MODELO NACIONAL DE GESTIÓN DE RIESGOS DE **SEGURIDAD DIGITAL**

GOBIERNO DE COLOMBIA

Tabla de contenido

Tabla de imágenes

Índice de tablas

Introducción

El avance tecnológico y el uso masivo de las tecnologías de la información y las comunicaciones (TIC) han permitido optimizar las actividades ejecutadas por las entidades colombianas ya sean de carácter público, privado o de cualquier índole. Este avance ha incrementado el uso de las TIC, particularmente en la prestación de servicios esenciales a la nación.

En los últimos veinte años el acceso a internet ha desempeñado un papel significativo en los sectores económicos y sociales a nivel mundial y lo convierte en una herramienta clave para la interacción continua entre las diversas instancias tales como la ciudadanía, entidades y Gobiernos.

Así mismo, los cambios provocados por la evolución continua de la tecnología, y en general de las redes informáticas, han inclinado a algunas entidades y ciudadanos a utilizarlas como medios para incrementar su productividad, para ser más competitivos en los negocios, para satisfacer necesidades propias y para generar valor. Por otra parte, en otros escenarios se ha incrementado el uso de la tecnología con fines delictivos o para generar amenazas informáticas; este propósito busca afectar otras infraestructuras tecnológicas, sistemas de información financieros, personas e, incluso, llegar a impactar la economía de toda una nación. Es por esta razón, que los estados han incrementado su preocupación por los riesgos a los que puedan estar expuestas las instituciones (entidades, organizaciones, empresas y la misma ciudadanía) y han decidido incluir en sus planes estratégicos modelos de ciberseguridad y ciberdefensa encaminados básicamente a fortalecer la seguridad de su nación y por ende, de todos los que la componen.

En Colombia, gracias a las estrategias desarrolladas por el MinTIC, durante el primer trimestre de 2017, se cuenta con una cifra de veintiocho millones de

conexiones a internet de banda ancha[1], lo que evidencia un aumento considerable en la economía digital del país. Así mismo, conscientes de que la seguridad digital es fundamental para el desarrollo del país, en los últimos años se ha puesto a la vanguardia la lucha contra las amenazas en el ámbito digital con estrategias tales como: la creación de lineamientos como la Política para Ciberseguridad y Ciberdefensa (CONPES 3701 y 3854), un modelo de seguridad y privacidad de la información (MSPI) y misiones de asistencia técnica internacional. Igualmente, el apoyo de diferentes organizaciones para la prevención y gestión de incidentes (MinTIC, Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT, Equipo de respuesta a incidentes de seguridad informática CSIRT, - Centro Cibernético Policial de la Policía Nacional), los mecanismos de investigación (Fiscalía General de la Nación, Centro Cibernético Policial) y de judicialización (rama judicial). Con el conjunto de estas organizaciones se busca aumentar la capacidad de defensa ante las amenazas presentes en el medio digital.

De igual forma, el Gobierno colombiano ha facilitado la creación de políticas como el CONPES 3854 de 2016 para la protección del entorno digital y cibernético; en él se involucran a todos los ciudadanos y sectores económicos para fortalecer la prosperidad económica, social y ambiental del país. Es aquí donde aquellas infraestructuras críticas de la nación toman un valor preponderante y se hace necesario ser más especializados en esta identificación, al punto de determinar cuáles de ellas se pueden considerar infraestructuras críticas cibernéticas (ICC), que, al estar inmersas en un ambiente altamente digital, presentan mayor exposición a riesgos que pueden afectar a la nación a nivel social, ambiental y por supuesto, económico.

Dado lo anterior, el Gobierno ha designado al Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC, la elaboración del Modelo Nacional de

---

[1]http://www.eltiempo.com/tecnosfera/novedades-tecnologia/numero-de-conexiones-a-banda-ancha-en-colombia-116374

Gestión de Riesgos de Seguridad Digital, de ahora en adelante (MGRSD), como respuesta a lo definido en la estrategia E.1.2[2] del documento CONPES 3854 y su plan de acción y seguimiento (PAS). Este modelo está basado en buenas prácticas nacionales e internacionales para la gestión de riesgos y tiene como fin contribuir a la prosperidad económica y social, por medio de acciones que conlleven al aprovechamiento de un entorno digital seguro.

Así mismo, el MGRSD se articula con los lineamientos emitidos por el comando conjunto cibernético (CCOC) en lo relacionado con infraestructura crítica cibernética (ICC), lo que permite a las entidades gestionar los riesgos que afectan sus procesos misionales donde se involucran tecnologías de operación que son críticas para el país.

Finalmente, el modelo se complementa con una serie de guías que orientan el uso y la aplicación del MGRSD, en las cuales se tienen en cuenta la naturaleza de la entidad, el sector económico donde se desarrolla la misión u objetivo principal e incluso, de forma directa, al ciudadano común.

[2] El Ministerio de Tecnologías de la Información y las Comunicaciones diseñará un modelo de gestión de riesgos de seguridad digital, teniendo en cuenta el marco conceptual de esta política, los estándares de seguridad internacionales y el marco de gestión de riesgos integral a nivel nacional. El modelo debe 1. ser parte integral del proceso de toma de decisiones; 2. estar soportado en el conjunto de principios fundamentales de la política nacional de seguridad digital; 3. incluir los mecanismos para identificar, evaluar y tratar el riesgo de seguridad digital, así como para seleccionar medidas de seguridad, de preparación y de recuperación; y 4. asegurar la aplicación de protocolos seguros y de controles respectivos para medir la efectividad en la implementación por parte de las múltiples partes interesadas. Dicho modelo debe incorporar los lineamientos y orientaciones que emita la comisión nacional digital y de información estatal.

1. Generalidades

1.2 Derechos de autor

Todas las referencias a los documentos del modelo nacional de gestión de riesgos de seguridad digital son derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

De igual forma, son derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, todas las referencias a las políticas, definiciones o contenido relacionados con los documentos del modelo nacional de gestión de riesgos de seguridad digital publicadas en el compendio de las normas técnicas colombianas vigentes.

En consecuencia, el Ministerio de Tecnologías de la Información y las Comunicaciones goza de los derechos de autor[3] establecidos en la ley 23 de 1982 y demás normas concordantes y complementarias, respecto de los documentos del modelo nacional de gestión de riesgos de seguridad digital y su contenido.

---

[3] **Ley 1520 de 2012.** Artículo 5. El artículo 12 de la Ley 23 de 1982 quedará así: "Artículo 12. El autor o, en su caso, sus derechohabientes, tienen sobre las obras literarias y artísticas el derecho exclusivo de autorizar, o prohibir: a) La reproducción de la obra bajo cualquier manera o forma, permanente o temporal, mediante cualquier procedimiento incluyendo el almacenamiento temporal en forma electrónica.

Ley 1450 de 2011. Artículo 28. Propiedad intelectual obras en cumplimiento de un contrato de prestación de servicios o de un contrato de trabajo. El artículo 20 de la ley 23 de 1982 quedará así: "Artículo 20. En las obras creadas para una persona natural o jurídica en cumplimento de un contrato de prestación de servicios o de un contrato de trabajo, el autor es el titular originario de los derechos patrimoniales y morales; pero se presume, salvo pacto en contrario, que los derechos patrimoniales sobre la obra han sido transferidos al en cargante o al empleador, según sea el caso, en la medida necesaria para el ejercicio de sus actividades habituales en la época de creación de la obra. Para que opere esta presunción se requiere que el contrato conste por escrito. El titular de las obras de acuerdo a este artículo podrá intentar directamente o por intermedia persona acciones preservativas contra actos violatorios de los derechos morales informando previamente al autor o autores para evitar duplicidad de acciones".

Ley 23 de 1982. Artículo 30. El autor tendrá sobre su obra un derecho perpetuo, inalienable, e irrenunciable para: a) Reivindicar en todo tiempo la paternidad de su obra y, en especial, para que se indique su nombre o seudónimo cuando se realice cualquiera de los actos mencionados en el artículo 12 de esta ley.

Las reproducciones, referencias o enunciaciones de estos documentos deberán ir siempre acompañadas por el nombre o seudónimo del titular de los derechos de autor (Ministerio de Tecnologías de la Información y las Comunicaciones).

Lo anterior, sin perjuicio de los derechos reservados por parte de entidades tales como la *International Standard Organization* (ISO), Icontec, entre otras, respecto de referencias, definiciones, documentos o contenido relacionado en el modelo nacional de gestión de riesgos de seguridad digital y sus documentos o anexos que son de su autoría o propiedad.

1.1. Audiencia

El modelo nacional de gestión de riesgos de seguridad digital está diseñado para ser aplicado por entidades públicas de orden nacional y territorial, organizaciones privadas y mixtas, entidades que conforman la fuerza pública colombiana y ciudadanía en general.

Nota: aun cuando el MGRSD está diseñado para todos los sectores del país, en el caso específico de la ciudadanía o sectores gubernamentales que no tienen asociación alguna de tipo corporativo, se creó una guía independiente con un enfoque orientado al uso cotidiano del entorno digital (familiar, escolar o personal), el cual presentará casos puntuales de riesgos comunes, así como herramientas para gestionarlos. Por lo anterior, se recomienda para esta audiencia específica dirigirse concretamente al documento en mención.

2. Justificación

El Gobierno nacional, a través del documento CONPES 3854 del 11 de abril de 2016 estableció la política nacional de seguridad digital que busca "**fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el País**".[4]

De acuerdo con lo anterior, y para dar cumplimiento a la política nacional de seguridad a través del MinTIC, se desarrolla el presente modelo nacional de riesgos de seguridad digital que tiene como objetivo "alcanzar beneficios sociales y económicos, proveer servicios esenciales, operar infraestructuras críticas, preservar los derechos humanos y los valores fundamentales y proteger a las personas frente a las amenazas de seguridad digital".[5] El modelo está orientando a incrementar la conciencia ciudadana y las capacidades del Gobierno y de las empresas en general para identificar, analizar, evaluar y tratar los riesgos de seguridad digital.

Finalmente, la política nacional de seguridad busca apoyar al país en el cumplimiento de las recomendaciones y las mejores prácticas internacionales en gestión de riesgos de seguridad digital emitidas a nivel mundial y recientemente por la organización para la cooperación y el desarrollo económicos (OCDE). Por lo tanto, este modelo brinda los elementos necesarios para que, a través de las guías,

4 Tomado del CONPES 3854 del 11 de abril de 2016 - numeral 5.1 objetivo general.

5 Tomado del pliego de condiciones definitivo, concurso de méritos abierto FTIC-CM-02-17, elaborar el modelo nacional de gestión de riesgos de seguridad digital bajo los lineamientos establecidos en el CONPES 3854 del 11 de abril de 2016. Pág. 4.

se puedan aplicar las prácticas en todos los sectores del país y se apoye la vinculación de Colombia dentro de esta organización.

3. Alcance del modelo nacional de gestión de riesgos de seguridad digital (MGRSD)

El Ministerio de Tecnologías de la Información y las Comunicaciones ha establecido como su principal meta que un gran número de entidades en Colombia, independiente de si son de carácter público o privado, acojan este modelo como su principal referencia para ejecutar o desarrollar la gestión de riesgos de seguridad digital. La idea es que aquellas entidades que aún no han desarrollado algún proceso de gestión de riesgos, en algún nivel de la organización, consideren la metodología planteada en el presente modelo y desarrollen las guías de orientación para su aplicación; particularmente las guías del sector económico cuando así lo requieran, de acuerdo con los documentos descritos más adelante.

Por otra parte, el Ministerio de Tecnologías de la Información y las Comunicaciones, también es consciente de que en la mayoría de las entidades públicas, privadas o mixtas se han adoptado metodologías de gestión de riesgos de seguridad de la información, con la aplicación de una parte significativa del presente modelo.

Con base en lo anterior y teniendo en cuenta la premisa de "*Construir sobre lo construido*", MinTIC indica a las entidades, que ya tengan adoptada una metodología de gestión de riesgos o algún modelo de riesgos en el marco de seguridad de la información o seguridad digital, para que adapten este MGRSD y tomen en consideración las recomendaciones aquí sugeridas para aplicarlas en las respectivas guías:

Cuatro guías de orientación para la aplicación del modelo para las entidades del 1. Sector público y de Gobierno, 2. Sector mixto y privado, 3. Sector fuerza pública y 4. Dirigida a la ciudadanía. Las tres primeras desarrollan las fases para la aplicación de la gestión del riesgo de la seguridad digital (GRSD), mientras que la última, describe lo que un ciudadano del común debe tener en cuenta para gestionar el riesgo.

La descripción de las guías con su nombre exacto son las siguientes:

- Guía de orientación para la GRSD en el Gobierno nacional, territoriales y sector público;
- Guía de orientación para la GRSD en el sector privado y mixto;
- Guía de orientación para la gestión de riesgos de seguridad digital en la fuerza pública;
- Guía de sensibilización en gestión de riesgos de seguridad digital para la ciudadanía en general.

Trece guías que contienen los riesgos, amenazas y vulnerabilidades de la infraestructura crítica cibernética (ICC) más comunes en el ambiente digital y tecnologías de operación que son aplicables a cada uno de los sectores económicos del país y la misión principal de cada entidad.

Las mencionadas guías de ICC se identifican así:

- Guía para la GRSD el sector infraestructura crítica cibernética alimentación y agricultura
- Guía para la GRSD el sector infraestructura crítica cibernética agua
- Guía para la GRSD el sector infraestructura crítica cibernética comercio, industria y turismo
- Guía para la GRSD el sector infraestructura crítica cibernética educación
- Guía para la GRSD el sector infraestructura crítica cibernética electricidad
- Guía para la GRSD el sector infraestructura crítica cibernética financiero
- Guía para la GRSD el sector infraestructura crítica cibernética gobierno
- Guía para la GRSD el sector infraestructura crítica cibernética RRNN y medio ambiente
- Guía para la GRSD el sector infraestructura crítica cibernética recursos minero-energéticos
- Guía para la GRSD el sector infraestructura crítica cibernética defensa
- Guía para la GRSD el sector infraestructura crítica cibernética salud y protección social

- Guía para la GRSD el sector infraestructura crítica cibernética TIC
- Guía para la GRSD el sector infraestructura crítica cibernética transporte

Nota: la planificación e implementación del MGRSD, en cada entidad, está determinada por las necesidades, objetivos, requisitos de seguridad, procesos misionales y por el tamaño y estructura. Cada aplicación de la gestión del riesgo trae consigo necesidades, audiencias, percepciones y criterios.

Es importante aclarar que el punto en común de todas las entidades será el reporte de información de riesgos a los entes designados por el Gobierno. Para el caso de entidades privadas, este reporte será opcional o voluntario. Para las entidades públicas, será de carácter obligatorio.

4. Glosario

Acceso a la información pública

Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Actitud hacia el riesgo

Enfoque de la organización para evaluar y eventualmente buscar, retener, tomar o alejarse del riesgo. (NTC ISO 31000:2011).

Activo

Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854:2016, pág.56).

Activo cibernético

En relación con la privacidad de la información, se refiere al activo que contiene información que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Amenaza

Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (ISO 2700:2016).

Amenaza cibernética

Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (CONPES 3854).

Análisis del riesgo

Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (NTC ISO 31000:2011).

Apetito de riesgo

Es el máximo nivel de riesgo que los accionistas están dispuestos a aceptar. (Componente COSO ERM II)

Ataque cibernético

Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia).

CCOC

Comando Conjunto Cibernético, grupo de ciberseguridad y ciberdefensa creado por el Ministerio de Defensa para apoyar todos los aspectos relacionados con seguridad cibernética en conjunto con el CCP y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT.

CERT

Computer Emergency Response Team (Equipo de respuesta a emergencias cibernéticas). (Universidad Carnegie-Mellón).

Cibercrímen (Delito cibernético)

Conjunto de actividades ilegales asociadas con el uso de las tecnologías de la información y las comunicaciones, como fin o como medio. (CONPES 3854, pág. 87).

Ciberdefensa

Es el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. (CONPES 3854, pág. 88).

Ciberseguridad

Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio. (CONPES 3854, pág. 87).

Ciberterrorismo

Es el uso del ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o Estado trayendo como consecuencia una violación a la voluntad de las personas. (CONPES 3854, pág. 88).

Ciberdelincuencia

Acciones ilícitas que son cometidas mediante la utilización de un bien o servicio informático. (Ministerio de Defensa de Colombia).

Ciberdelito/Delito cibernético

Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia).

Ciberespacio

Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Cibernética

Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnica de funcionamiento de las conexiones de los seres vivos y de las máquinas. (Diccionario de la lengua española).

Cibernético

Adjetivo masculino y femenino para denominar todo cuanto tiene relación con la cibernética: órgano cibernético, proceso cibernético o que está especializado en cibernética, así como también a la persona que se dedica a ella. (Diccionario de la lengua española).

Convergencia

Evolución coordinada de redes que antes eran independientes hacia una uniformidad que permita el soporte común de servicios y aplicaciones. (Rec. UIT-T Q.1761, 3.1).

CSIRT

Por su sigla en inglés: *Computer Security Incident Response Team* (Equipo de respuesta a incidentes de seguridad cibernética). (http:// www.first.org).

Comunicación y consulta

Procesos continuos y reiterativos que una organización lleva a cabo para suministrar, compartir u obtener información e involucrarse en un diálogo con las partes involucradas con respecto a la gestión del riesgo. (NTC ISO 31000:2011).

Consulta

La consulta es un proceso de doble vía de la comunicación informada entre una organización y sus partes involucradas, acerca de algún tema, antes de tomar una decisión o determinar una dirección para dicho tema. La consulta es: un proceso que tiene impacto en la decisión a través de la influencia más que del poder; y: una entrada para la toma de decisiones, no para la toma conjunta de decisiones. (NTC ISO 31000 definición 2.12.).

Compartir el riesgo

Compartir con otra de las partes el peso de la pérdida o el beneficio de la ganancia proveniente de un riesgo particular. (NTC ISO 31000:2011).

Conocimiento, capacidades y empoderamiento

Las múltiples partes interesadas deben entender los riesgos de seguridad digital. Deben ser conscientes de que el riesgo de seguridad digital puede afectar el logro de sus objetivos económicos y sociales, y el de otros. Deben estar educados al respecto, poseer las habilidades necesarias para entender el riesgo, administrarlo y evaluar su impacto. (CONPES 3854, pág. 25).

Consecuencia

Resultado o impacto de un evento que afecta a los objetivos. (NTC ISO 31000:2011).

Contexto externo

Ambiente externo en el cual la organización busca alcanzar sus objetivos. (NTC ISO 31000:2011).

Contexto interno

Ambiente interno en el cual la organización busca alcanzar sus objetivos. (NTC ISO 31000:2011).

Control

Medida que modifica al riesgo. (NTC ISO 31000:2011), medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Cooperación

Las múltiples partes interesadas deben cooperar, incluso más allá de sus fronteras, a nivel regional e internacional.

Criterios del riesgo

Términos de referencia frente a los cuales se evalúa la importancia de un riesgo. (NTC ISO 31000:2011).

Derechos humanos y valores fundamentales

Las múltiples partes interesadas deben gestionar los riesgos de seguridad digital de manera transparente y compatible con los derechos humanos y los valores fundamentales. La implementación de la gestión de riesgos de seguridad digital debe ser compatible con la libertad de expresión, el libre flujo de la información, la confidencialidad de la información, la protección de la privacidad y los datos personales. Las organizaciones deben tener una política general de transparencia acerca de sus prácticas y procedimientos para la gestión de riesgos de seguridad digital.

Entorno digital

Ambiente, tanto físico como virtual, sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web. (CONPES 3854, pág. 87).

Entorno digital abierto

En el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica. (CONPES 3854, pág. 87).

Establecimiento del contexto

Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo y establecimiento del alcance y los criterios del riesgo para la política para la gestión del riesgo. (NTC ISO 31000:2011).

Evaluación del control

Revisión sistemática de los procesos para garantizar que los controles son adecuados y eficaces. (NTC ISO 31000:2011).

Evaluación del riesgo

Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables. (NTC ISO 31000:2011).

Evento de seguridad de la información

Ocurrencia que indica una posible brecha de seguridad de la información o falla de los controles. (ISO/IEC 27035:2016).

Evitar el riesgo

Decisión de no involucrarse o de retirarse de una situación de riesgo. (NTC ISO 31000:2011).

Evento

Presencia o cambio de un conjunto particular de circunstancias. (NTC ISO 31000:2011).

Fuente de riesgo

Elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo. (NTC ISO 31000:2011).

Frecuencia

Medición del número de ocurrencias por unidad de tiempo. (NTC ISO 31000:2011).

Gestión del riesgo

Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. (NTC ISO 31000:2011).

Gestión de riesgos de seguridad digital

Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan

oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego. (CONPES 3854, pág. 24).

ICC

Es la denominación de lo que el CCOC ha definido como infraestructuras críticas cibernéticas en el ámbito colombiano.

Identificación del riesgo

Proceso para encontrar, reconocer y describir el riesgo. (NTC ISO 31000:2011).

Incidente digital

Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).

Incidente de seguridad de la información

Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información de la organización o comprometer sus operaciones. (ISO/IEC 27035:2016).

Infraestructura crítica cibernética nacional

Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública. (CONPES 3854, pág. 29).

Inventario de activos

Sigla en inglés: *Assets inventory*. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos (ISO 27000.ES).

ISO

Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización, cuyo objetivo es establecer, promocionar y gestionar estándares. (http://www.iso.org).

Marco de referencia para la gestión del riesgo

Conjunto de componentes que brindan las bases y las disposiciones de la organización para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo, a través de toda la organización. (NTC ISO 31000:2011).

Monitoreo

Verificación, supervisión, observación crítica o determinación continúa del Estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado. (NTC ISO 31000:2011).

Múltiples partes interesadas

El Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la fuerza pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades. (CONPES 3854, pág. 29).

Nivel de riesgo

Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad. (NTC ISO 31000:2011).

Organización

Grupo de personas e instalaciones con distribución de responsabilidades, autoridades y relaciones. (NTC ISO 31000:2011).

Parte involucrada

Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada, por una decisión o una actividad. (NTC ISO 31000:2011).

Peligro

Una fuente de daño potencial. (NTC ISO 31000:2011).

Pérdida

Cualquier consecuencia negativa o efecto adverso, financiero u otro. (NTC ISO 31000:2011).

Perfil del riesgo

Descripción de cualquier conjunto de riesgos. (NTC ISO 31000:2011).

Política

Intenciones y dirección de una organización como las expresa formalmente su alta dirección. (ISO/IEC 27000:2016).

Política para la gestión del riesgo

Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. (NTC ISO 31000:2011).

Posibilidad

Se utiliza como descripción general de la probabilidad o la frecuencia. (NTC ISO 31000:2011).

Plan para la gestión del riesgo

Esquema dentro del marco de referencia para la gestión del riesgo que especifica el enfoque, los componentes y los recursos de la gestión que se van a aplicar a la gestión del riesgo. (NTC ISO 31000:2011).

Probabilidad

Oportunidad de que algo suceda. (NTC ISO 31000:2011).

Proceso para la gestión del riesgo

Aplicación sistemática de las políticas, los procedimientos y las prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, y de identificación, análisis, evaluación, tratamiento, monitoreo y revisión del riesgo. (NTC ISO 31000:2011).

Propietario del riesgo

Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo. (ISO GUIA 73:2009).

Responsabilidad

Las múltiples partes interesadas deben asumir la responsabilidad de la gestión del riesgo de seguridad digital. Deben rendir cuentas sobre la base de sus funciones y su capacidad para actuar, teniendo en cuenta el posible impacto de sus decisiones sobre los demás. Deben también reconocer que un cierto nivel de riesgo de seguridad digital tiene que ser aceptado para lograr los objetivos económicos y sociales. (CONPES 3854, pág. 25).

Revisión

Acción que se emprende para determinar la idoneidad, conveniencia y eficacia de la materia en cuestión para lograr los objetivos establecidos. (NTC ISO 31000:2011).

Reducción del riesgo

Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo. (NTC ISO 31000:2011).

Resiliencia

Es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. (CONPES 3854, pág. 87).

Retención del riesgo

Aceptación del peso de la pérdida o del beneficio de la ganancia proveniente de un riesgo particular. (NTC ISO 31000:2011).

Riesgo

Efecto de la incertidumbre sobre los objetivos. (NTC ISO 31000:2011).

Riesgo inherente

Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto. (NTC ISO 31000:2011).

Riesgo residual

Remanente después del tratamiento del riesgo. (NTC ISO 31000:2011).

Seguridad de la información

Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas. (ISO/IEC 27001:2016).

Seguridad digital

Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (CONPES 3854, pág. 29).

Servicios esenciales

Los necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las administraciones públicas (Tomado del documento ICC del CCOC).

SGC

Sistema de gestión de calidad.

SGSI

Sistema de gestión de seguridad de la información.

Sistema para la gestión del riesgo

Conjunto de elementos del sistema de gestión de una organización involucrados en la gestión del riesgo. (NTC ISO 31000:2011).

Telecomunicaciones

Toda transmisión y recepción de signos, señales, escritos, imágenes y sonidos, datos o información de cualquier naturaleza por hilo, radiofrecuencia, medios ópticos u otros sistemas electromagnéticos. (Resolución MinTIC 202 de 2010).

TI

Tecnologías de la información.

TO

Tecnología de operación

TIC (Tecnologías de la información y las comunicaciones)

Conjunto de recursos, herramientas, equipos, programas informáticos aplicaciones, redes y medios que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes. (Ley 1341/2009 TIC).

Tratamiento del riesgo

Proceso para modificar el riesgo. (ISO/IEC Guía 73:2009).

Valoración del riesgo

Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo. (ISO GUÍA 73:2009).

Vulnerabilidad

Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (CONPES 3854, pág. 87).

5. Objetivos del MGRSD

5.1 Objetivo general

Brindar un marco de gestión de riesgos de seguridad digital en el cual se identifiquen las amenazas y vulnerabilidades a las que una entidad pueda estar expuesta desde la perspectiva del entorno cibernético, con el fin de fortalecer el ambiente de control, intensificar la confianza de las múltiples partes interesadas en el medio digital e impulsar la prosperidad económica, social de la entidad y, por ende, del país.

5.2 Objetivos específicos

a. Establecer una metodología para la gestión de riesgos de seguridad digital.
b. Orientar a las múltiples partes interesadas en la gestión de riesgos de seguridad digital, incluso aquellas que posean, administren o estén relacionadas con infraestructura crítica cibernética (ICC);
c. Fomentar un modelo de comunicación y de colaboración en la gestión de los riesgos digitales, entre las múltiples partes interesadas;
d. Orientar a la ciudadanía en general sobre el uso responsable del medio digital;
e. Impulsar la economía digital del país mediante la implementación del modelo;
f. Servir de base para facilitar a todo nivel la toma de decisiones sobre aspectos relacionados con la seguridad digital en el país.

6. Propósito y aplicabilidad del MGRSD

Para el diseño de este modelo se han tenido en cuenta el marco conceptual de la política nacional de seguridad digital, los estándares de seguridad internacionales y el marco de gestión de riesgos a nivel nacional; con el cual se pretende:

a. Ser parte integral del proceso para la toma de decisiones en las entidades públicas, privadas, mixtas, la fuerza pública y la ciudadanía en general;
b. Sustentar el modelo de acuerdo con el conjunto de principios fundamentales de la política nacional de seguridad digital;
c. Incluir los mecanismos para identificar, analizar, evaluar y tratar el riesgo de seguridad digital, así como para seleccionar medidas de seguridad, de preparación y de recuperación;
d. Promover a que las múltiples partes interesadas y la ciudadanía en general realicen la aplicación de políticas, procedimientos, protocolos y controles respectivos para garantizar la efectividad en la implementación de la gestión de riesgos de seguridad digital;
e. Incorporar los lineamientos y orientaciones que emita la Comisión Nacional Digital y de Información Estatal[6].

Para la aplicación del presente modelo es importante que la entidad, cualquiera que sea su naturaleza, establezca previamente un gobierno de seguridad de la información con base en las metodologías dispuestas para tal fin. Estas son: el

[6] Comisión nacional digital y de información estatal, su objeto es la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para la interacción con los ciudadanos y el uso efectivo de la información en el Estado colombiano, emitir los lineamientos rectores del grupo de respuesta a emergencias cibernéticas de Colombia del Ministerio de Defensa Nacional y asesorar al Gobierno nacional en materia de políticas para el sector de tecnologías de la información y las comunicaciones, de conformidad con la definición que de éstas hace la ley. https://www.mintic.gov.co/portal/604/articles-3602_documento.pdf Hoja 1 y 2.

modelo de seguridad y privacidad de la información (MSPI) del MinTIC (o del que haga sus veces) o un sistema de gestión de seguridad de la información (SGSI) de acuerdo con estándares como: NTC-ISO/IEC27001:2013 o NTC-ISO 27005:2011, entre otras.

7. Estructura general del modelo nacional de gestión de riesgos de seguridad digital

El Modelo Nacional de Gestión de Riesgos de Seguridad Digital está estructurado como lo indica el siguiente gráfico:

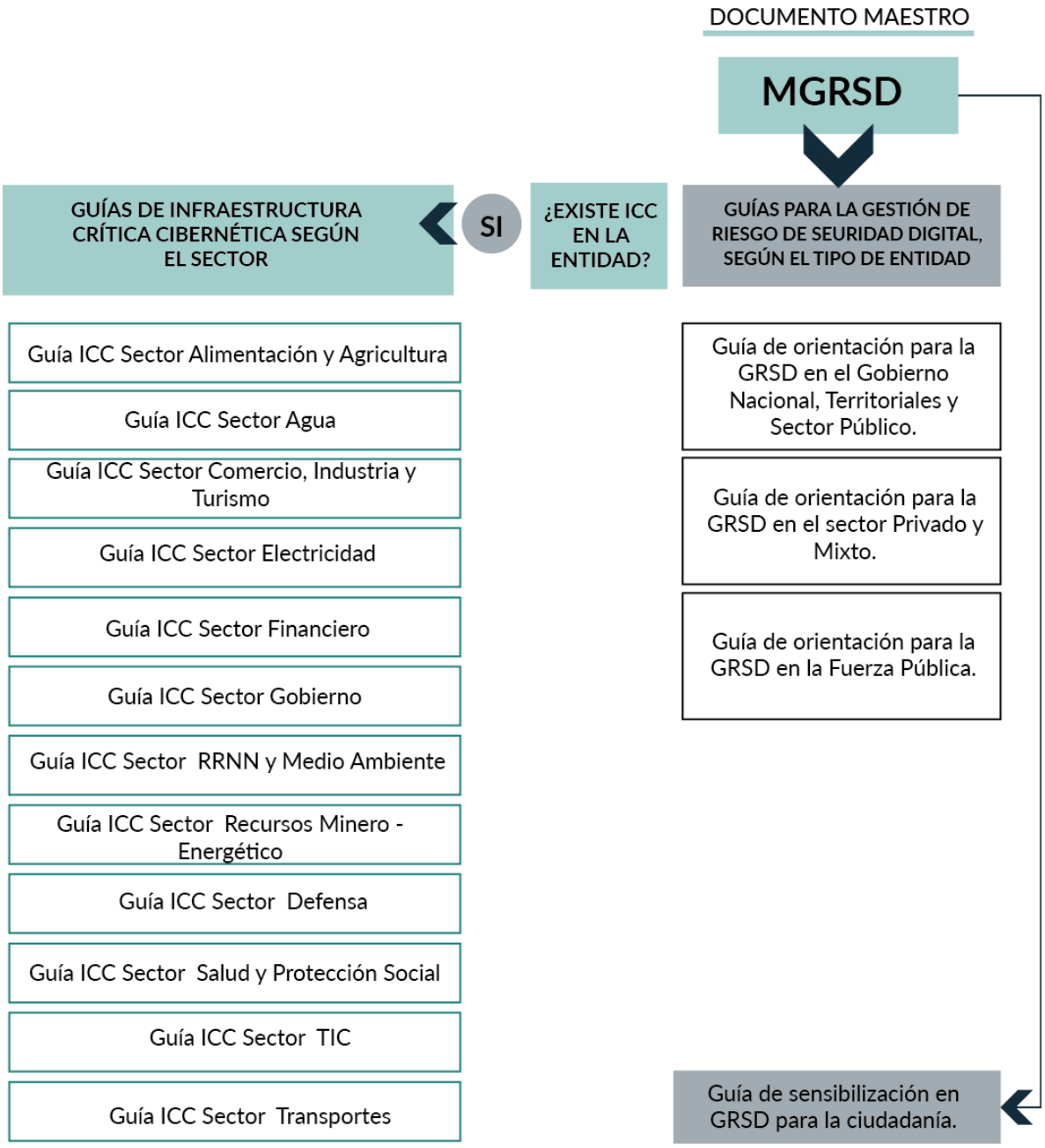

Imagen 1. Interacción del modelo de gestión del riesgo digital: guías de orientación para la GRSD y guías para el sector ICC. Fuente: elaborado por el autor.

Documento maestro: Todas las entidades deberían iniciar con el presente documento maestro MGRSD, el cual hace referencia a los lineamientos generales que establece la gestión de riesgos de seguridad digital.

Guías para la gestión de riesgo de seguridad digital, según el tipo de entidad: para realizar la aplicación del modelo se han propuesto cuatro guías de orientación para la gestión del riesgo de seguridad digital, según el tipo de sector (Gobierno nacional, territoriales y sector público; sector privado y mixto; sector fuerza pública y ciudadanía en general). Las cuales:

- Describen claramente, paso a paso, cómo se debe llevar a cabo la aplicación del modelo en cualquier tipo de entidad y qué elementos debe tener en cuenta un ciudadano del común respecto a la gestión de los riesgos de seguridad digital que le conciernen;
- Contienen actividades que permiten armonizar los objetivos del modelo durante su aplicación.
- Permiten la interacción con las guías de los sectores de infraestructura crítica cibernética en lo concerniente a la identificación de activos, riesgos, amenazas y vulnerabilidades y controles de TI y de TO, asociados a dichas infraestructuras críticas.

Guías de infraestructura crítica cibernética según el sector: adicionalmente, como apoyo al MGRSD y a las guías de orientación para la GRSD, mencionadas, las guías se definen según los sectores de infraestructura crítica cibernética. Estas tienen como objetivo orientar a las entidades que realizan la GRSD sobre infraestructuras críticas cibernéticas (ICC), en lo relacionado a los tipos de activos, riesgos, amenazas, vulnerabilidades y controles, tanto de tecnologías de información (TI) como de tecnologías de operación (TO) que podrían hacer parte de las ICC.

Nota: la aplicación de una o varias guías de infraestructura crítica cibernética se decidirá por parte de cada entidad de acuerdo con el contexto[7], misión, objetivo o razón de ser.

[7] Entiéndase por contexto, todo lo que comprende la misión, visión y objetivos de la entidad.

8. Gestión del riesgo de seguridad digital

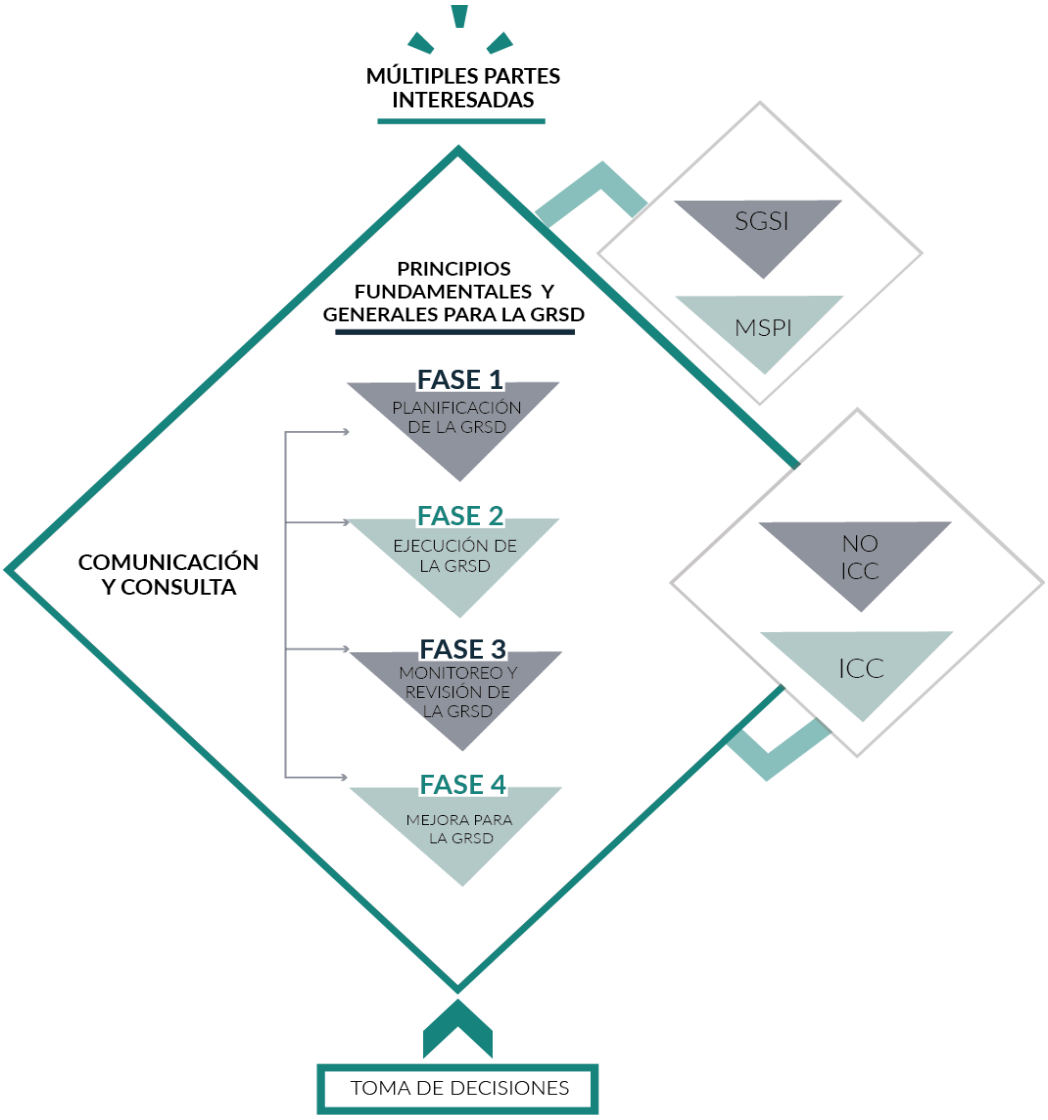

Imagen 2. Marco conceptual del MGRSD. Fuente: elaborado por el autor.

El marco conceptual del Modelo de Gestión de Riesgos de Seguridad Digital (MGSD) provee una guía para la implementación de gestión de riesgos de seguridad digital basado en principios generales y fundamentales donde se establece una interacción con los Sistemas de Gestión de la Seguridad de la Información (SGSI) o para el caso de las entidades del sector público colombiano con el Modelo de

Privacidad y Seguridad de la Información (MPSI); así como la relación con los activos de información que soportan la operación de cualquier Entidad u Organización a nivel general y en particular con las denominadas infraestructuras Criticas Cibernéticas por el CCOC. Los aspectos de seguridad y activos de información incluyendo las mencionadas ICC se interrelacionan con el MGRSD en todas sus fases o componentes:

- ✓ Planificación de la GRSD: Consiste en la definición de contextos, variables para posterior análisis y evaluación de riesgos y en general todos los aspectos que se desarrollarán en los demás componentes.
- ✓ Ejecución de la GRSD: Consiste en el desarrollo de las actividades para el análisis y evaluación de los riesgos de seguridad digital, se identifican aspectos inherentes y residuales de los mismos, así como la definición del tratamiento de los riesgos en el marco de la seguridad de la información y particularmente en las ICC.
- ✓ Monitoreo y Revisión de la GRSD: Consiste en la permanente evaluación que permita asegurar que dicha gestión se está llevando a cabo bajo los aspectos y lineamientos definidos por cualquier entidad para sus riesgos de seguridad digital. Se desprenden aspectos de reporte y aseguramiento del seguimiento de todos los planes de tratamiento que se derivan de su aplicación.
- ✓ Mejora de la GRSD: Componente que tiene una orientación para establecer los mecanismos que permitan alcanzar un mayor grado de madurez de la GRSD en cualquier entidad. El mejoramiento continuo se estará dando de forma progresiva en la medida que se cumplan con los objetivos de la GRSD así como la definición y aplicación modelos de evaluación de riesgos de seguridad digital con una orientación menos subjetiva y basada en modelos matemáticos que brinden mayor exactitud en la medición de las variables de impacto de los riesgos de seguridad digital sobre los activos de información y las ICC identificadas.

Por último, este marco conceptual del MGRSD define la comunicación y consulta como un elemento transversal a cada una de las fases o componentes de la gestión

del riesgo y a su vez orienta a las entidades u organizaciones a una mayor y mejor toma de decisiones frente a los posibles riesgos de seguridad digital, incluyendo las ICC que puedan tener impacto incluso en la seguridad digital de la nación colombiana.

Cada uno de los componentes enunciados en el presente modelo se describe a continuación:

8.1 Múltiples partes interesadas

El MGRSD está diseñado para desarrollar una gestión de riesgos de seguridad digital en cualquier entidad, ya sea pública (de orden nacional o territorial), organización privada, mixta o fuerza pública. El modelo toma como base que la entidad cuenta con un conocimiento previo de seguridad de la información, de la aplicación del MSPI o de un SGSI en el ambiente digital.

De acuerdo con el (CONPES 3854, pág. 29) y en general con los sistemas de gestión mundialmente reconocidos establecen que las múltiples partes interesadas incluyen: el Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la fuerza pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia, la sociedad civil, entes de control a nivel nacional tipo contralorías y personerías, entre otras; y a nivel internacional, entidades como el Banco Interamericano de Desarrollo (BID) o el Banco Mundial (BM), que pueden tener un mayor interés dada la financiación de programas sociales a través de entidades públicas como ministerios o entidades del sector público, entre otros; quienes dependen del entorno digital para todas o algunas de sus actividades económicas y sociales, y quienes pueden ejercer distintos roles y tener diferentes responsabilidades.

8.2 Interacción del MGRSD con el modelo de seguridad y privacidad de la información (MSPI) o sistemas de gestión de seguridad de la información (SGSI)

Conforme lo indica el ámbito de aplicación del decreto 1078 de 2015 respecto a la implementación de la estrategia de gobierno en línea (GEL), las entidades públicas deben realizar la implementación del modelo de seguridad y privacidad de la información (MSPI) con el objetivo de conformar un sistema de gestión de seguridad de la información al interior de la entidad.

En el modelo de seguridad y privacidad de la información (MSPI) se incorpora un componente de gestión de riesgos en las etapas de planificación, implementación evaluación y mejora. Este modelo lo aplican las entidades públicas, privadas y mixtas que en algunos casos tienen la obligatoriedad de ejecutar el sistema de gestión de seguridad de la información (SGSI).

De acuerdo con lo anterior, la relación e interacción entre la gestión de seguridad de la información con el modelo nacional de gestión de riesgos de seguridad digital (MGRSD) se visualiza en la imagen 3 y se describe de la siguiente manera:

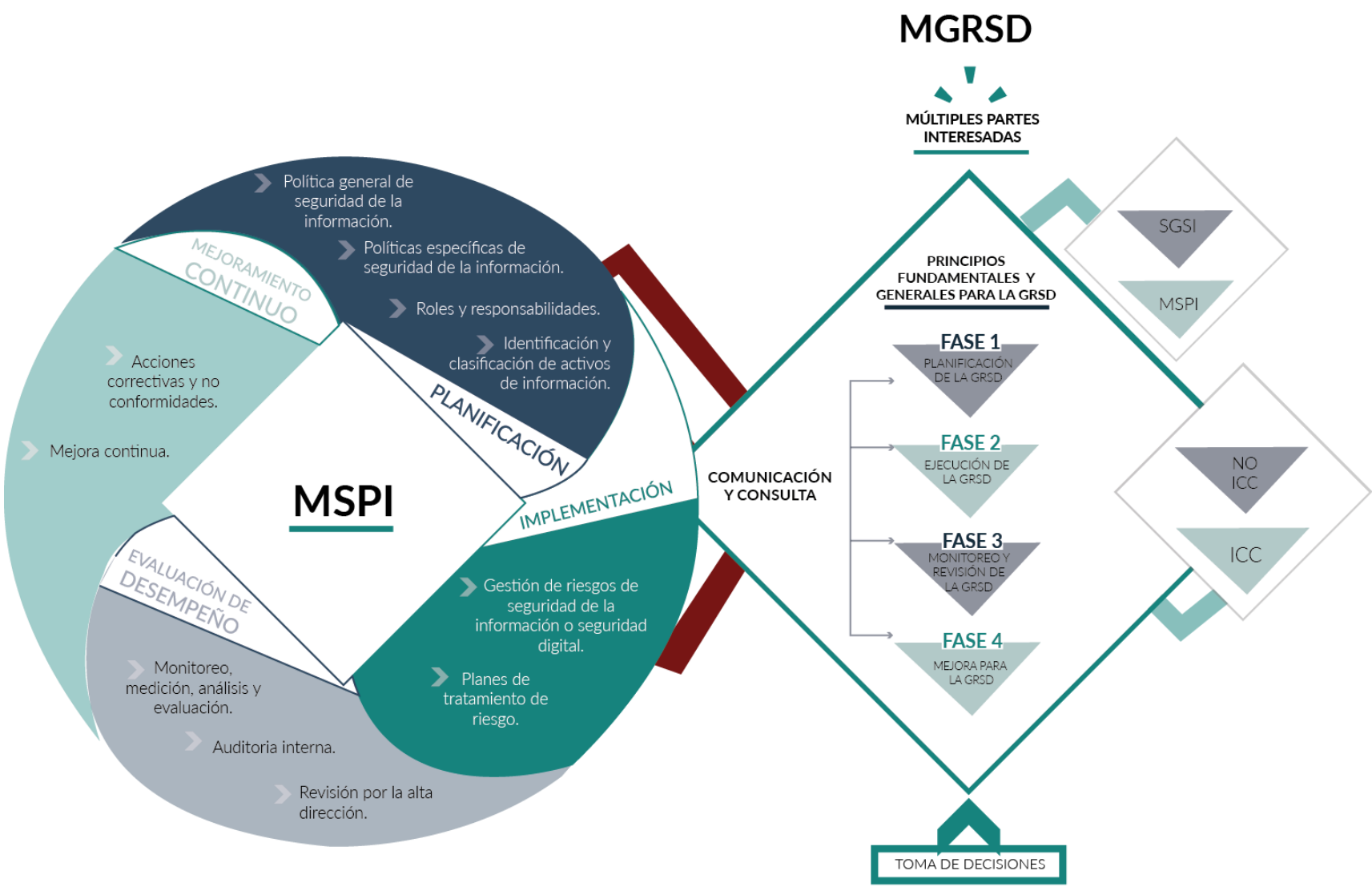

Imagen 3. Interacción entre el MSPI y el MGRSD. Fuente: MinTIC.

Según el llamado Ciclo Deming[8], se definen las actividades en el planear (P), hacer (H), verificar (V) y actuar (A), de cualquier sistema de gestión. En el caso específico de este documento, la gestión de seguridad de la información en el MSPI abarca las etapas de planeación e implementación y en el presente MGRSD se incluye monitoreo, revisión y mejora para las actividades propias de la gestión de riesgos, en este caso, riesgos de seguridad digital.

Es importante aclarar que la gestión de riesgos de seguridad digital no solamente contempla las actividades de identificación, evaluación y tratamiento, sino también la implementación del plan de tratamiento de riesgos conforme a los niveles definidos por cada una de las entidades. Es por esta razón, que los modelos sincronizan conceptos y actividades en las primeras fases, tanto para el MSPI como para el SGSI. Sin embargo, las entidades también deberán aplicar de forma transversal las fases de comunicación y de consulta, así como la de monitoreo y revisión del MGRSD, las cuales están relacionadas con las fases de evaluación del desempeño y mejora continua del MSPI o del SGSI.

8.3 Principios para la gestión del riesgo de seguridad digital

El MGRSD tiene como soporte los siguientes principios fundamentales y generales y está encaminado a crear las condiciones para que las múltiples partes interesadas y la ciudadanía en general puedan gestionar la seguridad digital de sus actividades económicas y sociales. Esto fomenta la confianza en el entorno digital.

Principios fundamentales (PF): los principios fundamentales están establecidos dentro del documento (CONPES 3854 del 11 de abril de 2016); a continuación se presenta su interacción con el MGRSD.

[8] Definido por Edwards Deming es una estrategia de mejoramiento continuo dentro de un ciclo de calidad en cuatro pasos a saber: planear, hacer, verificar y actuar. Tomado y traducido de *The Deming Management Method*, Mary Walton.

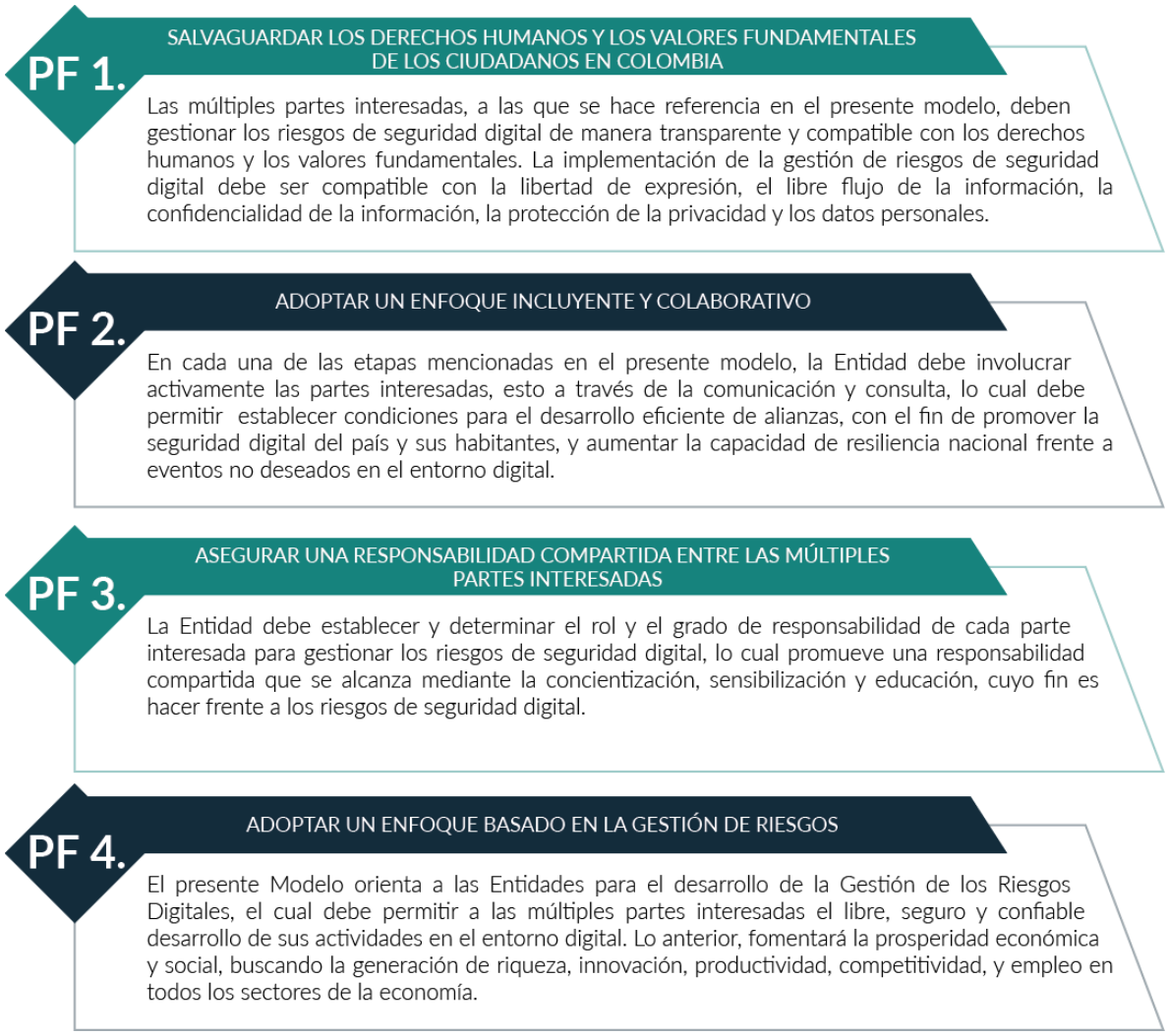

Imagen 4. Principios fundamentales para la GRSD. Fuente: elaborado por el autor.

Principios generales (PG): los principios generales estan basados en lo definido por la norma para la gestión del riesgo: principios y directrices. NTC-ISO 31000:2011.e Estos principios se encuentran inmersos en el desarrollo del MGRSD y las guías correspondientes a todos los sectores económicos del país. Las entidades pueden adoptar los principios de manera progresiva, con el fin de promover una conducta de gestión de riesgos de seguridad digital.

PG 1. LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL CREA Y PROTEGE EL VALOR

Mediante la Gestión de Riesgos, la Entidad garantiza un entorno digital seguro y abierto, que generaconfianza en los ciudadanos para que se incrementen sus participantes, y se fortalezca la economía digital del país.

PG 2. LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL ES UNA PARTE INTEGRAL DE TODOS LOS PROCESOS DE LA ORGANIZACIÓN

La entidad debe incluir todos los procesos organizacionales que las soportan al realiar la Gestión de Riesgos de Seguridad Digital.

PG 3. LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL ES PARTE DE LA TOMA DE DESICIONES

El presente modelo establece la toma de desiciones como una salida en la Gestión de Riesgos de Seguridad Digital., pues la Entidad al tomar sus desiciones bajo este enfoque soportan los objetivos de las actividades socioeconómicas y no las debilitará.

PG 4. LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL ABORDA EXPLICITAMENTE LA INCERTIDUMBRE

La creciente relevancia del entorno digital sobre las actividades socioeconomicas, y su alto dinamismo, ha traído consigo un conjunto de incertidumbres, riesgos, amenazas, vulnerabilidades e incidentes e diversos tipos, a los que se encuentran expuestos los individuos y las organizaciones, públicas y privadas. Riesgos de Seguridad Digital acarrean rincertidumbres, por eso deben gestionarse constantemente.

PG 5. LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL ES PARTE DE LA TOMA DE DESICIONES

La evaluación de riesgos debe llevarse a cabo de manera sistemática y continua, evaluando las posibles consecuencias de las amenazas y las vulnerabilidades digitales en las actividades económicas y sociales en juego.

PG 6. LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL SE BASA EN LA MEJOR INFORMACIÓN DISPONIBLE.

Para una adecuada gestión del riesgo, la entidad en cada una de las fase enunciadas en el presente modelo, debe tomar como base información verídica como datos históricos, experiencia, retroalimentación de las partes involucradas, entre otros.

PG 7. LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL ESTÁ ADAPTADA.

La gestión de los riesgos de seguridad digital se alinea con otros sistemas de gestión de riesgos que la entidad tenga implementados.

PG 8. LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL TOMA EN CONSIDERACIÓN LOS FACTORES HUMANOS Y CULTURALES.

La entidad debe considerar las capacidades, percepciones e intenciones de individuos externos es internos, los cuales pueden facilitar o dificultar el logro de los objetivos de la organización.

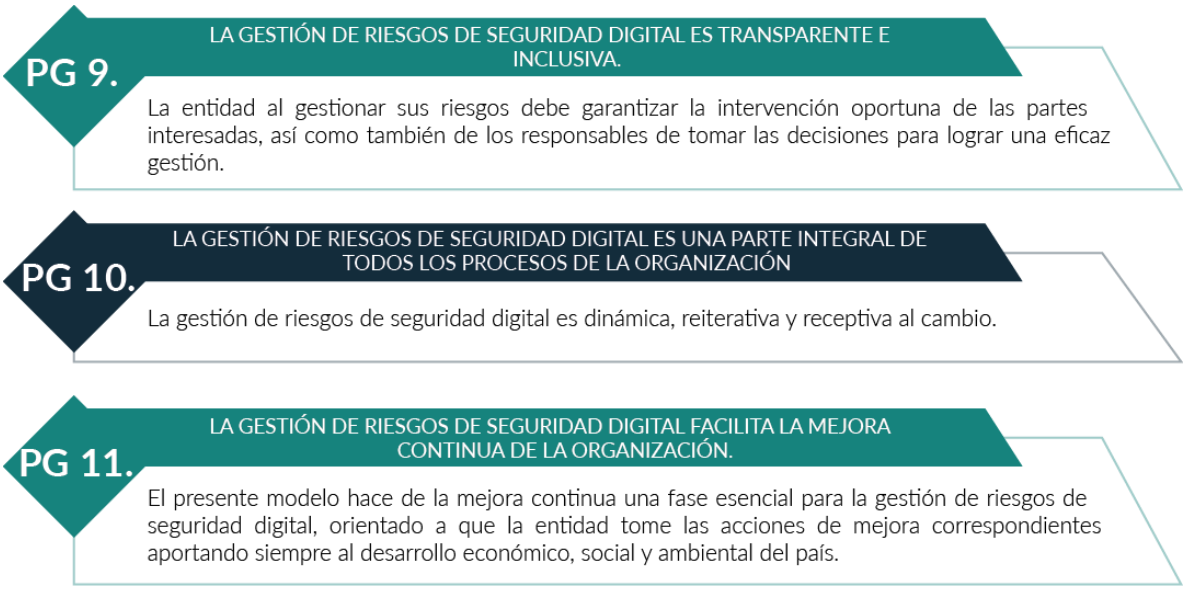

Imagen 5. Principios generales para la GRSD. Fuente: elaborado por el autor.

8.4 Fase 1. Planificación de la gestión de riesgo de seguridad digital (GRSD)

Imagen 6. Descripción de la fase 1. Planificación de la GRSD. Fuente: elaborado por el autor.

El propósito de la planificación de la gestión del riesgo de seguridad digital es esencial, pues es el punto de partida para el desarrollo de la GRSD, la cual se centra

en la ejecución de una serie de actividades previas y orienta a las entidades para que establezcan o formalicen:

a. Un compromiso de la alta dirección;
b. El establecimiento del contexto organizacional en el entorno digital;
c. La identificación de partes interesadas y procesos donde se desarrollará la gestión de seguridad digital;
d. El desarrollo de una política de gestión de riesgo o la armonización con una política de seguridad de la información existente;
e. La definición de roles y responsabilidades para la gestión de riesgos de seguridad digital;
f. Los recursos necesarios para la gestión de riesgos de seguridad digital;
g. Los criterios para la gestión del riesgo de seguridad digital.

Estos aspectos deben ser definidos en conjunto con la alta dirección de la entidad y con los involucrados en los procesos o áreas objeto de la gestión de riesgos de seguridad digital.

8.4.1 Liderazgo y compromiso de la alta dirección

El liderazgo y compromiso se establece desde la fase de planificación, de esta forma la entidad garantiza que la gestión del riesgo de seguridad digital sea pertinente y actualizada periódicamente.

La alta dirección debe adquirir el compromiso de facilitar el cumplimiento de los objetivos sobre la gestión del riesgo de seguridad digital, a través del establecimiento de políticas, roles y responsabilidades, que aporten los recursos necesarios para que el proceso se desarrolle en la entidad de forma efectiva.

8.4.2 Establecimiento del contexto organizacional en el entorno digital

Dentro del contexto organizacional interno y externo, es importante que la entidad que tome como referencia este modelo para la gestión de los riesgos de seguridad digital, identifique cuáles son los aspectos que generan mayor impacto en los

procesos misionales y cuáles son los objetivos organizacionales relacionados con el medio digital (usuarios, infraestructura, servicios y aplicaciones); una vez detectados, permite tomar decisiones acertadas dentro del proceso de gestión de riesgos de seguridad digital. Por lo tanto, en la medida en que se vayan presentando cambios en el contexto, se pueden presentar nuevos eventos o riesgos que deben ser atendidos como parte del proceso.

Nota: para implementar esta actividad, se establece el numeral 4.1.2. Contexto de la entidad, dentro de las guías de orientación para la gestión de riesgos de seguridad digital, de acuerdo con el tipo de entidad al que pertenece (Gobierno nacional, entes territoriales y sector público, mixto y privado, así como las entidades relacionadas con la fuerza pública).

8.4.3 Identificación de partes interesadas y procesos donde se aplique la gestión de gestión de seguridad digital

La entidad debe identificar las partes interesadas que afecten o puedan verse afectadas en el entorno digital. Estas se definen en el numeral 8.1. *Múltiples partes interesadas* del presente documento.

De igual forma, como parte de la fase de planificación, se hace necesaria la identificación de los procesos en los cuales se desarrolla la gestión de riesgos de seguridad digital.

Nota: para implementar esta actividad, se establece el numeral 4.1.3. Identificación de las partes interesadas, dentro de las guías de orientación para la gestión de riesgos de seguridad digital, de acuerdo con el tipo de entidad al que pertenece (Gobierno nacional, entes territoriales y sector público, mixto y privado, así como fuerza pública).

8.4.4 Asociación de la política de gestión de riesgos de seguridad digital con políticas existentes

Para la asociación de la política de gestión de riesgo de seguridad digital, la entidad debe tener en cuenta los lineamientos establecidos por los diferentes sistemas de gestión de riesgos ya implementados internamente, con el fin de que las políticas se armonicen en una sola. Lo anterior, debe considerarse como parte de evidencia del compromiso con la GRSD y evitar la multiplicidad de políticas.

Si la entidad no cuenta con ninguna política, debe desarrollar una en la que se evidencie el compromiso de aplicar la GRSD.

Nota: para implementar esta actividad, se establece el numeral 4.1.5. Asociación de la política de gestión de riesgos de seguridad digital con políticas existentes, dentro de las guías de orientación para la gestión de riesgos de seguridad digital, de acuerdo con el tipo de entidad al que pertenece (Gobierno nacional, entes territoriales y sector público, mixto y privado, así como fuerza pública).

8.4.5 Definición de roles y responsabilidades para la gestión de riesgos de seguridad digital (GRSD)

Según los principios generales, la gestión del riesgo es una actividad que se realiza en toda la organización. Por lo tanto, la dirección es responsable de apoyar el proceso en su totalidad. Esto incluye la planificación estratégica, la gestión de proyectos y la gestión de cambio, entre otros.

Por otra parte, la GRSD debe ser compromiso de cada uno de los integrantes de la entidad, no obstante, la gestión es responsabilidad de los líderes de proceso, los cuales son los propietarios de los riesgos. Igualmente, la entidad al aplicar el MGRSD debe definir claramente quién se hará cargo de la coordinación, seguimiento, reporte de los avances, logros e inconvenientes relacionados con la gestión de los riesgos de seguridad digital.

Nota: para implementar esta actividad, se establece el numeral 4.1.6. Definición de roles y responsabilidades, dentro de las guías de orientación para la gestión de riesgos de seguridad digital, de acuerdo con el tipo de entidad al que pertenece

(Gobierno nacional, entes territoriales y sector público, mixto y privado, así como fuerza pública).

8.4.6 Recursos para el desarrollo de la gestión de riesgos de seguridad digital

La entidad debe destinar recursos suficientes para el desarrollo de la GRSD y realizar de manera periódica el seguimiento y control de:

- La ejecución del presupuesto asignado para la GRSD;
- Los recursos humanos destinados para tal efecto;
- Las herramientas que se determinen para la aplicación de los controles;
- En general, todo lo asociado con los proyectos estratégicos donde se registre evidencia del desarrollo de esta actividad.

Nota: para implementar esta actividad, se establece el numeral 4.1.7. Definición de recursos, dentro de las Guías de orientación para la gestión de riesgos de seguridad digital, de acuerdo con el tipo de entidad al que pertenece (Gobierno nacional, entes territoriales y sector público, mixto y privado, así como fuerza pública).

8.4.7 Criterios para la gestión del riesgo de seguridad digital

Esta actividad en la etapa de planeación es quizá la que mayor importancia tiene para la aplicación del resto de actividades del proceso de GRSD. La entidad deberá establecer los niveles de referencia frente a los cuales se determina la importancia del riesgo. En consecuencia, se deben tener en cuenta los criterios de probabilidad e impacto, su valoración, el tratamiento de los riesgos, las cualidades y características de los controles, los criterios de riesgo y el apetito o zona de aceptación del riesgo.

La entidad puede definir escalas de medición de forma autónoma o basada en metodologías adoptadas previamente. La determinación del número de criterios de impacto y probabilidad, así como los de la zona de riesgos, es una decisión propia de la entidad. Por lo tanto, puede definir si utiliza niveles de probabilidad e impacto

con 3, 4, 5, 6 o 7 criterios por cada variable, así como tres o cuatro zonas de riesgo (que se dan tras la combinación de impacto y probabilidad por riesgo analizado).

Por otra parte, las variables para determinar el nivel de impacto que tenga la materialización del riesgo analizado sobre el activo de información identificado (el cual puede ser una ICC), se definen así: confidencialidad, integridad y disponibilidad de la información digital, como también los aspectos social, económico y ambiental que se pueden generar a través de la materialización de los riesgos. Las tres últimas variables están definidas en la guía de identificación de infraestructura crítica cibernética del CCOC; así que cada entidad que decida establecer la gestión de riesgos de seguridad digital, debe determinar si posee o no ICC a nivel nacional.

Nota: para implementar esta actividad, se establece el numeral 4.1.8. Establecimiento de criterios, dentro de las guías de orientación para la gestión de riesgos de seguridad digital, de acuerdo con el tipo de entidad al que pertenece (Gobierno nacional, entes territoriales y sector público, mixto y privado, así como fuerza pública).

8.5 Fase 2. Ejecución de la gestión de riesgos de seguridad digital (GRSD)

Esta fase contempla las actividades para la ejecución de la gestión de riesgos de seguridad digital. Cada una de las acciones define sus salidas o entregables, las cuales se ilustran a continuación:

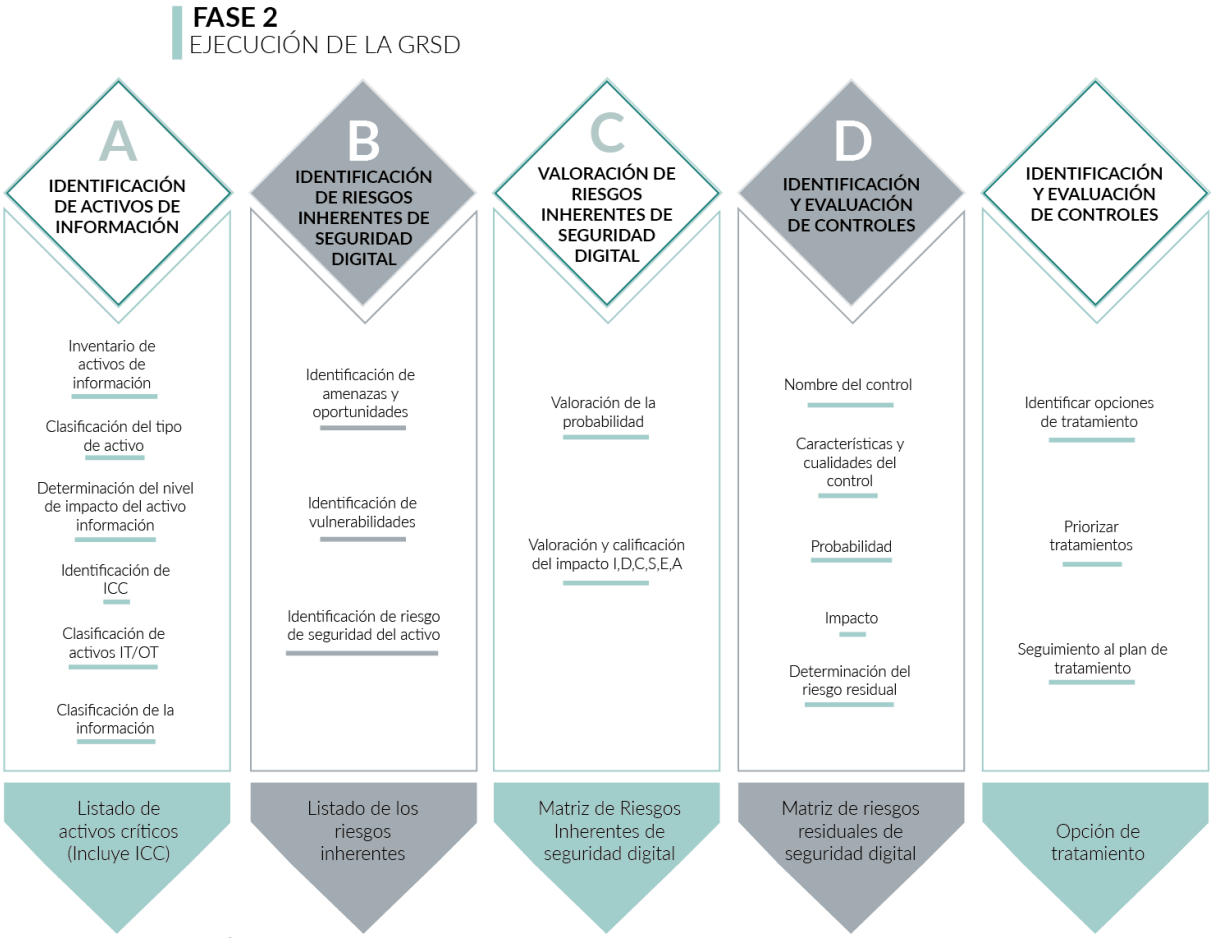

Imagen 7. Ejecución de la GRSD. Fuente: elaborado por el autor

Las actividades propias de la fase 2, se describen a continuación:

Identificación de los activos de información: la entidad debe identificar todos los activos de información (se incluyen los que corresponden a las ICC) y se clasifican de acuerdo con la normatividad vigente y aplicable (por ejemplo, para entidades públicas se deben tener en cuenta la ley 1712 de 2014 y la ley 1581 de 2012), que determinan la importancia del activo para la entidad e identifican el nivel de criticidad.

Es importante resaltar que si la entidad presta servicios esenciales, *"los necesarios para el mantenimiento de las funciones sociales básicas, salud, seguridad, bienestar social y económico de los ciudadanos o el funcionamiento de las*

instituciones del Estado y las administraciones públicas"[9], se deben establecer cuáles de los servicios esenciales hacen parte de la infraestructura crítica nacional, de acuerdo con los criterios de criticidad definidos por el CCOC, en la *"Guía para la identificación de infraestructura crítica cibernética (ICC) de Colombia Primera Edición"*[10] y en ese caso, deben reportarse al CCOC y, posteriormente, a la aplicación del proceso de la GRSD. Es decir, se deben reportar las ICC identificadas en la entidad y también los riesgos asociados a estas infraestructuras críticas.

Nota: para implementar esta actividad, se establece el numeral 4.2.1 Identificación de activos de información, dentro de las guías de orientación para la gestión de riesgos de seguridad digital, de acuerdo con el tipo de entidad al que pertenece (Gobierno nacional, entes territoriales y sector público, mixto y privado, así como fuerza pública).

Identificación de riesgos inherentes de seguridad digital: para que la entidad identifique los riesgos inherentes de seguridad digital, debe tener en cuenta las amenazas y las vulnerabilidades asociadas a cada activo.

Nota: para implementar esta actividad, se establece el numeral 4.2.2 Identificación de riesgos inherentes de seguridad digital, dentro de las guías de orientación para la gestión de riesgos de seguridad digital, de acuerdo con el tipo de entidad al que pertenece (Gobierno nacional, entes territoriales y sector público, mixto y privado, así como fuerza pública).

Valoración de riesgos inherentes de seguridad digital: una vez identificados los riesgos inherentes de seguridad digital para cada activo identificado, se deben

---

[9] Guía para la identificación de infraestructura crítica cibernética (ICC) de Colombia, primera edición CCOC.

10 Guía para la identificación de infraestructura crítica cibernética (ICC) de Colombia, primera edición CCOC.

determinar la probabilidad e impacto de los criterios establecidos, durante la fase de planeación.

Nota: para implementar esta actividad, se establece el numeral 4.2.3 Valoración de riesgos inherentes de seguridad digital, dentro de las guías de orientación para la gestión de riesgos de seguridad digital, de acuerdo con el tipo de entidad al que pertenece (Gobierno nacional, entes territoriales y sector público, mixto y privado, así como fuerza pública).

Identificación y evaluación de controles: por cada riesgo inherente de seguridad digital identificado, se deben establecer los controles asociados. Así mismo, se determinan las cualidades y características de cada control, que tienen la posibilidad de disminuir el nivel de riesgo, desplazarlas a una zona de riesgo menor a la inherente y determinar si definitivamente es aceptable o no.

Lo anterior significa que, dependiendo de la efectividad de los controles asociados (o ya existentes) a cada riesgo, se obtiene un nuevo valor de la probabilidad e impacto al identificar el riesgo residual y determinar el tipo de tratamiento que se le debe dar a cada uno de los riesgos.

Nota: para implementar esta actividad, se establece el numeral 4.2.4 Identificación y evaluación de controles, dentro de las guías de orientación para la gestión de riesgos de seguridad digital, de acuerdo con el tipo de entidad al que pertenece (Gobierno nacional, entes territoriales y sector público, mixto y privado, así como fuerza pública).

Tratamiento de los riesgos de seguridad digital: la entidad debe establecer los criterios para definir el o los tratamientos de los riesgos, dependiendo del nivel residual obtenido de seguridad digital.

En esta fase, particularmente, se deben tener claras cuáles son las alternativas de tratamiento de los riesgos. Las buenas prácticas de gestión de riesgos definen que el tratamiento suele darse sobre mitigar, aceptar, transferir o evitar el riesgo.

Ahora bien, independiente del tipo de tratamiento, es importante que la entidad defina los planes de acción que se van a realizar para cada riesgo digital. Lo anterior significa que cada plan de acción es un mapa de ruta para acercar el riesgo a la zona de riesgo aceptable. Sin embargo, para aquellos riesgos que no se puedan llevar a esta zona, se debe articular con un plan de continuidad, dado que los riesgos ya no se podrían controlar de manera preventiva.

Nota: para implementar esta actividad, se establece el numeral 4.2.5. Tratamiento de los riesgos de seguridad digital, dentro de las guías de orientación para la gestión de riesgos de seguridad digital, de acuerdo con el tipo de entidad al que pertenece (Gobierno nacional, entes territoriales y sector público, mixto y privado, así como la fuerza pública).

8.6 Fase 3. Monitoreo, revisión y reporte de la gestión del riesgo de seguridad digital

Luego de completar la fase 2, la entidad debe determinar la efectividad de las actividades. Esto se puede hacer mediante una revisión periódica y usando diferentes estrategias como las descritas a continuación:

Imagen 8. Descripción de la fase 3. Monitoreo y revisión de la GRSD. Fuente: elaborado por autor

8.6.1 Revisión por la alta dirección

El compromiso y liderazgo establecido por la alta dirección de la entidad se ve reflejado con la ejecución de revisiones periódicas y el seguimiento al proceso de gestión de riesgo de seguridad digital.

8.6.2 Auditorías internas y externas

Para realizar un monitoreo efectivo, así como las revisiones periódicas a la GRSD, la entidad debe programar y ejecutar auditorías internas y externas, con alcances definidos, con el fin de asegurar la efectividad en la gestión de riesgos de seguridad digital (GRSD).

8.6.3 Medición del desempeño

La entidad podrá asegurar que las medidas de gestión de riesgos de seguridad digital son apropiadas para cumplir los objetivos económicos y sociales, a través de la definición y establecimiento de métricas para evaluar periódicamente la gestión. Esto incluye la definición de indicadores que permitan mantener monitoreados y controlados los riesgos de seguridad digital y así propender por minimizar su materialización.

8.6.4 Rendición de cuentas

Como parte integral de la gestión de riesgos de seguridad digital, es importante tener presente que una vez la entidad haya implementado o adaptado la GRSD bajo este modelo, los resultados obtenidos durante la medición del desempeño y los cambios correspondientes a la mejora continua, deben comunicarse y reportarse a la alta dirección y a las partes interesadas. Lo anterior, con el fin de que la evaluación de riesgos se contemple como insumo para la toma de decisiones.

8.6.5 Reporte de la gestión del riesgo de seguridad digital al interior de la entidad

La entidad debe reportar periódicamente a la alta dirección y a las partes interesadas, la siguiente información:

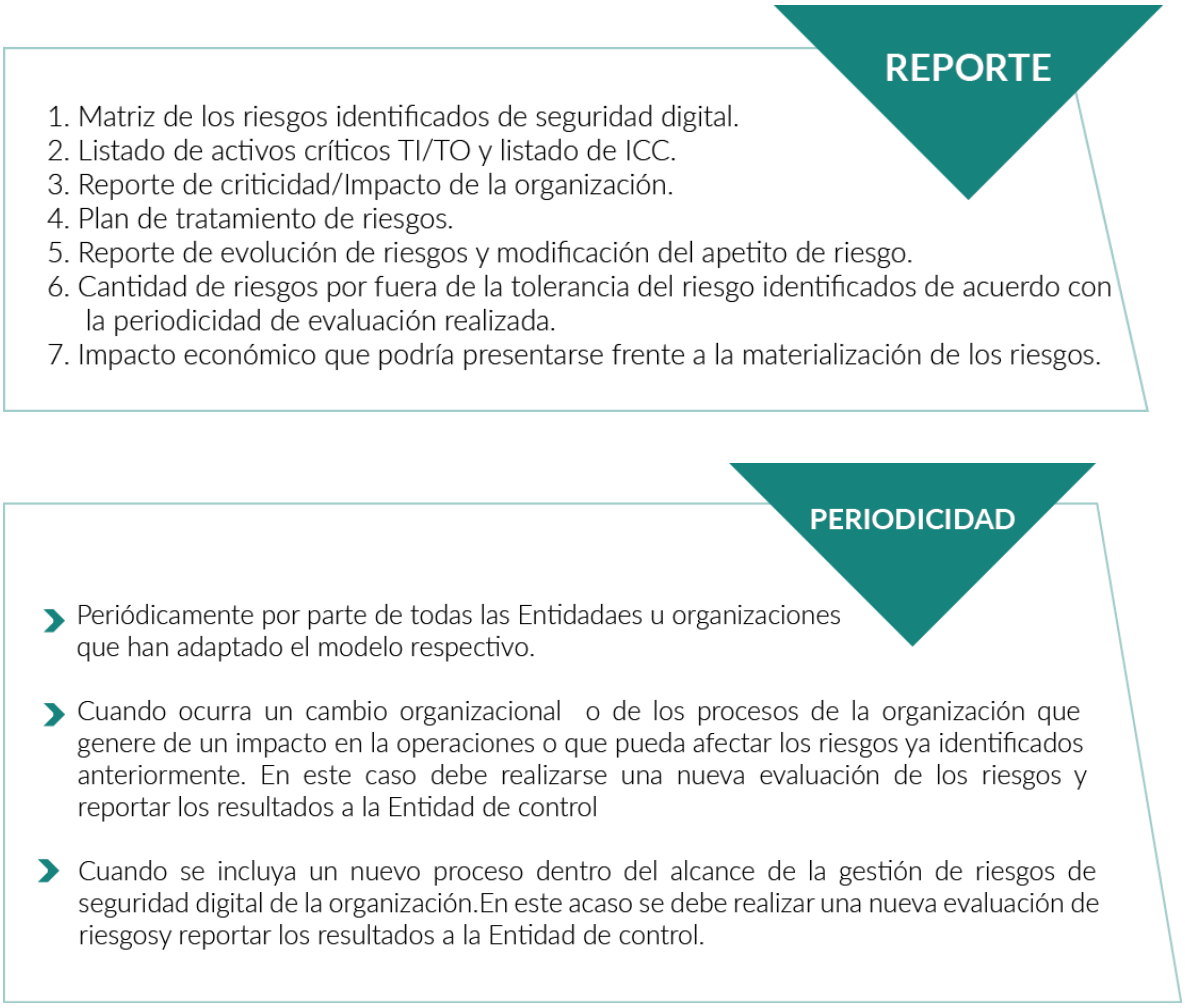

Imagen 9. Reporte de información por parte de la entidad. Fuente. elaborado por MinTIC.

8.6.6 Reporte de la gestión del riesgo de seguridad digital a entidades de interés especial

Una vez la Entidad obtenga los resultados de la gestión de riesgos de seguridad digital (GRSD) deberá consolidar la siguiente información (previamente obtenida con la aplicación del modelo) con el fin de reportarla a los grupos de interés especial según se indicará a continuación:

Información a consolidar:

- Activos digitales críticos

- Riesgos con nivel crítico
- Amenazas críticas
- Vulnerabilidades críticas
- Servicios digitales críticos
- Las infraestructuras críticas cibernéticas (ICC) identificadas y los riesgos, amenazas y vulnerabilidades relacionados con estas.

Reportes a entidades de interés especial, si se es entidad pública:

Los activos y servicios digitales críticos (aquellos que afectan gravemente al funcionamiento de la entidad) y los riesgos, amenazas y vulnerabilidades más importantes identificados durante el ejercicio de riesgos, deberán ser reportados al CSIRT de Gobierno.

Reportes a entidades de interés especial, si se es entidad privada:

Los activos y servicios digitales críticos (aquellos que afectan gravemente al funcionamiento de la entidad) y los riesgos, amenazas y vulnerabilidades más importantes identificados durante el ejercicio de riesgos, deberán ser reportados a la alta dirección de la entidad para la debida gestión interna y a los CSIRT Sectoriales una vez estos se hayan creado.

Reportes a entidades de interés especial, si se es operador o dueño de Infraestructuras Críticas Cibernéticas:

Sean entidades públicas o privadas, las infraestructuras críticas cibernéticas (ICC) que hayan sido identificadas y los riesgos, amenazas y vulnerabilidad críticas relacionados con estas, deberán reportarse al CCOC, dado que es la entidad encargada de administrar esta información.

Nota 1: Los reportes de información a las entidades de interés especial, definidos para entidades públicas son de obligatorio cumplimiento, para las entidades privadas se invita a su realización como ejercicio colaborativo en el fortalecimiento de la seguridad digital del país.

Nota 2: Los reportes previos se realizarán empleando los controles necesarios para garantizar la seguridad y confidencialidad de la información contenidos en ellos (Acuerdos de confidencialidad y controles técnicos adecuados).

Nota 3: para implementar estas actividades, se establece el numeral 4.3. Fase 3. Monitoreo y Revisión, dentro de las guías de orientación para la gestión de riesgos de seguridad digital, de acuerdo con el tipo de entidad al que pertenece (Gobierno nacional, entes territoriales y sector público, mixto y privado, así como las entidades correspondientes a la fuerza pública).

Es importante indicar que los reportes de riesgos de seguridad digital a las entidades de interés especial indicados previamente, no implican o significan el traslado de la responsabilidad sobre los riesgos o su tratamiento.

8.7 Fase 4. Mejora para la gestión del riesgo de seguridad digital

Es claro que la gestión de riesgo de seguridad digital debe orientarse hacia un enfoque cíclico y dinámico, por ende, deberá estar en continua revisión por parte de la entidad[11]. Esto tiene como fin preservar la confidencialidad, integridad y disponibilidad de los activos de información y propender por minimizar los impactos económico, social y ambiental que se puedan derivar de estos riesgos. Una vez sean mejoradas las actividades que correspondan, estas serán incluidas en el plan de comunicaciones de la entidad, a fin de que sean conocidas por todas las partes interesadas.

La entidad debe identificar las oportunidades de mejora conforme a los criterios establecidos en sus diferentes sistemas de gestión. Lo anterior, con el fin de enfocar sus esfuerzos en la mejora de los procesos que hacen parte de la gestión de riesgos de seguridad digital (GRSD).

[11] Guía de mejora continua de la estrategia GEL de MinTIC.

Nota: para implementar esta actividad, se establece el numeral 4.4. Fase 4. Mejoramiento continuo de la gestión del riesgo de seguridad digital, dentro de las Guías de orientación para la gestión de riesgos de seguridad digital, de acuerdo con el tipo de entidad al que pertenece (Gobierno nacional, entes territoriales y sector público, mixto y privado, así como las entidades de la fuerza pública).

8.8 Comunicación y consulta

Esta fase es transversal a toda la gestión de riesgo de seguridad digital. Por lo tanto, se considera esencial dado que permite asegurar su entendimiento por parte de las múltiples partes interesadas. De acuerdo con lo anterior, cada parte interesada deberá comunicar y consultar[12] de acuerdo con sus roles y responsabilidades, los resultados obtenidos como parte de las actividades realizadas en cada una de las fases del MGRSD.

Finalmente, los resultados de la GRSD deberán ser comunicados a la alta dirección para que puedan soportar la toma de decisiones.

Nota: para implementar estas actividades, se establece el numeral 4.4.1. Comunicación y consulta, dentro de las guías de orientación para la gestión de riesgos de seguridad digital, de acuerdo con el tipo de entidad al que pertenece (Gobierno nacional, entes territoriales y sector público, mixto y privado, así como las entidades de la fuerza pública).

8.9 Comunicación y capacitación de la aplicación del modelo de gestión de riesgos de seguridad digital (GRSD)

Es fundamental que el personal de la entidad, las partes interesadas y la ciudadanía en general cuenten con la preparación, entendimiento y convicción para ejecutar

[12] La consulta representa coordinación de responsabilidades y en algunos casos hasta permisos. Este último caso puede abarcar áreas internas y partes externas, sobre todo cuando se requiere información o cooperación.

cada una de las fases desarrolladas en este modelo. Para lograr este objetivo, las entidades deben destinar recursos suficientes que permitan formar un plan completo y coherente donde las personas tengan la oportunidad de comprender y apropiarse del modelo, a través de sensibilización, capacitación y educación permanente.

La comunicación y adiestramiento debe estar alineada con el programa de capacitación definido por la entidad, con el fin de asegurar que cubra la totalidad del personal. Esto permite que cada uno cumpla con sus roles y responsabilidades en la gestión del riesgo de seguridad digital.

9. Anexos

9.1 Anexo 1. Marco Legal

El ordenamiento jurídico colombiano incluye una gran variedad de disposiciones de rango constitucional, legal y reglamentario, que rigen diversas actividades en cuanto al entorno de la seguridad digital y que resultan vitales en el desarrollo del modelo de gestión de riesgos de seguridad digital (MGRSD).

A continuación, se presentan las principales disposiciones que conforman el marco normativo a nivel nacional como referente para el MGRSD:

Tabla 1. Normativa nacional relacionada con asuntos de seguridad digital

Norma	Contenido
Constitución Política de Colombia	Artículos 13, 15, 20, 21, 22, 44, entre otros. Se destacan a manera de ejemplo el Art. 15, el cual dispone: *"Todas las personas tienen derecho a su intimidad personal y 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. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución (…)"*; así como el Art. 20, en el cual se establece que: *"Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.* *Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura."*.
Ley 527 de 1999 (Comercio electrónico)	Se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establece certificación y se dictan otras disposiciones. Se tratan conceptos como: mensaje de datos (artículos 2º y 5º), el principio de equivalencia funcional (artículos 6, 8, 7, 28, 12 y 13), la autenticación electrónica (artículo 17), la firma electrónica simple (artículo 7), la firma digital (artículo 28), y la firma electrónica certificada (artículo 30, modificado por el artículo 161 del decreto ley 019 de 2012).
Ley 594 de 2000 (Ley general de archivos)	Habilita el uso de nuevas tecnologías de manera general, lo cual viabiliza el uso de firmas electrónicas simples, certificadas y firmas digitales.
Ley 599 de 2000 (Código penal)	En particular las materias atinentes a: i) violación a los derechos patrimoniales de autor y derechos conexos (modificación introducida por la Ley 1032 de 2006); ii) protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las TIC (modificación introducida por la Ley 1273 de 2009)
Ley 679 de 2001 (Pornografía y explotación sexual con menores)	Esta ley contempla en el artículo 6 un sistema de autorregulación, en virtud del cual el Gobierno Nacional, por intermedio del Ministerio de Comunicaciones hoy Ministerio de Tecnologías de la Información y las Comunicaciones,

Norma	Contenido
	promoverá e incentivará la adopción de sistemas de autorregulación y códigos de conducta eficaces en el manejo y el aprovechamiento de redes globales de información. Estos códigos se elaborarán con la participación de organismos representativos de los proveedores y usuarios de servicios de redes globales de información.
Ley 962 de 2005 (Racionalización de trámites y procedimientos)	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Se destaca el numeral 4 del Art. 1º, el cual dispone que: *"(…) serán de obligatoria observancia los siguientes principios como rectores de la política de racionalización, estandarización y automatización de trámites, a fin de evitar exigencias injustificadas a los administrados:* *(…)* *4. Fortalecimiento tecnológico. Con el fin de articular la actuación de la Administración Pública y de disminuir los tiempos y costos de realización de los trámites por parte de los administrados, se incentivará el uso de medios tecnológicos integrados, para lo cual el Departamento Administrativo de la Función Pública, en coordinación con el Ministerio de Comunicaciones, orientará el apoyo técnico requerido por las entidades y organismos de la Administración Pública. (…)".*
Ley 964 de 2005	El artículo 45 de esta ley señala que los emisores de valores deben constituir un Comité de auditoría, donde se expresan aspectos relacionados con los riesgos y controles identificados por los diversos entes de control que intervienen en la evaluación de control interno de la entidad, integrado por lo menos por 3 miembros de la Junta Directiva incluyendo todos los independientes. *"El Comité deberá estar conformado por tres (3) miembros de la Junta o Consejo directivo, quienes además podrán designar personas independientes a la administración de la entidad para apoyar la labor del Comité.* *A las reuniones del Comité pueden ser citados, con la frecuencia necesaria y con el fin de suministrar las explicaciones pertinentes acerca de asuntos de control interno, el Presidente o Gerente de la entidad, el vicepresidente financiero o quien detente el cargo equivalente,*

Norma	Contenido
	el auditor interno o contralor, el revisor fiscal, así como cualquier otro funcionario que el Comité considere conveniente."
Ley 1150 de 2007 (Medidas para la eficiencia y la transparencia)	Mediante esta Ley se introducen medidas para la eficiencia y la transparencia en la contratación estatal, estableciendo en su Art. 3º, el sistema electrónico para la contratación pública (SECOP).
Circular Externa SFC 052 de 2007	Por la cual la Superintendencia Financiera de Colombia incrementa los estándares de seguridad y calidad para el manejo de la información a través de medios y canales de distribución de productos y servicios que ofrecen a sus clientes y usuarios las entidades vigiladas por esta.
Ley Estatutaria 1266 de 2008 (Habeas data)	Contempla las disposiciones generales en relación con el derecho de habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273 de 2009	Por medio de esta Ley 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, entre otras disposiciones.
Ley 1336 de 2009 (Explotación, pornografía y el turismo sexual con niños)	Se adiciona y robustece la ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. Esta ley establece dos medidas para contrarrestar la explotación sexual y la pornografía infantil que se relacionan tangencialmente con las TIC. En primer lugar, establece en el artículo 4 (autorregulación de café internet códigos de conducta) que todo establecimiento abierto al público que preste servicios de internet o de café internet deberá colocar en un lugar visible un reglamento de uso público adecuado de la red, y deberá indicar que la violación a este genera la suspensión del servicio al usuario.
Ley 1341 de 2009 (Sector TIC)	Mediante esta Ley se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones. Especialmente los artículos 4, 11 y 26.

Norma	Contenido
Decreto 1727 de 2009 (Habeas Data)	Se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros Países, deben presentar la información de los titulares de la información.
Decreto 2952 de 2010 (Habeas data)	Este decreto reglamenta los artículos 12 y 13 de la ley 1266 de 2008, en este sentido establece que con fundamento en el principio constitucional de solidaridad surgen obligaciones a cargo del Estado y de los ciudadanos, en virtud de las cuales cuando se presenten situaciones de fuerza mayor, es posible otorgar a las víctimas de secuestro, desaparición forzada y personas secuestradas, debido a su estado de debilidad manifiesta, un tratamiento diferenciado en la administración de su información financiera, crediticia y comercial.
Ley 1437 de 2011 (Uso de medios electrónicos procedimiento administrativo)	Consagra la utilización de medios electrónicos en el procedimiento administrativo y permite adelantar los trámites y procedimientos administrativos, el uso de registros electrónicos, de documentos públicos en medios electrónicos, notificaciones electrónicas, archivos electrónicos de documentos, expedientes electrónicos y sedes electrónicas. Lo anterior, con el fin de que los ciudadanos interactúen con validez jurídica y probatoria. Especialmente los artículos 59 al 64.
Ley 1453 de 2011 (Seguridad ciudadana)	Por medio de la cual se reforma el código penal, el código de procedimiento penal, el código de infancia y adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad. Especialmente el Art. 53, que modifica el Art. 236 de la Ley 906 de 2004.
Ley 1564 de 2012 Código General del Proceso	Art. 103, el cual permite el uso de las TIC en todas las actuaciones de la gestión y trámites de los procesos judiciales con el fin de facilitar el acceso a la justicia.
Resolución CRC 5050 de 2017	Por medio de esta Resolución, *"(…) se compilan las Resoluciones de Carácter General vigentes expedidas por la Comisión de Regulación Comunicaciones*".
Ley 1581 de 2012 (Habeas data)	Se dictan disposiciones generales para la protección de datos. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y

Norma	Contenido
	privada, sin embargo, a los datos financieros se les continúa aplicando la ley 1266 de 2008, excepto los principios.
Ley 1712 de 2014 (Uso de las TIC)	Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantías del derecho y las excepciones a la publicidad de la información. Toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente.
Decreto 1704 de 2012 (Interceptación legal de comunicaciones)	Determina que la interceptación legal de comunicaciones es un mecanismo de seguridad pública que busca optimizar la labor de investigación de los delitos que adelantan las autoridades y organismos de inteligencia. De esta manera, se determina que los proveedores que desarrollen su actividad comercial en el territorio nacional deben implementar y garantizar en todo momento la infraestructura tecnológica necesaria que provea los puntos de conexión y de acceso a la captura del tráfico de las comunicaciones que cursen por sus redes, para que los organismos con funciones permanentes de policía judicial cumplan, previa autorización del fiscal general de la nación, con todas las labores inherentes a la interceptación de las comunicaciones requeridas.
Decreto 2758 de 2012 (Modifica la estructura del Ministerio de Defensa)	Se reestructura la organización del Ministerio de Defensa Nacional, en el sentido de asignar al despacho del viceministro la función de formular políticas y estrategias en materia de ciberseguridad y ciberdefensa. Adicionalmente, le encarga a la Dirección de Seguridad Pública y de Infraestructura, la función de implementar políticas y programas que mantengan la seguridad pública y protejan la infraestructura, así como hacerle seguimiento a la gestión relacionada con el riesgo cibernético en el sector defensa y diseñar el plan estratégico sectorial en materia de ciberseguridad y ciberdefensa.
Decreto ley 019 de 2012 (Entidades de certificación digital)	Establece las siguientes actividades que las entidades de certificación acreditadas podrán realizar en el país, tales como: producir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas, emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles, y publicar certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los

Norma	Contenido
	literales f) y g) del artículo 26 de la ley 527 de 1999, entre otras. Especialmente los Art. 70 y 71.
Resolución SIC No. 76434 de 2012 (Habeas data)	Resolución expedida por la SIC, por medio de la cual se imparten instrucciones relativas a la protección de datos personales, en particular acerca del cumplimiento de la ley 1266 de 2008, sobre reportes de información financiera, crediticia, comercial de servicios y la proveniente de terceros países.
Resolución 3933 de 2013 del Ministerio de Defensa Nacional (Crea y organiza grupos internos de trabajo)	Creó el Grupo ColCERT y asignó funciones a la dependencia de La Dirección de Seguridad Pública y de Infraestructura del Ministerio de Defensa Nacional respecto a promover el desarrollo de capacidades locales o sectoriales para la gestión operativa de los incidentes de ciberseguridad y ciberdefensa en las infraestructuras críticas nacionales, el sector privado y la sociedad civil.
Ley estatutaria 1621 de 2013 (Para la función de inteligencia y contrainteligencia en Colombia)	Expide normas para fortalecer el marco jurídico que permita a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir adecuadamente con su misión constitucional y legal.
Decreto 0032 de 2013 (Creación de la Comisión nacional digital y de información estatal)	El Ministerio de Tecnologías de la Información y las Comunicaciones en cumplimiento de los lineamientos señalados en el documento CONPES 3701, creó, a través de este decreto, la Comisión Nacional Digital y de Información Estatal cuyo objeto es la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para la interacción con los ciudadanos y el uso efectivo de la información en el Estado colombiano.

Norma	Contenido
Circular externa SIC 02 del 3 de noviembre de 2015	La Superintendencia de Industria y Comercio impartió instrucciones a los responsables del tratamiento de datos personales, personas jurídicas de naturaleza privada inscritas en las cámaras de comercio y sociedades de economía mixta, para efectos de realizar la inscripción de sus bases de datos en el Registro Nacional de Bases de Datos a partir del 9 de noviembre de 2015.
Decreto 415 de 2016	Se adiciona el decreto único reglamentario del sector de la función pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones; Arts. 2.2.35.5; 2.2.35.6
Decreto 1078 de 2015	Decreto Único Reglamentario del sector TIC. En particular las normas atinentes ala Estrategia de Gobierno en Línea.

Fuente: adaptado de CRC, 2015, 2016 y 2017

9.2 Anexo 2. Referencias para la gestión del riesgo digital

Las metodologías enunciadas a continuación, establecen un marco de referencia en el desarrollo del proceso para la gestión de riesgos. En ellas se hacen mención de las políticas, definiciones o contenido relacionados que se encuentran publicadas en el compendio de las Normas Técnicas Colombianas NTC ISO/IEC, en las guías técnicas colombianas (GTC) vigentes, así como en los anexos con derechos reservados por parte de ISO/Icontec.

Tabla 2. Referencias para gestión del riesgo digital.

Nombre de la metodología	Descripción	Aplicación de la metodología en MGRSD	Webgrafía
NTC ISO/IEC 27005:2009	Norma internacional que provee directrices para la gestión de riesgo de seguridad de la información. La norma incluye un catálogo de amenazas y vulnerabilidades a manera de ejemplo, una herramienta de mucha utilidad cuando se está iniciando el proceso de implementación.	La norma ISO 27005 incluye un catálogo de amenazas y vulnerabilidades, muchas de ellas orientadas a TI, por lo que son útiles para la identificación del riesgo digital en el modelo.	https://www.iso.org/home.html
NTC ISO 31000:2011	Esta norma técnica colombiana, provee los principios, directrices genéricas, marco de trabajo y un proceso destinado a gestionar cualquier tipo de riesgo, en cualquier organización. Esta norma no es certificable.	Se toma como referencia, el proceso para la gestión del riesgo	https://www.iso.org/home.html

Nombre de la metodología	Descripción	Aplicación de la metodología en MGRSD	Webgrafía
NTC 5722:2012	Contiene los requisitos para que las empresas implanten, mantengan y mejoren un sistema de gestión de continuidad de negocio. Es de las primeras normas alineadas con el esquema de alto nivel de ISO. Acatar tales requisitos conduce a que las empresas puedan recibir la certificación internacional.	Uno de los propósitos transmitidos desde la política de seguridad y los lineamientos CONPES se refiere a la continuidad de las operaciones corporativas y en especial de aquellas plataformas críticas de la infraestructura del país.	NTC 5722:2012
ISO IEC/27031:2011	Describe los conceptos y principios de la disponibilidad de tecnología de información y comunicación (TIC) para la continuidad del negocio y proporciona un marco de métodos y procesos para identificar y especificar todos los aspectos, tales como criterios de desempeño, diseño e implementación, y mejorar la preparación de las TIC para asegurar la continuidad del negocio.	*Se articula de forma natural. *Claramente se indica que uno de los roles de la preparación para gestionar la continuidad tecnológica es responder al entorno de riesgos que permanece en constante cambio. *Propone la reducción del riesgo asociado a las TIC, que se puede considerar dentro de la etapa de gestión de riesgos de continuidad en tales ejercicios.	Norma ISO IEC/27031:2011.

Nombre de la metodología	Descripción	Aplicación de la metodología en MGRSD	Webgrafía
ISO IEC/27032:2012	Contempla la descripción y estandarización de los lineamientos para aplicar y mejorar el estado de ciberseguridad e involucrar diferentes aspectos técnicos. Este estándar consigna las mejores prácticas para asegurar el ciberespacio, las diferencia de los demás temas de seguridad generales y las enfoca hacia la gestión de riesgos del mismo ciberespacio.	Propone controles de ciberseguridad orientados a la mitigación de los riesgos y su mejora continua.	https://www.iso.org/home.html
ISO IEC/27014:2013	Esta norma provee los conceptos y principios para el gobierno de la seguridad de la información, a través de los cuales las organizaciones pueden evaluar, dirigir, monitorear y comunicar todas las actividades relacionadas con seguridad de la información.	Sistema de gestión de riesgo	https://www.iso.org/home.html

Nombre de la metodología	Descripción	Aplicación de la metodología en MGRSD	Webgrafía
ISO IEC/38500:2015	Estándar que fija unos objetivos básicos para un buen gobierno de los procesos y decisiones empresariales relacionadas con los servicios de TI, estos objetivos son: 1. Asegurar que las partes interesadas puedan confiar en el gobierno corporativo de TI. 2. Informar y orientar al equipo directivo sobre el uso de las TIC. 3. Proporcionar herramientas para que la alta dirección pueda evaluar el gobierno de las TIC.	El gobierno corporativo de TI es la base para alinear objetivos y metas de TI con los objetivos estratégicos de las organizaciones; por lo tanto, el modelo de riesgos digitales deberá estar enmarcado o soportado en los diferentes procesos de gobierno corporativo de las TI. Uno de los objetivos de la implementación de la norma ISO38500 es el de gestionar los riesgos de forma eficiente.	https://www.iso.org/home.html
Magerit versión 3:2012	Metodología de análisis y gestión de riesgos de los sistemas de información. Implementa el proceso de gestión de riesgos de acuerdo con el ciclo PHVA, dentro de un marco de trabajo para que los órganos del Gobierno tomen decisiones y tengan en cuenta los riesgos derivados del uso de tecnologías de la información.	Se toma como base la gestión del riesgo de TI	https://administracionelectronica.gob.es/pae_Home#.Wd5Vo2jWzIU

Nombre de la metodología	Descripción	Aplicación de la metodología en MGRSD	Webgrafía
Octave	Octave, por sus siglas en inglés. Es una metodología desarrollada por *Computer Emergency Response Team* (CERT), que tiene como objetivo facilitar la evaluación de riesgos en una organización. Metodología de análisis de riesgos, que los estudia con base en tres principios: confidencialidad, integridad y disponibilidad.	Se toma como base la gestión del riesgo de TI	https://www.cert.org/
NIST 800-30/-39	Esta metodología proporciona una guía para la realización de cada una de las etapas del proceso de evaluación de riesgos es decir, se preparan para la evaluación, realizan la evaluación y mantienen la evaluación; adicionalmente, orienta las evaluaciones de riesgos y otros procesos de gestión de riesgos de la organización	Se toma como base la gestión del riesgo de TI	https://www.nist.gov/
MIPG	El modelo integrado de planeación y gestión	Se toma como base guía para la administración del riesgo	http://www.funcionpublica.gov.co/documents/418537/506921/MECI+2016.pdf/d44fdcb5-3629-42f0-8e7c-be9359b027fb

Nombre de la metodología	Descripción	Aplicación de la metodología en MGRSD	Webgrafía
COSO I- COSO-ERM / *Committee of Sponsoring Organization of the Treadway Commission*	*Internal Control-Integrated* Framework. Facilita a las empresas a evaluar y mejorar sus sistemas de control interno, basada en la siguiente estructura: - Ambiente de control - Evaluación de riesgos - Actividad de control - Información comunicacional - Monitoreo	Gestión y administración de los riesgos.	www.coso.org
Circular de la Superintendencia Financiera de Colombia 042 capítulo 23	Tiene como objetivo regular y estandarizar los aspectos de seguridad de la información e incluye la seguridad digital en las empresas, instituciones o entidades que se encuentran sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia (SFC).	Análisis del riesgo	https://www.superfinanciera.gov.co/jsp/index.jsf
Circular de la Superintendencia Financiera de Colombia 038 capítulo de TI capítulo 7	Es una circular externa dirigida a las entidades sometidas a su inspección, las cuales deben implementar o ajustar su sistema de control interno. Puntualmente, el capítulo 7.5.2 establece que las entidades deben desarrollar una serie de procedimientos que les permita la minimización de los costos y daños causados por los riesgos.	Gestión de los riesgos en forma integral con la aplicación de diferentes estrategias que permitan llevarlos hacia niveles tolerables.	https://www.superfinanciera.gov.co/jsp/index.jsf

Nombre de la metodología	Descripción	Aplicación de la metodología en MGRSD	Webgrafía
SOX	*Sarbanes Oxley Act*. Es una ley norteamericana aprobada en el año 2002, su objetivo es el de aplicar lineamientos de control a los eventos de corrupción e irregularidades en el sector financiero.	- Monitorear los diferentes procesos cibernéticos. - Sancionar a los ejecutivos que cometen fraudes. - Incrementar presupuestos para auditorías y diferentes investigaciones de las diversas comisiones de seguridad. - Restaurar la confianza en los diferentes informes a presentar.	http://www.soxlaw.com/
Basilea III Marco regulador global para reforzar los bancos y sistemas bancarios	Es un conjunto integral de reformas elaborado por el Comité de Supervisión Bancaria de Basilea para fortalecer la regulación, supervisión y gestión de riesgos del sector bancario.	Herramientas de seguimiento dentro del sector financiero.	http://www.bis.org/bcbs/basel3_es.htm
ITIL / ISO 20000-1	Esta norma tiene como objetivo la evaluación y estandarización para la prestación de los servicios de tecnología con calidad y el uso de las mejores prácticas de gestión y operación tecnológica.	Gestión de riesgo.	https://www.itgovernance.co.uk/iso20000
Cobit/Isaca	Cobit ayuda a las empresas a crear el valor óptimo desde IT, mantiene el equilibrio entre la generación de beneficios, la optimización de los niveles de riesgo y el uso de recursos.	N/A	http://www.isaca.org/cobit/

Nombre de la metodología	Descripción	Aplicación de la metodología en MGRSD	Webgrafía
Practice standard for project risk management/project Management Institute	Proporciona un punto de referencia para la profesión de gestión de proyectos. La mayor parte del tiempo define los proyectos de la gestión de riesgos como buenas prácticas.	Referencia para el manejo de riesgos en proyectos.	www.pmi.org
ISAE 3402	Antes conocida como SAS-70; es un conjunto de "buenas prácticas" para la evaluación de proveedores externos. La evaluación, cuyo objetivo es garantizar la calidad de las soluciones externalizadas, se formula de manera independiente y es aceptada dentro del sector.	Seguridad de la información.	www.isae3402.com
ISA-99/IEC 62443	El estándar ISA-99/IEC 62443 es el estándar mundial para la seguridad de los sistemas de control industrial en el dominio de las organizaciones de tecnología operativa (OT).	Seguridad de los sistemas de control industrial en el dominio de las organizaciones de tecnología operativa (OT).	www.isa.org

Nombre de la metodología	Descripción	Aplicación de la metodología en MGRSD	Webgrafía
SSAE 16	Estándar de auditoría. Reconocido internacionalmente y el enfoque está en los controles internos y externos que posee una empresa que presta servicios a terceros.	Seguridad de la información.	http://www.aicpa.org/Pages/default.aspx

Fuente: elaborado por el autor

10. Bibliografía

(GC), G. o. (s.f.). *Information Management (IM) Strategy*. Recuperado el Enero de 2014, de http://www.tbs-sct.gc.ca/im-gi/ims-sgi/ims-sgi-eng.asp

3º Comité insititucional de Desarrollo administrativo. (2013).

Collins, J. (2009). *How the might Falls.*

Copley, R. (s.f.). *How to create a Local Government Digital Service. ComputerWeekly.com [Online]*. Recuperado el Enero de 2014, de http://www.computerweekly.com/opinion/How-to-create-a-Local-Government-Digital-Service

Cultura, M. d. (2008). *http://www.reddebibliotecas.org.co/.* Recuperado el 2014, de http://www.reddebibliotecas.org.co/Cultura/Documents/Descargas/Documento_Politicadeculturadigital.pdf.

Dalzell, T. (2009). The Routledge Dictionary of Modern American Slang and Unconventional English. En T. Dalzell, *The Routledge Dictionary of Modern American Slang and Unconventional English.*

Departamento Administrativo de la Función Pública. (s.f.). *Departamento Administrativo de la Función Pública*. Recuperado el 12 de 2013, de http://www.dafp.gov.co

Dinero, R. (Septiembre de 2013). *Dinero.com*. Recuperado el Enero de 2014, de http://www.dinero.com/actualidad/nacion/articulo/falta-inversion-ciencia-tecnologia/184412.

El Ministerio de Tecnologías de la Información y las Comunicaciones diseñará un modelo de gestión de riesgos de seguridad digital, t. e. (s.f.).

El Ministerio de Tecnologías de la Información y las Comunicaciones diseñará un modelo de gestión de riesgos de seguridad digital, teniendo en cuenta el

marco conceptual de esta política, los estándares de seguridad internacionales y el marco de gestión d. (s.f.).

Energético., M. d. (2009). *Politicas y lineamientos de Operación del Sector Minero Energético.* Bogota.

Engineering, U. C. (Octubre de 2010). *What is system architecture?* Recuperado el Enero de 2014, de http://www.incoseonline.org.uk/Program_Files/Publications/zGuides_8.aspx?CatID=Publications

Framework, E. M. (s.f.). *Enhanced Management Framework*. Recuperado el Enero de 2014, de http://www.tbs-sct.gc.ca/emf-cag/abu-ans/abu-ans-eng.asp

Gartner, C. P. (Septiembre de 2009). *Gartner*. Recuperado el Enero de 2014, de Gartner: http://www.gartner.com/newsroom/id/1159617

Gartner, M. d. (s.f.). Recuperado el 12 de 2013, de http://blogs.msdn.com/b/architectsrule/archive/2008/06/12/gartner-it-infrastructure-and-operations-maturity-model.aspx

Government, U. (Noviembre de 2010). *Directgov 2010 and beyond: revolution not evolution.* Recuperado el Enero de 2014, de https://www.gov.uk/government/publications/directgov-2010-and-beyond-revolution-not-evolution-a-report-by-martha-lane-fox

Government, U. (Marzo de 2012). *UK Government Reference Architecture Version 1.0*. Recuperado el Enero de 2014, de https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266257/UK-Reference-Architecture-V1-0-HMG-Branded.pdf

Government., U. (Marzo de 2009). *What is the MODAF Meta-Model?* Recuperado el Enero de 2014, de

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/48836/20090310_modaf_meta_model_v1_0-U.pdf

Guerrero R, G. A.-M. (s.f.). *Sistema de Salud de Colombia. Salud Pública, Proyecto: Salud Electrónica.*

ISACA. (2012). Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. En *COBIT 5 AN ISACA FRAMEWORK* (pág. 31 a 31).

Línea, G. e. (s.f.). *Manual para la implementación de la Estrategia de Gobierno en línea en las entidades del orden nacional de la República de Colombia – Estrategia 2012-2015 para el Orden Nacional, Estrategia 2012-2017 para el Orden Territorial.* Bogotá, Colombia.

línea, P. g. (2010). *Manual para la implementación de la estrategia de gobierno en línea versión 2010.* Bogotá.

Ministerio de Agricultura. (s.f.). *Ministerio de Agricultura*. Recuperado el 01 de 2014, de https://www.minagricultura.gov.co

Ministerio de Agricultura. (s.f.). *Ministerio de Agricultura*. Recuperado el 01 de 2014, de https://www.minagricultura.gov.co

Ministerio de las TICs. (2013). *8. Presentacion PET Rama Judicial 18092013.pptx.* Bogotá.

Ministerio de las TICs. (2013). *9. Plan Estratégico TI y los objetivos Misionales_27092013.pptx.* Bogotá.

Ministerio de las TICs. (2013). *Incorporación de las TIC en la Rama Judicial v3.2 nov11.pptx.* Bogotá.

Ministerio de las TICs. (2013). *VICETI_Informe Modelo Contextual y Conceptual Sector Justicia_30092013.docx.* Bogotá.

MinTIC. (s.f.). *MinTIC*. Recuperado el Enero de 2014, de http://www.mintic.gov.co/images/documentos/planes_programas_mintic/plan_de_accion_2013_enero_31.pdf

nacional, M. d. (2008). *Lineamientos para la formulación de planes estratégicos de incorporación de tecnologías de información y comunicación (TIC) en Instituciones de Educación Superior.*

Planeación, D. N. (2010). *Documento CONPES 3650 Importancia Estrategica de la Estrategia de Gobierno en Línea.* Bogota.

Porter, M. (2008). Chapter 1. En M. Porter, *"The Five Competitive Forces that Shape Strategy" in On Competition Update and Expanded Edition.* Harvard Business review.

Project Management Institute. (s.f.). *Project Management Institute PMI*. Recuperado el 12 de 2013, de http://www.pmi.org/

Proposed Set of Treasury Board Policy Instruments. (s.f.). Recuperado el Enero de 2014, de http://www.tbs-sct.gc.ca/prp-pep/ffgt-cpgt-eng.asp

PROYECTO ADECUACION Y AMPLIACION DE HARDWARE Y SOFTWARE PARA EL DAPRE - RESUMEN EJECUTIVO AREA DE INFORMACIÓN DE SISTEMAS - DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPÚBLICA. (s.f.). Bogotá.

Publica, D. A. (2014). *Modelo Integrado de Planeación y Gestión.* Bogota.

República, P. d. (2011). *Política editorial y actualización de contenidos web.* Bogotá.

Social, M. d. (2013). *Informe de actividades 2012 -2013 Sector Administrativo de Salud y Protección Social.*

Young-Joo Lee*, Y.-I. K.-J. (s.f.). *Advancing Government-wide Enterprise Architecture – A Meta-model Approach.* Seoul, Korea: Department of Information Resource Service, NIA(National Information society Agency).