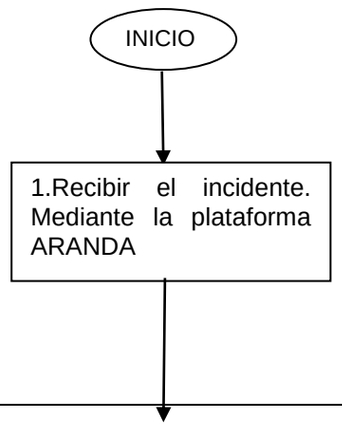
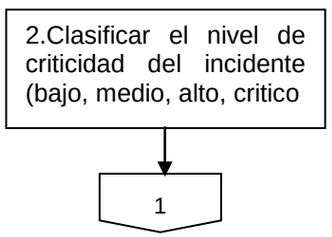
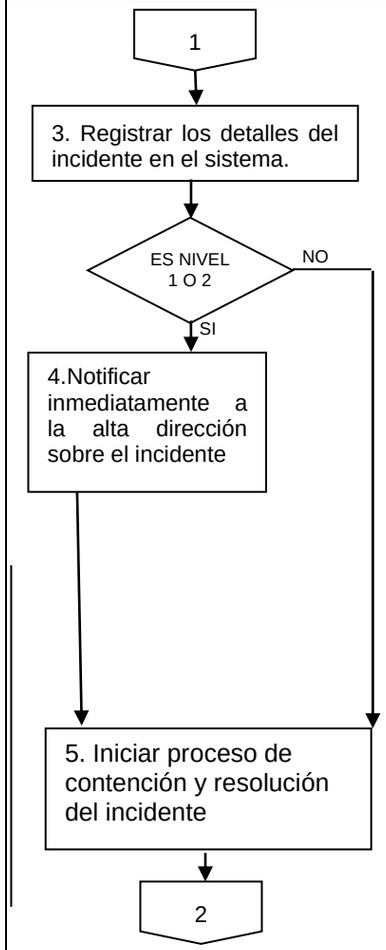
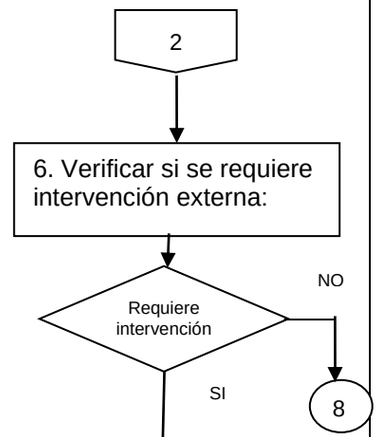
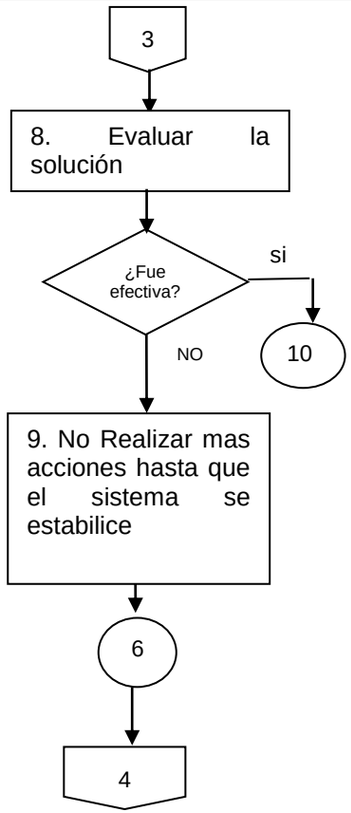
República de Colombia Gobernación de Santander	**GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL**	**CÓDIGO**	AP-TIC-PR-16
		VERSIÓN	0
		FECHA DE APROBACIÓN	28/01/2025
		PÁGINA	1 de 6

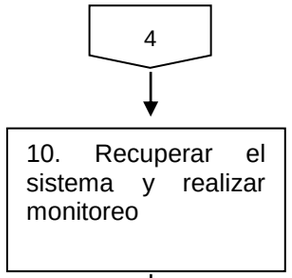
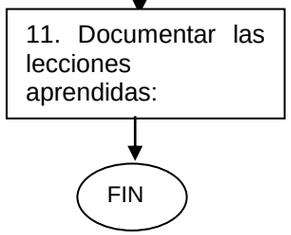
PROCESO	Tecnologías de la Información y las comunicaciones	**SECRETARIA U OFICINA**	Secretaría de Tecnologías de la Información y las Comunicaciones
PROCEDIMIENTO	Procedimiento de Gestión de Incidentes de Seguridad Digital		
OBJETIVO	Establecer los lineamientos y actividades necesarias para gestionar de manera efectiva los incidentes de seguridad digital, garantizando la confidencialidad, integridad y disponibilidad de los activos de información, en cumplimiento con las directrices de MinTIC.		
ALCANCE	Este procedimiento aplica para todos los incidentes de seguridad digital que afecten los activos de información de la organización, desde su detección hasta su cierre y documentación.		

FLUJOGRAMA	**ACTIVIDADES**	**RESPONSABLES**		**PUNTOS DE CONTROL**	**REGISTROS**
[No] [Nombre de la Actividad]	**[Descripción de la Actividad]**	**AREA**	**CARGO**		**[Documento] [Código]**
	1. Recibir el incidente mediante la plataforma de soporte técnico ARANDA: - El usuario reporta el incidente a través de la plataforma ARANDA, la cual registra los detalles del reporte. - Se asigna un número de ticket para hacer seguimiento del incidente. Asignar el reporte al instructor o técnico de acuerdo con la disponibilidad de los mismos	Dirección de Sistemas de información	Profesional Universitario Instructor	Ticket en plataforma Aranda Formulario de reporte de incidente	N.A.
	2. Clasificar el nivel de criticidad del incidente (bajo, medio, alto, crítico) según el impacto y urgencia.	Dirección de Sistemas de información	Profesional de apoyo Instructor	Acta de reunión firmada	Acta de reunión AP-AI-RG-111

FLUJOGRAMA	ACTIVIDADES	RESPONSABLES		PUNTOS DE CONTROL	REGISTROS
[No] [Nombre de la Actividad]	[Descripción de la Actividad]	AREA	CARGO		[Documento] [Código]
	3. Registrar los detalles del incidente en el sistema. - Descripción - Archivos de Soporte - Secretaría - Dirección - Extensión Telefónica de Contacto Si el incidente es Nivel 1 o 2 (alto o crítico): realizar actividad 4 4. Notificar de manera inmediata a la alta dirección sobre el incidente e iniciar con la resolución. Si el incidente es Nivel 3 o 4 (bajo o medio): continuar en la actividad 5 5. Iniciar el proceso de contención y resolución del incidente.	Dirección de Sistemas de información	Profesional de apoyo Instructor	3. Registro Y Gestión De Eventos E incidentes De Seguridad Digital Diligenciado en la plataforma 4. Forest, Correo Electrónico 5. Novedades registradas en la plataforma	5.Carta de Notificación (AP-AI-RG-110)

FLUJOGRAMA	ACTIVIDADES	RESPONSABLES		PUNTOS DE CONTROL	REGISTROS
[No] [Nombre de la Actividad]	[Descripción de la Actividad]	AREA	CARGO		[Documento] [Código]
	6. Verificar si se requiere intervención externa: - Evaluar si el incidente debe ser reportado a las autoridades pertinentes (CSIRT Gobierno, COLCERT, etc.) - Si es necesario, realizar el reporte externo correspondiente. - Si no es necesario, continuar con el proceso interno de resolución. Pasa a la actividad 8	Dirección de Sistemas de información	Director de Sistemas de información Profesional Universitario Profesional de apoyo Instructor	Reporte de incidente remitido a la autoridad (correo electrónico)	Acta de reunión (ap-ai-rg-129_registro_de_reunion_v6) Solicitud de intervención (AP-AI-RG-110)
7. Recolectar evidencias y realizar contención inicial: 3	7. Recolectar evidencias y realizar contención inicial: Recopilar registros, capturas de pantalla, y demás evidencias relevantes del incidente para remitir la información a la autoridad externa y se implementen acciones iniciales para contener el impacto del incidente y evitar su propagación.	Dirección de Sistemas	Profesional Universitario Profesional de apoyo Instructor	Reporte de incidente remitido a la autoridad (correo electrónico) Novedades registradas en la plataforma	Solicitud de intervención (AP-AI-RG-110)

FLUJOGRAMA	ACTIVIDADES	RESPONSABLES		PUNTOS DE CONTROL	REGISTROS
[No] [Nombre de la Actividad]	[Descripción de la Actividad]	AREA	CARGO		[Documento] [Código]
	8. Evaluar la solución - Determinar si la solución implementada fue efectiva para resolver el incidente. 9. la solución no fue efectiva, no realizar más acciones hasta que el sistema se estabilice e iniciar las acciones de contención desde la actividad 6.	Dirección de Sistemas	Profesional Universitario Profesional de apoyo Instructor	Acta de reunión firmada	Acta de reunión (código)

FLUJOGRAMA	ACTIVIDADES	RESPONSABLES		PUNTOS DE CONTROL	REGISTROS
[No] [Nombre de la Actividad]	[Descripción de la Actividad]	AREA	CARGO		[Documento] [Código]
	10. Si la solución fue efectiva, proceder con la recuperación del sistema afectado y el monitoreo post-incidente.	Dirección de Sistemas de información	Profesional Universitario Profesional de apoyo Instructor	Informe de recuperación y seguimiento	Informe de recuperación y seguimiento de informe (código)
	11. Documentar las lecciones aprendidas: - Analizar el incidente y su resolución para identificar oportunidades de mejora. - Registrar las lecciones aprendidas en la documentación del proceso. - Implementar las mejoras necesarias en los procedimientos.	Dirección de Sistemas	Profesional Universitario Profesional de apoyo Instructor	Informe de lecciones aprendidas	Informe de lecciones aprendidas

SALIDA DE LA ACTIVIDAD	lecciones aprendidas a partir de la gestión del incidente.
DEFINICIONES	**ARANDA:** Plataforma de mesa de ayuda técnica en la gobernación de Santander.
OBSERVACIONES	

CONTROL DE CAMBIOS				
VERSIÓN	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**	**REVISÓ**	**APROBÓ**
0	28/01/2025	Se crea el procedimiento	. SANDRA LILIANA BAUTISTA ESCOBAR **DIRECTORA GOBIERNO DIGITAL**	SHIRLEY PAOLA CASTELLANOS MARTÍNEZ **SECRETARIA TIC**