a la Sub-TIC.	Funcionario	Milldesk Correo Electrónico Llamada telefónica
2	Identificar Incidente	Revisar el evento reportado para determinar si es un incidente de seguridad de la información. - Si no es un incidente ***Ver disposición 6.1.***	Dirección Siar Oficial de Seguridad de la información	Milldesk **FO-RI-01** Registro de Evento Operativo
3	Verificar incidente	Determinar si el incidente compromete la base de datos. Si compromete la base de datos ***Ver disposición 6.4.*** Si no compromete la base de datos debe continuar las actividades del presente procedimiento.	Oficial de seguridad de la información Oficial de protección de datos personales	Correo electrónico
4	Analizar y Evaluar	Analizar y evaluar el incidente según el reporte por parte del funcionario, adicionalmente debe ser diligenciado en el FO-TI-25 por el oficial de seguridad de la información. Si el incidente al ser evaluado, su nivel de criticidad o de Impacto es clasificado como 'Superior', el oficial de seguridad de la información deberá reportar el plan de mejoramiento al analista SIG para su seguimiento en la matriz MT-GI-03 Plan de Mejoramiento del SIG.	Oficial de Seguridad de la información Analista SIG	**FO-TI-25** Gestión de incidentes. **MT-GI-03** Plan de mejoramiento

5	Ejecutar el plan de acción	Realizar las actividades de Contención y Recuperación registradas en el FO-TI-25 de cada funcionario responsable. Hacer el seguimiento a los resultados presentados.	Funcionario responsable	Milldesk
6	Post -Incidente	Registrar las consecuencias, la prevención, y los antecedentes del incidente que se presenta, en el **FO-TI-23**.	Oficial de Seguridad de la Información	**FO-TI-25** Gestión de incidentes.

No.	Actividad	Descripción de la actividad	Responsable	Registro

9. DOCUMENTOS RELACIONADOS

FO-RI-01 Registro de Evento Operativo
FO-TI-25 Formato Gestion de Incidente
FO-TI-24 Bitácora base de conocimiento gestión de incidentes
FO-TI-23 Bitácora seguimiento a la disponibilidad de los servicios
DA-TI-03 Clasificación de incidentes.
MT-GI-03 Plan de mejoramiento del SIG

10. CONTROL DE CAMBIOS

La trazabilidad de los cambios generados en el documento podrá ser consultada en el Listado Maestro de Documentos.

Versión	Descripción Del Cambio	Fecha de Aprobación
1	Elaboración inicial del documento	25/04/2023

Elaborado Por:	Revisado Por:	Aprobado Por:
RICARDO MARIA SUAREZ ORTIZ **Cargo:** Subgerente TIC	**SERGIO ALEJANDRO CUELLAR** **Cargo:** Analista SIG	**NÉSTOR BONILLA RAMÍREZ** **Cargo:** Gerente General