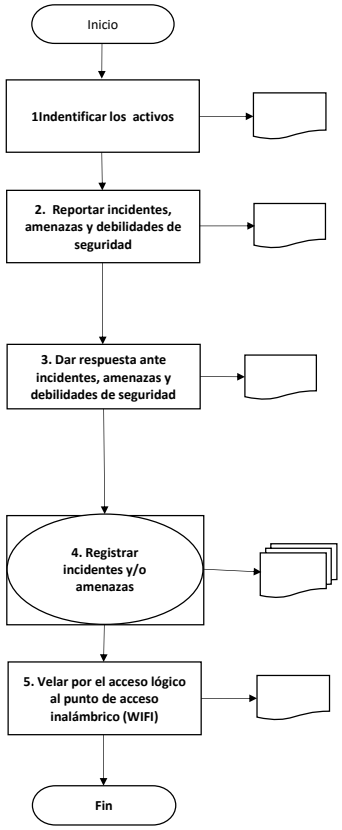
	Procedimiento	Gestión de Incidentes, Amenazas y Debilidades de Seguridad	Código:	GT-PD-09
	Proceso	Gestión de Tecnologías de la Información	Versión:	1
			Páginas:	1 DE 1

Objetivo:	Establecer las directrices ante la ocurrencia de incidentes o la detección de amenazas y/o debilidades que pudiesen comprometer la seguridad de los activos de información con el fin de de tener un protocolo especifico para responder ante cualquier requerimiento que afecte la disponibilidad de los servicios tecnologicos que se preseten al interior de la entidad basandose en la mejores practicas documentdadas por MSPI emitido por los entes de control.		
Alcance:	Este procedimiento aplica a todos los funcionarios (planta, contratista), terceros que presten servicios a la FUGA y o que realicen algún otro tipo de actividad , para lo cual requieran el uso de sistemas y servicios basados en tecnologías de información, inicia con la solicitud de soporte y finaliza con el registro controlado de los accesos vulnerables que puueda tener la entidad.		
Responsable del Procedimiento	Subdirector (a) Gestión Corporativa	Corresponsables del procedimiento	Profesional de apoyo de gestión de tecnología
Definiciones:	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.		
	MSPI: Modelo seguridad y privacidad de la información siglas emitidas por el Ministerio de tecnologias de la información.		
	Atención de Incidentes de Seguridad: Recibe y resuelve los incidentes de seguridad de acuerdo con los procedimientos establecidos.		
	Recolección y Análisis de Evidencia Digital: Toma, preservación, documentación y análisis de evidencia cuando sea requerida.		
Políticas de operación:	El Funcionario y/o contratista debe Informar inmediatamente al proceso de Gestión de la Información ante la ocurrencia de incidentes o la detección de amenazas y/o debilidades que pudiesen comprometer la seguridad de los activos de información de la institución a traves de correo electronico al grupo de soporte .		

DESCRIPCIÓN DEL PROCEDIMIENTO

Flujo grama	Descripción de la actividad	Registro	Responsable (rol)	Tiempo estimado de ejecución
	**1. Indentificar los activos** Indentificar los activos de información deberán ser protegidos ante incidentes, amenazas y/o debilidades: Servidores. Equipos de conectividad (Firewall, Routers, Switches, Access points.). Enlaces de telecomunicaciones (Internet, MPLS, Telefonía) Computadores personales. Impresoras. Sistema de control de acceso y cámaras de video vigilancia. Central telefónica y Equipos telefónicos. Sistemas de información, aplicaciones y software en general.	GT-FT-10 Activos de información	Profesional de apoyo de gestión de tecnología	5 días habiles
	2. Reportar incidentes, amenazas y debilidades de seguridad Revisar incidentes o amenazas que será mediante la verificación del correo electrónico a mesadeayuda@fuga.gov.co, asunto “Incidente de seguridad de información”. identificar el incidente o amenaza y a que recursos tecnológicos podría estar afectando.	Informes GLPI	Profesional de apoyo de gestión de tecnología	1 día habil
	3. Dar respuesta ante incidentes, amenazas y debilidades de seguridad Detectar las causas del problema y los elementos afectados, se debe informar a la Dirección sobre el plan de solución, tiempos involucrados y recursos necesarios, dependiendo del grado de complejidad y magnitud del problema, quien deberá realizar las gestiones correspondientes, incluyendo la comunicación al COLCERT con apoyo técnico del proceso de Gestión tecnológica	*imágenes captura de pantalla de la actividad - Correo electronicos	Profesional de apoyo de gestión de tecnología	de acuerdo a la incidencia
	4. Registrar incidentes y/o amenazas Mantener un registro actualizado de incidentes y/o amenazas, incluyendo todas las acciones o medidas que se implementen para solucionarlos, ya sea de forma total o parcial **PC: Profesional de apoyo de gestión de tecnología mensualmente, deberá generar un reporte de incidentes, con objeto de identificar posibles vulnerabilidades, deja evidencia en el formato de registro de incidentes**	Formato registro incidentes (documento no controlado)	Profesional de apoyo de gestión de tecnología	de acuerdo a la incidencia
	5. Velar por el acceso lógico al punto de acceso inalámbrico (WIFI) Velar que los puntos o de acceso (conocido como Access Point) deberán ser manipulados solamente por personal de la sección de Infraestructura y Redes.	*imágenes captura de pantalla de la actividad	Profesional de apoyo de gestión de tecnología	una vez al año

CONTROL DE CAMBIOS

Fecha	Versión	Razón del Cambio	Responsable Equipo SIG
Fecha	**Versión**	**Razón del Cambio**	**Responsable Equipo SIG**
30/12/2019	1	Versión inicial	Deisy Estupiñan Apoyo equipo SIG-MIPG-Oficina Asesora de Planeación

ELABORÓ:		REVISÓ		APROBO	
Nombre:	EDWIN DIAZ	Nombre:	LICETTE YOBELY MOROS LEON	Nombre:	LICETTE YOBELY MOROS LEON
Cargo:	Profesional apoyo gestión de tecnología	Cargo:	Subdirectora Gestiòn Corporativa	Cargo:	Subdirectora Gestiòn Corporativa