



<b>GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: SI-CR-001</b>			
		<b>Versión: 5</b>			
		<b>Fecha: 30/Ago/2017</b>			
		<b>Clasificación: 1. Restringido</b>			
<b>OBJETIVO:</b>	Prevenir la materialización de riesgos de la seguridad de la información que afecten el desarrollo de la misión de la Entidad, así como impartir lineamientos para la protección de datos y archivos de inteligencia y contrainteligencia, dando cumplimiento al marco legal vigente.				
<b>ALCANCE:</b>	Inicia con la identificación de necesidades y requerimientos de seguridad de la información y seguridad informática, así como el establecimiento de políticas para la protección de datos y archivos de inteligencia y contrainteligencia; finalizando con la verificación y control del cumplimiento de los límites, fines y principios establecidos en la ley.				
<b>RESPONSABLES DEL PROCESO:</b>	Seguridad de la información: Jefe Centro de Protección de Datos Protección de datos de inteligencia y contrainteligencia: Coordinador Grupo interno de trabajo de apoyo a la formulación de políticas para la protección de datos de IC				
<b>DESCRIPCIÓN DEL PROCESO</b>					
PROVEEDORES	ENTRADAS	CICLO PHVA	ACTIVIDADES	SALIDAS	USUARIOS
<ul style="list-style-type: none"> <li>* Direccionamiento Estratégico.</li> <li>* Entidades Estatales que emiten lineamientos, efectúan seguimiento y evaluación de la administración pública</li> <li>* Todos los procesos</li> <li>* Proveedores</li> <li>* Inteligencia estratégica y Contrainteligencia de Estado</li> <li>* Gestión seguridad operacional</li> <li>* Gestión Jurídica</li> <li>* Gestión de seguridad de la información</li> <li>* Auditoría interna</li> <li>* Gestión SIGI</li> <li>* Inspección General</li> </ul>	<ul style="list-style-type: none"> <li>* Marco de referencia y diagnóstico situacional</li> <li>* Normatividad vigente</li> <li>* Plan Estratégico Institucional</li> <li>* Buenas prácticas de gestión en materia de seguridad de la información</li> <li>* Informes de auditorías externas</li> <li>* Solicitudes y requerimientos en materia de seguridad de la información</li> <li>* Información y registros de los procesos/dependencias</li> <li>* Necesidades y requerimientos para el establecimiento de lineamientos para el ingreso y protección de datos y archivos de inteligencia estratégica y contrainteligencia de Estado</li> <li>* Autoevaluación de datos y archivos de inteligencia y contrainteligencia</li> <li>* Información gestión proceso/dependencia: datos indicadores, monitoreo de riesgos, plan integrado anual</li> <li>* Recomendaciones, observaciones o hallazgos</li> </ul>	<ul style="list-style-type: none"> <li><b>P</b></li> <li><b>H</b></li> <li><b>V</b></li> <li><b>A</b></li> </ul>	<ul style="list-style-type: none"> <li>* Realizar programación de las actividades del proceso/dependencia</li> <li>* Mantener y mejorar el Sistema de Gestión de Seguridad de la Información</li> <li>* Controlar los procesos de manipulación, transporte y custodia de la información</li> <li>* Asegurar activos de información</li> <li>* Gestionar eventos e incidentes de seguridad de la información</li> <li>* Elaborar políticas para la protección de datos y archivos de inteligencia y contrainteligencia</li> <li>* Verificar la aplicación y cumplimiento de las políticas para la protección de datos y archivos de inteligencia y contrainteligencia</li> <li>* Realizar medición y seguimiento a indicadores de desempeño, monitoreo a riesgos y seguimiento al plan integrado anual del proceso/dependencia</li> <li>* Implementar acciones de mejoramiento</li> </ul>	<ul style="list-style-type: none"> <li>* Programación anual</li> <li>* Lineamientos, métodos, técnicas y herramientas para la implementación del sistema de gestión de seguridad de la información</li> <li>* Seguimiento, evaluación y mejora del sistema de gestión de seguridad de la información</li> <li>* Atención solicitudes y requerimientos en materia de seguridad de la información</li> <li>* Reportes en la atención de eventos e incidentes de seguridad de la información</li> <li>* Políticas para la protección de datos y archivos de inteligencia y contrainteligencia</li> <li>* Informes de verificación del cumplimiento de las políticas de protección de datos y archivos de inteligencia y contrainteligencia</li> <li>* Reporte de medición y seguimiento a indicadores de desempeño</li> <li>* Reporte del monitoreo a riesgos</li> <li>* Reporte del seguimiento al plan integrado anual</li> <li>* Evaluación y seguimiento a las acciones de mejoramiento</li> </ul>	<ul style="list-style-type: none"> <li>* Direccionamiento estratégico</li> <li>* Todos los procesos</li> <li>* Inteligencia estratégica y Contrainteligencia de Estado</li> <li>* Gestión seguridad operacional</li> <li>* Director General DNI</li> <li>* Comité de actualización, corrección y retiro de datos y archivos de inteligencia y contrainteligencia</li> <li>* Auditoría interna</li> <li>* Gestión SIGI</li> <li>* Inspección General</li> </ul>