Proyecto de Resolución	
Dependencia que desarrollará el proyecto de Norma	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
Proyecto de Resolución	"Por la cual se establecen los Objetivos, Política General y Políticas Específicas del Sistema de Gestión de Seguridad de la Información en la Unidad para la Atención y Reparación Integral a las Víctimas- UARIV- y se deroga la Resolución No 740 del 11 de noviembre de 2014"

1. Los antecedentes y las razones de oportunidad y conveniencia que justifican su expedición	Que el inciso primero del artículo 15 de la Constitución Política establece que: "Todas las personas tienen derecho a su intimidad personal, familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas" Que la Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones (…)" Que el artículo 1 de la Ley Estatutaria No 1712 de 2014 relacionada con la Transparencia y el Derecho de Acceso a la Información Pública Nacional, tiene por objeto: "regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información." Que el literal a) del artículo 6 ibídem define la información como: " un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen"; y así mismo en los literales que se relacionan a continuación realiza la siguiente clasificación: "b) Información pública. Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal; c) Información pública clasificada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley; d) Información pública reservada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley (…)"

	Que, de acuerdo con lo anterior, dicha normatividad consagra los instrumentos de gestión para información pública a través de: i. Registro de Activos de Información; ii. Índice de Información Clasificada y Reservada y iii. Esquema de Publicación de Información. Que la Ley Estatutaria No 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" reviste un tratamiento especial y conforme al artículo 17 de dicha normatividad se señalan los deberes del responsable respecto al tratamiento de datos dentro de los cuales se destacan los siguientes literales: "a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data" (…) (…) "d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento". Que la Ley 1448 de 2011 "Por la cual se dictan medidas de atención, asistencia y reparación integral a las víctimas del conflicto armado interno y se dictan otras disposiciones" en su artículo 166, crea la crea la Unidad para la Atención y Reparación Integral a las Víctimas, como una Unidad Administrativa especial con personería jurídica y autonomía administrativa y patrimonial y a través del artículo 29 dispone que: "(…) Las autoridades garantizarán la confidencialidad de la información suministrada por las víctimas y de manera excepcional podrá ser conocida por las distintas entidades que conforman el Sistema Nacional de Atención y Reparación de las Víctimas para lo cual suscribirán un acuerdo de confidencialidad respecto del uso y manejo de la información". Que los datos e información que se genere obtengan, use o se almacene, custodie, distribuya, envie, intercambie y/ o modifique en la Unidad para la Atención y Reparación Integral a las Víctimas, en cada uno de sus procesos misionales, de apoyo y estratégicos son sensibles y deben manejarse en condiciones que garantice su confiabilidad, oportunidad y seguridad. Que el artículo 2.2.9.1.1.1 del Decreto 1078 de 2015 subrogado por el artículo 1 del Decreto 1008 de 2018 señala: "los lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como: el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital". Que el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015 subrogado por el artículo 1 del Decreto 1008 de 2018 dispone que: "la Política de Gobierno Digital será definida por el Ministerio de Tecnologías de la Información y las Comunicaciones y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC, conforme se describe a continuación:

(…)
(…)
1. Componentes de la Política de Gobierno Digital: Son las líneas de acción que orientan el desarrollo y la implementación de la Política de Gobierno Digital, a fin de lograr sus propósitos. Los componentes son:
1.1. TIC para el Estado: Tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades públicas, a través del uso de las Tecnologías de la Información y las Comunicaciones.
1.2. TIC para la Sociedad: Tiene como objetivo fortalecer la sociedad y su relación con el Estado en un entorno confiable que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño conjunto de servicios, la participación ciudadana en el diseño de políticas y normas, y la identificación de soluciones a problemáticas de interés común.
2. Habilitadores Transversales de la Política de Gobierno Digital: Son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.
3. Lineamientos y estándares de la Política de Gobierno Digital: Son los requerimientos mínimos que todos los sujetos obligados deberán cumplir para el desarrollo de los componentes y habilitadores que permitirán lograr los propósitos de la Política de Gobierno Digital.
4. Propósitos de la Política de Gobierno Digital: Son los fines de la Política de Gobierno Digital, que se obtendrán a partir del desarrollo de los componentes y los habilitadores transversales, estos son:
4.1. Habilitar y mejorar la provisión de servicios digitales de confianza y calidad.
4.2. Lograr procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información.
4.3. Tomar decisiones basadas en datos a partir del aumento, el uso y aprovechamiento de la información.
4.4. Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto.
4.5. Impulsar el desarrollo de territorios y ciudades inteligentes para la solución de retos y problemáticas sociales a través del aprovechamiento de las TIC"

Que el artículo 2.2.9.1.1.3 del Decreto 1008 de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones" establece los principios de la Política de Gobierno Digital siendo uno de ellos, la Seguridad de la Información que busca:

> "crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano".

Que el documento CONPES 3854 de 2016 establece la Política Nacional de Seguridad Digital, la cual contiene entre otros, principios fundamentales relacionados con: "PF1.

	Salvaguardar los derechos humanos y los valores fundamentales de los ciudadanos en Colombia, incluyendo la libertad de expresión, el libre flujo de información, la confidencialidad de la información y las comunicaciones, la protección de la intimidad y los datos personales y la privacidad, así como los principios fundamentales consagrados en la Constitución Política de Colombia. (…) y "PF4. Adoptar un enfoque basado en la gestión de riesgos, que permita a los individuos el libre, seguro y confiable desarrollo de sus actividades en el entorno digital. (…)". Que mediante el CONPES 3995 de 2020 establece la Política Nacional de Confianza y Seguridad Digital, la cual tiene como objetivo: "Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías" Que el artículo 2.2.9.1.2.1 del Decreto 1008 de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones" al señalar la estructura respecto a la Política de Gobierno Digital establece la seguridad de la información como elemento fundamental y habilitador transversal de la referida política. Que la Directiva Presidencial 03 de 2021 señala entre otros aspectos, los lineamientos de Seguridad Digital, siendo relevantes: "3.1. "Dar cumplimiento a las directrices en materia de seguridad digital y de la información que expida el MinTIC y las que se expidan en el marco de la política nacional de confianza y seguridad digital del Gobierno Nacional (…) 3.2. (…) fortalecer las medidas en materia de seguridad digital considerando las dinámicas que ha incorporado el uso de medios digitales: (…)" Que el artículo 1 de la Resolución 500 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital" expedida por el MINTIC tiene por objeto: "establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital. Que la Norma ISO 27001:2013 suministra requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de Gestión de Seguridad de la Información. Que mediante la Resolución No 569 de 2018 la Unidad para la Atención y Reparación Integral a las Víctimas adoptó y actualizó el Sistema Integrado de Gestión involucrando varios sistemas dentro de los cuales se encuentra el Sistema de Seguridad de la Información bajo la Norma Técnica ISO 27001:2013.

	Que según el artículo 6 de la resolución referida, el líder del Sistema de Gestión de Seguridad de la Información se encuentra a cargo de la Oficina de Tecnologías de la Información. Que la Oficina de Tecnologías de la Información de la Entidad tiene a su cargo el desarrollo de la Arquitectura Empresarial la cual consiste en la alineación de los datos, procesos, sistemas de información e infraestructura; y reviste importancia toda vez, que señala entre otros, los principios para el manejo y seguridad de la información. Dichos principios fueron aprobados por la Mesa de Gobierno Digital según acta del 30 de octubre de 2020. Que el Artículo 2.2.9.1.3.3 del Decreto 1008 de 2018 señala que el Comité Institucional de Gestión de Desempeño, es el responsable de orientar la implementación de la política de Gobierno Digital, conforme a lo establecido en el Modelo Integrado de Planeación y Gestión. Que el artículo 2.2.22.3.8 del Decreto 1083 de 2015 establece las funciones del Comité Institucional de Gestión y Desempeño, al cual se le adicionan las correspondientes a los comités que integra y/o sustituye; constituyéndose en una instancia que orienta no solamente la implementación del Modelo Integrado de Planeación y Gestión, sino también cada una de las políticas de Gestión y Desempeño necesarias para la mejora de los resultados y calidad en la prestación de servicios a los usuarios de la entidad. Que según lo señalado por el Departamento Administrativo de la Función Pública en el Manual Operativo del Modelo Integrado de Planeación y Gestión -MIPG- “es viable la conformación de los equipos técnicos de apoyo al Comité Institucional de Gestión y Desempeño para la formulación de estrategias de operación y articulación al interior de la entidad”, y Que la Unidad para la Atención y Reparación Integral a las Víctimas a través del Comité Directivo del 18 de junio de 2018, dio viabilidad para la creación de la Mesa de Gobierno Digital cuyo propósito será el cumplimiento de los logros establecidos en el marco de la Política y Estrategia de Gobierno Digital. Que la Mesa de Gobierno Digital es la encargada de articular y consensuar las acciones y soluciones que se relacionan con la política de Gobierno Digital, para la aprobación posterior por parte del Comité Institucional conforme a las funciones asignadas a la mesa de Gobierno Digital según la Circular Interna No 0036 de 2020. Que conforme a lo expuesto en párrafos precedentes es necesario para esta Entidad establecer los objetivos, política General y las Políticas Específicas orientadas al aseguramiento de la información respecto al manejo y uso de esta última por motivos de protección en términos de confidencialidad, integridad y disponibilidad frente a eventuales riesgos que se pueden configurar en la operación de la Unidad.
2. El ámbito de aplicación del respectivo acto y los sujetos a quienes va dirigido	Servidores públicos, Contratistas y colaboradores vinculados a través de operadores

3. La viabilidad jurídica, que deberá contar con el visto bueno de la Oficina Asesora Jurídica de la Entidad o la dependencia que haga sus veces	La viabilidad jurídica está soportada básicamente en la siguiente normativa: Constitución Política de Colombia • Ley 1273 de 2009 • Ley Estatutaria No 1712 de 2014 • Ley Estatutaria No 1581 de 2012 • Ley 1448 de 2011 • Decreto 1078 de 2015 • Decreto 1083 de 2015 • Decreto 1008 de 2018 • CONPES 3854 de 2016 • CONPES 3995 de 2020 • Directiva Presidencial 03 de 2021 • Resolución 500 de 2021 del MinTIC. • Resolución No 569 de 2018 de la Unidad para las Víctimas
4. Impacto económico si fuere el caso	NA
5. Disponibilidad presupuestal	NA
6. Impacto medioambiental o sobre el patrimonio cultural de la Nación	NA
7. El cumplimiento de los requisitos de consulta y publicidad	La presente Resolución deberá publicarse por 15 días calendario para efectos de consultas y observaciones, a través del correo joaquin.rojas@unidadvictimas.gov.co
8. Seguridad Jurídica: Dentro del año inmediatamente anterior y se había reglamentado la misma materia: SI: ___ NO: X	

EL PROYECTO CUMPLE CON LAS DIRECTRICES DE TÉCNICA NORMATIVA PREVISTAS EN EL TÍTULO 2 DE LA PARTE 1 DEL LIBRO 2 DEL DECRTO 1081 DE 2015: SI X NO___

VICTOR EDGARDO DURAN MARTINEZ
Jefe Oficina de Tecnologías de la Información

Proyectó: Joaquín Rojas Palomino