El futuro es de todos	Gobierno de Colombia	**FORMATO MEMORIA JUSTIFICATIVA**

Entidad originadora:	Ministerio de Tecnologías de la Información y las Comunicaciones
Fecha (dd/mm/aa):	26/10/2020
Proyecto de Decreto/Resolución:	"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"

1. ANTECEDENTES Y RAZONES DE OPORTUNIDAD Y CONVENIENCIA QUE JUSTIFICAN SU EXPEDICIÓN.

Las entidades públicas están cada vez más expuestas a sufrir incidentes de seguridad digital, lo cual, además de afectar su funcionamiento puede repercutir en la prestación de los servicios al ciudadano. De esta forma, el Informe Global de Riegos 2019 (FEM, 2019) presenta resultados de la Encuesta Global de Percepción de Riesgos la cual participan alrededor de 1.000 tomadores de decisiones del sector público, del sector privado, de la academia y de la sociedad civil quiénes evalúan los riesgos en general que enfrenta el mundo. En este sentido, alrededor de dos tercios de los encuestados esperan que los riesgos asociados con las noticias falsas y el robo de identidad aumenten en 2019, mientras que tres quintos señalaron lo mismo sobre la pérdida de privacidad para las organizaciones y los gobiernos .

Por otro lado, según el Centro para la Ciberseguridad (C4C, por sus siglas en inglés Center for Cybersecurity) del FEM, "se prevé que la pérdida económica debida al delito cibernético alcanzará los 3 billones de dólares para el año 2020, y el 74% de las empresas del mundo pueden ser hackeadas el próximo año" .

Es así, como en lo corrido del 2020, en el país se está empleando diferentes herramientas de análisis con el fin de evaluar cómo el aislamiento obligatorio ha incrementado los delitos informáticos y de esta forma generar las medidas necesarias para proteger a los ciudadanos colombianos, donde durante lo transcurrido del 2020, comparado con el mismo periodo de 2019 la fluctuación delictiva marcó las siguientes tendencias:

- Incremento del 38% en las DENUNCIAS por delitos informáticos 2020 vs 2019.

- El delito con mayor incremento desde el inicio de la cuarentena es la Suplantación de Sitios Web para Capturar Datos Personales (Phishing) con una variable DE CRECIMIENTO del 268% pasando de 130 a 478 denuncias en esta fecha. Con 76 diferentes vectores de ataque como falsas ayudas humanitarias.

- Incremento del 42% de la violación de datos personales.

- Incremento del 49% del acceso abusivo a sistemas informáticos.

- Incremento del 154% de la interceptación de datos.

Atendiendo estas situaciones frente al desempeño de las entidades del Estado, desde el Modelo Integrado de Planeación y Gestión v2 (MIPG) del Estado, se establecen los lineamientos y requisitos en la planificación, implementación, evaluación y mejoramiento continuo de la Arquitectura Institucional de las entidades públicas, a través de las dimensiones que éste plantea; es por esto, que desde las políticas de Gobierno Digital y Seguridad Digital, el Ministerio TIC desarrolla el Modelo de Seguridad y Privacidad de la Información, y la guía de riesgos de seguridad digital para las

entidades del Estado, sirviendo como instrumentos de estas políticas, apoyando el máximo aprovechamiento de las tecnologías de la información y las comunicaciones con el objetivo de generar confianza en el uso del entorno digital.

En línea con lo anterior, La seguridad y privacidad de la información, como habilitador transversal en la política de Gobierno Digital, busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la Información, para su implementación y mantenimiento, adicionalmente, este modelo se articula con la Guía para la administración de riesgos y diseño de controles en entidades públicas, definido directamente a través del anexo No. 4 que corresponde a la guía de riesgos de seguridad digital para las entidades del Estado, la cual busca dar lineamientos base para que las entidades puedan identificar cuáles son sus activos más importantes, identificar que situaciones podrían causar inconvenientes en el entorno digital y así mismo guiar a que la entidad tome decisiones sobre que hacer frente a los riesgos para gestionarlos de manera eficiente.

De la misma forma, se evidencia la correspondencia con otros lineamientos emitidos por el Departamento Administrativo de la Función Pública (DAFP) como, el Manual Operativo de MIPG, así mismo, se articula con los lineamientos de Privacidad emitidos por la Superintendencia de Industria y Comercio.

Finalmente, se resalta la forma en la cual estos desarrollos de lineamientos y las estrategias para su apropiación, responden directamente a lo definido en los siguientes documentos estratégicos del Gobierno:

- Plan Nacional de Desarrollo 2018-2022: Las políticas de seguridad y confianza digital como uno de los principios orientadores de la transformación digital
- Plan TIC 2018-2022: Traza proyectos e iniciativas relacionados con seguridad digital
- Política de Defensa y Seguridad: Acciones y estrategias para fortalecer las capacidades en ciberseguridad y protección de infraestructura crítica.
- Convenio de Budapest: principal instrumento internacional existente en esta materia, la persecución del Cibercrimen. Asistencia, lineamientos y guías marco normativo, casos exitosos, canales de comunicación.
- CONPES 3975: De acuerdo con lo señalado, es necesario adaptarse al uso y acceso a las nuevas tecnologías, y en línea con la implementación del CONPES 3795 Política Nacional para la Transformación Digital e Inteligencia Artificial, se deben adoptar los nuevos marcos de trabajo y mejores prácticas internacionales para afrontar los riesgos que trae consigo la 4RI.

INFORMACIÓN DE CONTEXTO

Política de Seguridad Digital

"En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades.

De esta forma, a través del Modelo operativo del Modelo Integrado de Planeación y Gestión – MIPG actualizado a través del Decreto 1499 de 2017, donde la política de Seguridad Digital fue integrada como una de las 18 políticas de planeación y Gestión, se determina que, para el orden nacional, en los Comités Sectoriales de Gestión y Desempeño darán las directrices para su implementación. Además, la articulación en materia de Seguridad Digital estará a cargo del enlace sectorial de seguridad digital quien será el encargado de rendir cuentas al Coordinador Nacional de Seguridad Digital acerca de la implementación de la Política Nacional de Seguridad Digital en el respectivo sector.

De otro lado, en el Comité Institucional de Gestión y Desempeño se debe articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la política. Para ello, se debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información en la entidad, el cual debe pertenecer a un área que haga parte de la Alta Dirección. Para las entidades cabeza de sector, el Responsable de Seguridad Digital será el enlace sectorial de seguridad digital.

En el orden territorial, MinTIC definirá los lineamientos para que las entidades territoriales definan la figura del enlace de Seguridad Digital territorial para la implementación de la política de Seguridad Digital, así como las instancias respectivas para la articulación con el Coordinador Nacional de Seguridad Digital.

Criterios diferenciales para la Política de Seguridad Digital

La implementación de la política se hará a través de la adopción con la Guía para la administración de riesgos y diseño

de controles en entidades públicas, así definido directamente a través del anexo No. 4 que corresponde a la guía de riesgos de seguridad digital para las entidades del Estado, que será desarrollada y socializada por MinTic, para que las entidades y departamentos administrativos de la rama ejecutiva inicialmente, para los entes territoriales y demás partes interesadas, se adelantarán jornadas de sensibilización en temas de Seguridad Digital.

Adicionalmente, Las entidades designadas, deberán dar cumplimiento a todas las actividades relacionadas en el plan de acción de seguimiento PAS del CONPES 3854 de 2016, actualizado mediante CONPES 3995 de 2020, el cual enfoca los esfuerzos del Gobierno en crear las condiciones para que se genere la confianza necesaria en el uso del entorno digital, para crear una sociedad más competitiva a través del aprovechamiento de las TIC.

Entendiendo/conociendo el MSPI

A. Qué es el MSPI y ¿Cómo funciona el MSPI?

¿Qué es el MSPI?

El Modelo de Seguridad y Privacidad de la Información (de ahora en adelante MSPI), establece un sistema de gestión de seguridad de la información (SGSI) que contempla un ciclo de operación de cuatro (4) fases (Planificación, Implementación, Evaluación de Desempeño y Mejoramiento Continuo), basadas en un ciclo PHVA, las cuales permiten que las entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información.

A través de la planificación e implementación del MSPI, las entidades determinan las necesidades y objetivos de seguridad de la información teniendo en cuenta su mapa de procesos y el tamaño de su infraestructura, permitiendo tener un panorama más amplio del estado actual en niveles de seguridad y, así poder determinar las medidas y controles que se deben aplicar para realizar un aseguramiento apropiado de las plataformas y diferentes medios donde se gestione la información.

De acuerdo con lo anterior, se han elaborado un conjunto de documentos asociados al MSPI, los cuales, a lo largo de los últimos años han sido utilizados por las diferentes entidades tanto del orden nacional como territorial para mejorar sus estándares en seguridad de la información.

¿Cómo funciona El MSPI?

El Modelo de Seguridad y Privacidad de la Información (MSPI) consta de cuatro (4) fases, precedidas por un análisis diagnóstico o análisis GAP, cuyo objetivo es identificar el estado actual de la entidad respecto a la implementación del

MSPI.

Cada una de las fases contiene requisitos, entregables y herramientas (guías) que ayudan en el desarrollo y mantenimiento del sistema de gestión de seguridad de la información.

Las cuatro fases se ilustran en la siguiente figura:

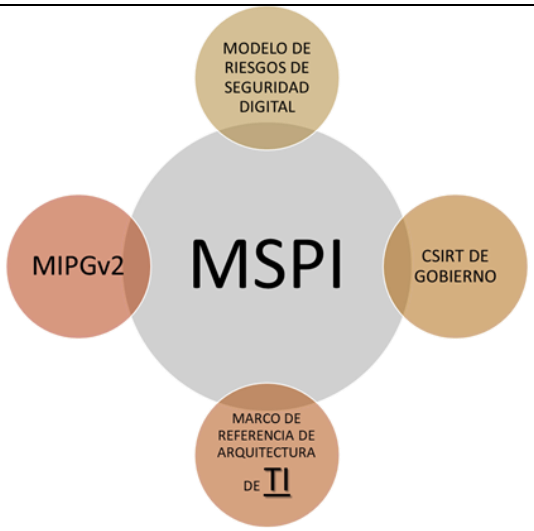
Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

Cada una de las fases se dará por completada, cuando se cumplan todos los requisitos definidos en cada una de ellas.

El MSPI contiene los requisitos y entregables para implementar un sistema de gestión de seguridad de la información, sin embargo, para el desarrollo y el cumplimiento de cada una de las fases, el Ministerio TIC ha diseñado un conjunto de lineamientos o guías anexas, que tendrán el objetivo de facilitar el entendimiento de los requisitos y dar herramientas a las entidades para su implementación.

A. Articulación del MSPI con distintas iniciativas

El MSPI, busca articularse con diferentes iniciativas del gobierno nacional, con el objetivo de proporcionar buenas prácticas de seguridad de la información desde diferentes perspectivas y mostrando la versatilidad y transversalidad que un sistema de gestión de seguridad de la información puede ofrecer.

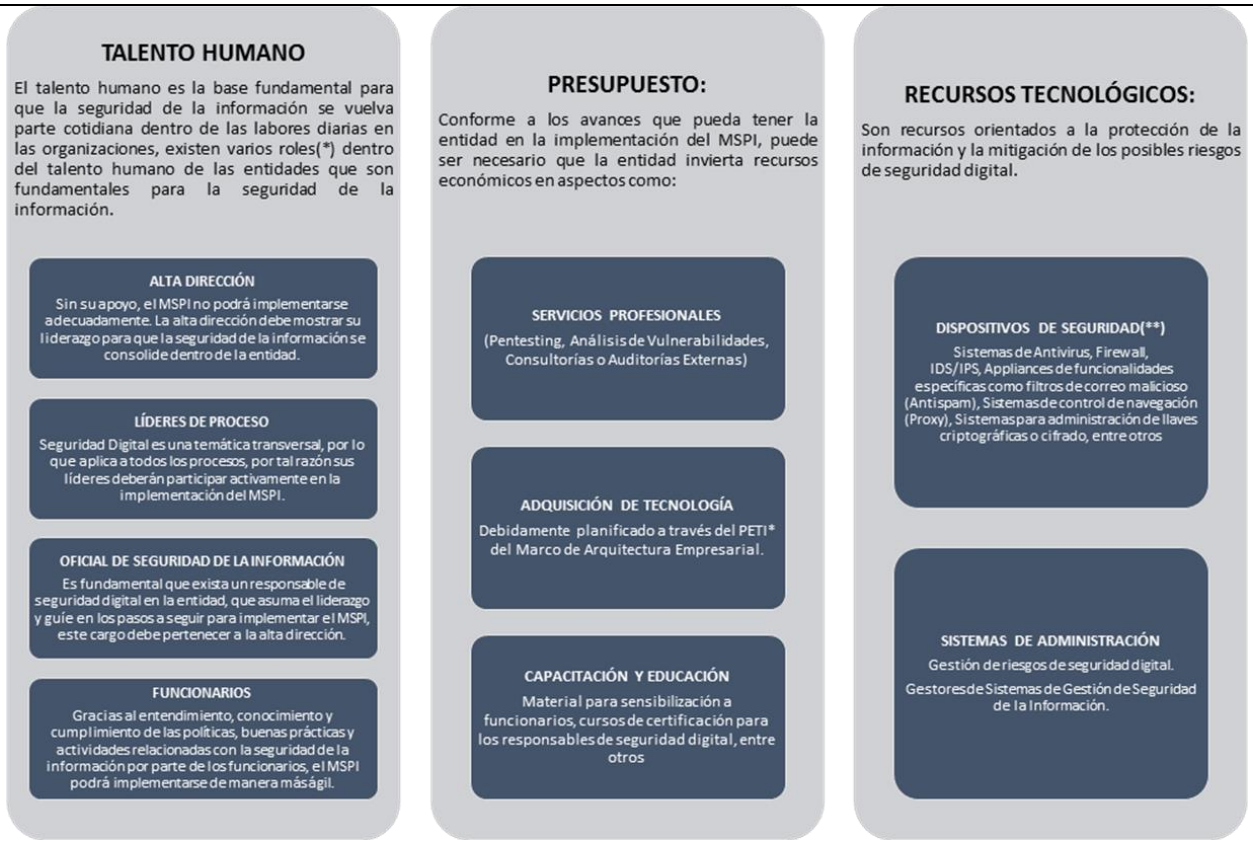


A continuación, se indica cómo operan y se integran paralelamente varias iniciativas junto al Modelo de Seguridad y Privacidad:

MODELO DE RIESGOS DE SEGURIDAD DIGITAL	MIPGv2	CSIRT	MARCO DE REFERENCIA
• Se articula en cada una de las fases del MSPI (Planificación, Implementación, Evaluación y Mejora). • Al desarrollar el Modelo de riesgos de seguridad digital (*A través de la Guía de Administración de Riesgo de DAFP*) se desarrollarán requisitos específicos del MSPI como: Gestión de Activos, Gestión de Riesgos, Planes de Tratamiento de Riesgos, Indicadores de Seguridad, Auditorías Internas entre otros, es decir, ambos modelos funcionan de forma paralela.	• El MSPI, forma parte de la Política de Gobierno Digital como habilitador transversal que a su vez pertenece a la Dimensión 3 *"Gestión con Valores para Resultados"*. • El MSPI a su vez aporta en el desarrollo de las políticas 11 *"Gobierno Digital"* y 12 *"Seguridad Digital"*, en las cuáles el Ministerio de Tecnologías de la Información y las Comunicaciones desempeña el rol de líder.	• El MSPI, prepara a las entidades públicas para que alcancen un grado de madurez y conocimiento suficiente en seguridad de la información dentro de la entidad, logrando que como mínimo se identifiquen cuales son los activos tecnológicos fundamentales para su funcionamiento y así poder interactuar de manera objetiva y concreta con el Equipo de Respuesta a Incidentes de Seguridad - **CSIRT Gobierno,** teniendo un apoyo adicional en la protección de estas infraestructuras esenciales para las entidades.	• El MSPI, aporta en la implementación y desarrollo de los lineamientos relacionados con seguridad que se encuentran dentro del MRAE. Asegurando así un avance paralelo en ambas estrategias. En cada uno de los dominios del Marco existen requisitos o controles de seguridad que el Modelo de Seguridad ayudará a su implementación.

¿Qué se requiere para implementar y mantener el MSPI?

Es necesario que las entidades designen unos recursos específicos para garantizar una implementación y mantenimiento óptimos del MSPI, ya que un sistema de gestión de seguridad de la información no funciona únicamente a base de tecnología, documentación y/o procedimientos. Teniendo en cuenta esta premisa, dentro de los recursos más importantes que debe garantizar la alta dirección para la implementación del MSPI, se pueden encontrar los siguientes:



Es por ello que el parágrafo del artículo 16 del Decreto 2106 de 2019 establece la necesidad y al mismo tiempo la obligación de que las autoridades dispongan de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

Dicha estrategia deberá estar debidamente armonizada con lo dispuesto en el artículo 2.2.9.1.2.1, del Decreto 1078 de 2015 (DUR-TIC), "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones" en cuanto a los habilitadores transversales de la Política de Gobierno Digital, particularmente al elemento de Seguridad y privacidad de la Información.

2. AMBITO DE APLICACIÓN Y SUJETOS A QUIENES VA DIRIGIDO

El proyecto de resolución se aplicará a sujetos señalados en el artículo 2.2.9.1.1.2. del Decreto 1078 de 2015 (DUR-TIC), "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"

3. VIABILIDAD JURÍDICA

(Por favor desarrolle cada uno de los siguientes puntos)

3.1 Análisis de las normas que otorgan la competencia para la expedición del proyecto normativo

Conforme al principio de "masificación del gobierno en línea" hoy Gobierno Digital, consagrado en el numeral 8 del artículo 2 de la Ley 1341 de 2009, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo

aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones.

De acuerdo con el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015 (DUR-TIC), "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", la Política de Gobierno Digital será definida por MinTIC 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.

Según el numeral 2, los habilitadores transversales de la Política de Gobierno Digital, son los ele¬mentos fundamentales de Seguridad y privacidad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los componentes y el logro de los propósitos de dicha Política.

El parágrafo del artículo 16 del Decreto 2106 de 2019, “Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública” señala que las autoridades deberán disponer de una estrategia de seguridad digital, para la gestión documental electrónica y preservación de la información, siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

3.2 Vigencia de la ley o norma reglamentada o desarrollada

Las disposiciones contenidas en el artículo 16 del Decreto 2106 de 2019que sustenta la expedición del proyecto normativo, se encuentran actualmente vigente y no ha tenido limitaciones vía jurisprudencia.

3.3. Disposiciones derogas, subrogadas, modificadas, adicionadas o sustituidas

Se desarrolla el parágrafo del artículo 16 del Decreto 2106 de 2019 a fin de establecer los lineamientos y estándares para que las entidades dispongan de una estrategia de seguridad digital y adoptar el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital

3.4 Revisión y análisis de la jurisprudencia que tenga impacto o sea relevante para la expedición del proyecto normativo (órganos de cierre de cada jurisdicción)

No existen decisiones judiciales de los órganos de cierre de cada jurisdicción que puedan tener impacto o ser relevantes para la expedición del acto administrativo.

3.5 Circunstancias jurídicas adicionales

No existe ninguna otra circunstancia jurídica que deba ser atendida al ser relevante para la expedición del acto.

4. IMPACTO ECONÓMICO (Si se requiere)

(Por favor señale el costo o ahorro de la implementación del acto administrativo)

La expedición de la resolución que aquí se estudia no representa una erogación económica adicional a la que vienen haciendo las entidades destinatarias para mantener sus inversiones en software, hardware y servicios, antes bien, se espera que en el mediano plazo se logren unos ahorros en estos rubros.

5. VIABILIDAD O DISPONIBILIDAD PRESUPUESTAL (Si se requiere)

(Por favor indique si cuenta con los recursos presupuestales disponibles para la implementación del proyecto normativo)

El proyecto de resolución no representa nuevas disponibilidades presupuestales a las ya dispuestas en el marco de la política de gobierno digital.

6. IMPACTO MEDIOAMBIENTAL O SOBRE EL PATRIMONIO CULTURAL DE LA NACIÓN (Si se requiere)

(Por favor indique el proyecto normativo tiene impacto sobre el medio ambiente o el Patrimonio cultural de la Nación)

El proyecto de resolución bajo análisis tiene un impacto muy positivo sobre el medio ambiente, pues se espera que con la adopción de los lineamientos y estándares para que las entidades dispongan de una estrategia de seguridad digital y la adopción del modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital, aumente la demanda por los servicios y trámites en línea, con la consecuente disminución del uso del papel, en armonía con la estrategia cero papel que desde hace unos años ha impulsado el Gobierno Nacional y este Ministerio.

De otra parte, el proyecto de decreto no tiene un impacto sobre el patrimonio cultural de la Nación

7. ESTUDIOS TÉCNICOS QUE SUSTENTEN EL PROYECTO NORMATIVO (Si cuenta con ellos)

ANEXOS:	
Certificación de cumplimiento de requisitos de consulta, publicidad y de incorporación en la agenda regulatoria *(Firmada por el servidor público competente –entidad originadora)*	N/A por el momento, dado que hasta ahora se publicará para consulta
Concepto(s) de Ministerio de Comercio, Industria y Turismo *(Cuando se trate de un proyecto de reglamento técnico o de procedimientos de evaluación de conformidad)*	N/A
Informe de observaciones y respuestas *(Análisis del informe con la evaluación de las observaciones de los ciudadanos y grupos de interés sobre el proyecto normativo)*	N/A por el momento, dado que hasta ahora se publicará para consulta
Concepto de Abogacía de la Competencia de la Superintendencia de Industria y Comercio *(Cuando los proyectos normativos tengan incidencia en la libre competencia de los mercados)*	N/A
Concepto de aprobación nuevos trámites del Departamento Administrativo de la Función Pública *(Cuando el proyecto normativo adopte o modifique un trámite)*	N/A
Otro *(Cualquier otro aspecto que la entidad originadora de la norma considere relevante o de importancia)*	N/A

Aprobó:

AURA MARIA CIFUENTES
Directora de Gobierno Digital

MANUEL DOMINGO ABELLO
Director Jurídico

Elaboró: Marco Emilio Sánchez – Contratista Dirección de Gobierno Digital
Angela Janeth Cortés Hernández – Asesora Despacho Viceministerio de Transformación Digital
Danny Alejandro Garzón Aristizábal – Contratista Equipo técnico Dirección de Gobierno Digital

Revisó: Juan Carlos Noriega - Asesor Despacho Viceministerio de Transformación Digital
Margarita Ricardo - Asesora Despacho Viceministerio de Transformación Digital
Walid David – Asesor Despacho Ministra de Tecnologías de la Información y las Comunicaciones
Manuel Domingo Abello Alvarez – Director Jurídico
Vanessa Gallego – Asesora Despacho de la Ministra de Tecnologías de la Información y las Comunicaciones

Aprobó: German Rueda – Viceministro de Transformación Digital