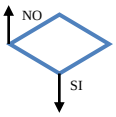
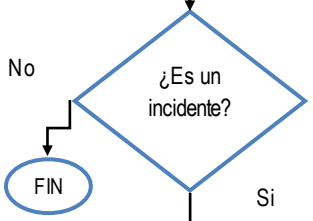
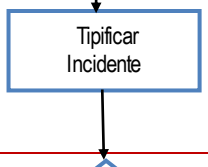
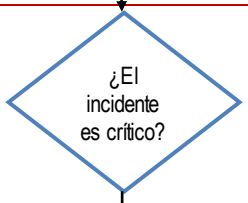
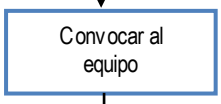
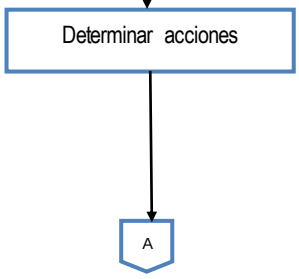
PROCEDIMIENTO: GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
OBJETIVO:		Establecer lineamientos para la gestión de incidentes de seguridad de la información, mediante la herramienta tecnológica de incidentes de la entidad, con el fin de dar solución a las partes interesadas y garantizar el tratamiento y recuperación eficiente ante un incidente que pueda afectar o atente los activos de información.
ALCANCE:	**Limite Inicial:**	Detección y/o reporte de un incidente de seguridad de la información.
	Limite Final:	Gestión, investigación, tratamiento y cierre del incidente de seguridad de la información.
PRODUCTOS:		Formato de incidentes de seguridad de la información
RESPONSABLE:		Oficial de Seguridad de la Información, Equipo de respuesta a incidentes de seguridad de la información (ISIRT), Funcionario, contratista, proveedor o terceras partes.

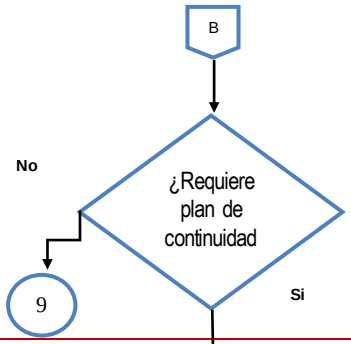
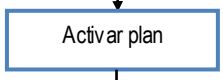
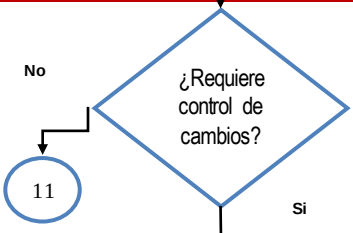
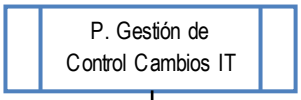
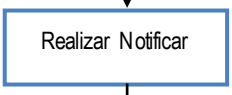
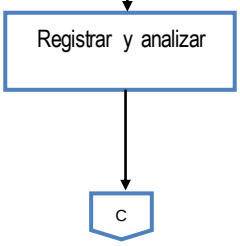
CUADRO DE CONVENCIÓN FLUJOGRAMA:

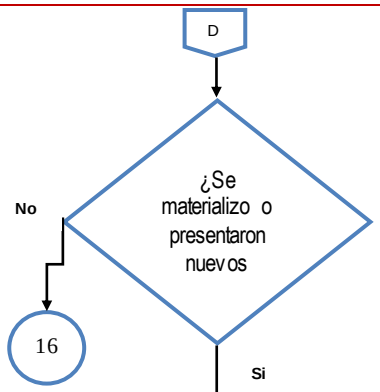
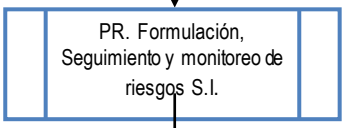
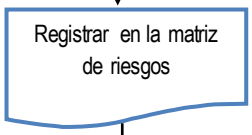
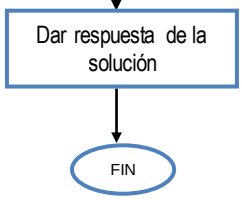
SÍMBOLO	SIGNIFICADO	USO
	Inicio / Fin	Indica el Inicio y el Final del Diagrama de Flujo.
	Operación Actividad	Símbolo de proceso, representa la realización de una operación o actividad. Esta debe ser concreta y en verbo infinitivo.
	Documento	Representa cualquier tipo de documento que se cree dentro de la actividad y que sirva de insumo para otra actividad del mismo procedimiento (Diferente Proceso y/o procedimiento).
	Punto de Control o de Decisión	Un rombo con una pregunta en su interior indica una decisión que tiene normalmente dos alternativas. En las líneas de conexión que salen del rombo se indican las respuestas a la pregunta, que dan lugar a los caminos seguidos en función de estas respuestas, dependiendo de que la condición se cumpla o que no se cumpla. Implica un retroceso o una continuidad en la tarea. (Ver **numeral 2.4.4.4** aclaración uso símbolo de rombo).
	Conector de dirección de flujo (Flecha)	Todos los símbolos deben ir enlazados entre sí, por flechas que indican cómo se realiza la secuencia. Las flechas indican el camino o flujo que sigue el ordenador desde el comienzo hasta la finalización, a través de todas las tareas. Para casos que la flecha genere trazos muy largos o que se cruzan con otras se puede utilizar un conector de círculo.
	Conector	Representa la continuidad del diagrama dentro de la misma página o en distinta página. Enlaza dos pasos no consecutivos y se identifica con números. **Para el caso de la SNR** el conector de círculo referenciará el número de la actividad de la columna "número de actividad" al cual se debe direccionar para dar continuidad al flujo.
	Conector de Página	Representa la continuidad del diagrama en otra página, conexión o enlace con otra hoja diferente en la que continua el diagrama de flujo, este se identifica con letras mayúsculas del abecedario, **se mantiene la misma letra inicialmente utilizada** siempre y cuando en el cambio de página se esté hablando de la misma actividad, **de lo contrario cambia de** letra. Ajustado a la SNR
	Conector de Procedimiento	Procedimiento predefinido: Se utiliza para identificar un documento con el cual interactúa el procedimiento, este símbolo se utiliza de manera opcional ya que el formato en la casilla de "Descripción de la actividad" se describen las interacciones de los procedimientos. Dentro del símbolo se debe citar el nombre del procedimiento.

POLÍTICAS OPERACIONALES

1. **Tipificar el incidente con la información recolectada por medio del Registro en el Sistema de la entidad**
2. **Determinar las acciones pertinentes para la solución o gestión del incidente de S.I. a partir de la investigación, causa, análisis y recolección de evidencias, así mismo, se debe evaluar la posible contingencia ante una intermitencia o interrupción de las operaciones y definir el o los responsable(s) de ejecutar dichas acciones. Activar comunicación COLCERT – CSIRT sectorial y notificar en Plataforma Nacional de seguimiento a incidentes de seguridad digital correo contacto@colcert.gov.co y/o malware@colcert.gov.co.**

N°	FLUJOGRAMA	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	CONTROL DE REGISTROS
1		Reportar el posible incidente de seguridad de la información (S.I.) **Nota:** Se podrá informar al coordinador o jefe inmediato para que pueda redirigir el mensaje al Oficial de seguridad de la información.	Funcionario, contratista, proveedor o terceras partes	Mesa de Ayuda E-mail Oficial de Seguridad de la información
2		Realizar el análisis del reporte y recolectar toda la información para determinar sí, ¿Es un incidente de seguridad de la información? **Sí;** Tipificar el incidente. Actividad número 3 **No;** Finalizar el procedimiento.	Oficial de Seguridad de la Información	No Aplica
3		Tipificar el incidente con la información recolectada por medio del Registro en el Sistema de la entidad **Nota:** Refiérase a las políticas de operación No. 1	Oficial de Seguridad de la Información	E-mail Oficial de Seguridad de la información. Registro en el Sistema Service Desk (número de ticket asignado por la herramienta)
4		¿El incidente de seguridad de la información es crítico? **Sí;** continuar con la actividad número 5 **No;** Continuar con la actividad número 9.	Oficial de Seguridad de la Información	Registro en el Sistema Service Desk
5		Convocar al equipo de respuesta de incidentes de Seguridad de la información para evaluar el incidente y en conjunto determinar las acciones a ejecutar.	Oficial de Seguridad de la Información	Registro en el Sistema Service Desk
6		Determinar las acciones pertinentes para la solución o gestión del incidente de S.I. a partir de la investigación, causa, análisis y recolección de evidencias, así mismo, se debe evaluar la posible contingencia ante una intermitencia o interrupción de las operaciones y definir el o los responsables de ejecutar dichas acciones. Activar comunicación COLCERT – CSIRT sectorial y notificar en Plataforma Nacional de seguimiento a incidentes de seguridad digital correo contacto@colcert.gov.co y/o malware@colcert.gov.co. **Ver política de operación No. 2**	Oficial de Seguridad de la Información Equipo de respuesta a incidentes de Seguridad de la información	Registro en el Sistema Service Desk

7		¿Se requiere activar el plan de continuidad? **Sí;** Continuar con la actividad número 8 **No;** Continuar con la actividad número 9.	Oficial de Seguridad de la Información Equipo de respuesta a incidentes de Seguridad de la información	No Aplica
8		Activar plan de continuidad del negocio OTI	Oficial de Seguridad de la Información Equipo de respuesta a incidentes de Seguridad de la información	Registro en el Sistema Service Desk
9		¿El incidente de seguridad de la información requiere gestión de control de cambios? **Sí;** Continuar con la actividad número 10 **No;** Si es el caso; continuar con la actividad número 11	Oficial de Seguridad de la Información Equipo de respuesta a incidentes de Seguridad de la información	Registro en el Sistema Service Desk
10		Gestionar Procedimiento Gestión de Control de Cambios IT de la OTI	Oficial de Seguridad de la Información	Formato de Control de cambios
11		Realizar notificación a las partes interesadas (Internas o externas) sobre el incidente reportado.	Oficial de Seguridad de la Información	E-mail Oficial de Seguridad de la información.
12		Registrar en la herramienta de Gestión de incidentes las lecciones aprendidas, cuantifica el costo del incidente y analiza la materialización o presencia de nuevos riesgos.	Oficial de Seguridad de la Información Equipo de respuesta a incidentes de seguridad de la información	Registro en el Sistema Service Desk

13		¿Se materializo o se presentan nuevos riesgos para la seguridad de la información? **Sí;** Continuar con la actividad número 14 **No;** Continuar con la actividad número 16 y Fin	Oficial de Seguridad de la Información	Registro en el Sistema Service Desk
14		Implementar los procedimientos de: Formulación, Seguimiento y monitoreo de riesgos para el Sistema de Seguridad de la Información.	Oficial de Seguridad de la Información	Matriz de riesgos de SGSI
15		Registrar en los riesgos en la respectiva matriz SGSI	Oficial de Seguridad de la Información	Matriz de riesgos de SGSI
17		Dar respuesta de la solución al incidente de Seguridad de la Información, aplicando las acciones establecidas y cerrar el caso. Fin	Equipo de respuesta a incidentes de seguridad de la información	Registro en el Sistema Service Desk

VERSIÓN DE CAMBIOS			
Código:	**Versión:**	**Fecha:**	**Motivo de la actualización:**

<table>
<tr><th></th><th colspan="5">ELABORACION Y APROBACION</th></tr>
<tr><th>ELABORÓ</th><th>REVISIÓN METODOLOGICA</th><th colspan="2">APROBÓ</th><th colspan="2">Vo. Bo Oficina Asesora de Planeación</th></tr>
<tr><td>Jorge Alberto Echeverri

Jaime Enrique Camacho Pardo</td><td>Jeiffe Jubelly Muñoz Robayo</td><td rowspan="2">Leyla Zoraya Guzmán Rodríguez</td><td rowspan="2">Oficina de Tecnología de la Información</td><td rowspan="2">Juan Carlos Torres Rodríguez</td><td rowspan="2">Coordinador del Grupo de Arquitectura Organizacional Mejoramiento Continuo o quien haga sus veces</td></tr>
<tr><td>Oficina de Tecnología de la Información – Sistema de Gestión de Seguridad y Privacidad de la información</td><td>Oficina Asesora de Planeación.</td></tr>
<tr><td>Fecha: 03 de Noviembre de 2022</td><td>Fecha: 29 de Noviembre de 2022</td><td colspan="2">Fecha: 30 de Noviembre de 2022</td><td colspan="2">Fecha Aprobación: 06 de Diciembre de 2022</td></tr>
</table>