COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Versión 2

DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA – DANE y FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA – FONDANE

JULIO DE 2020

Contenido

1. Justificación y antecedentes

La Alta Dirección[1] del Departamento Administrativo Nacional de Estadística – DANE y del Fondo Rotatorio del Departamento Administrativo Nacional de Estadística-FONDANE, actualizan la política general de seguridad y privacidad de la información, con el propósito de salvaguardar, conservar y proteger la información que administra en el ejercicio de sus funciones. Esta política determina herramientas necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información.

El referente utilizado para la formulación de la presente política es el Modelo de Seguridad y Privacidad de la Información- MSPI, establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones- MinTic. El MSPI recopila las mejores prácticas, nacionales e internacionales, suministrando los requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo en materia de seguridad y privacidad de la información. En el ejercicio de la revisión de la política general se identificó la necesidad de actualizarla en los siguientes aspectos:

- Incluir en el alcance al Fondo Rotatorio del Departamento Administrativo Nacional de Estadística-FONDANE.
- Integrar en la política general de seguridad el componente de privacidad.
- Incluir principios y políticas complementarias.
- Promover estrategias de comunicación para su conocimiento, apropiación y aplicación para lograr cultura de seguridad y privacidad de la información en el DANE y el FONDANE.
- Advertir sobre las posibles sanciones por el incumplimiento de la presente política, las políticas complementarias, los protocolos y los procedimientos en materia de seguridad y privacidad de la información.
- Establecer lineamientos para la presentación de reportes a la Alta Dirección.

2. Marco normativo

El ordenamiento jurídico colombiano contiene varias disposiciones normativas que regulan la protección de la seguridad y la privacidad de la información. La Constitución Política de Colombia, en su artículo 15, consagra que todas las personas tienen derecho a su intimidad personal, familiar y al buen nombre, debiendo el Estado respetarlos y hacerlos respetar. Del mismo modo, en el artículo 74 señala que es un derecho fundamental acceder a la información pública, salvo las excepciones que establezca la ley.

A su turno, la Ley 1712 de 2014, que regula el acceso a la información pública, dispuso que toda información en posesión, control o custodia de una entidad del Estado es pública, y no podrá ser reservada salvo disposición legal. Así mismo, definió que la información en posesión de una entidad pública que pertenezca al ámbito propio, particular, privado o semiprivado de una persona natural o jurídica se considerará como clasificada y gozará de protección. En cumplimiento de la Ley, las entidades públicas deben adoptar un índice actualizado de la información calificada como reservada y clasificada.

Una de las excepciones a la divulgación de la información pública, es la reserva estadística contenida en el artículo 5º de la Ley 79 de 1993. Este artículo estableció que la información obtenida por el DANE en el desarrollo de censos y encuestas no podrá darse a conocer al público ni a las entidades u organismos oficiales ni a las autoridades públicas, sino únicamente en resúmenes numéricos, que no haga posible deducir de ellos información alguna de carácter individual que pudiera utilizarse para fines comerciales, de

[1] La Alta Dirección en el DANE es el Director y Representante legal de FONDANE.

tributación fiscal, de investigación judicial o cualquier otro diferente del propiamente estadístico. Así mismo, el artículo 19 de la Ley 1712 de 2014 señaló que se encuentra reservada la información cuyo acceso pueda generar un daño al interés público relacionado con la estabilidad macroeconómica y financiera del país.

Respecto a la seguridad de la información, el Decreto 1078 de 2015, modificado por el Decreto 1008 de 2018, en su artículo 2.2.9.1.1.3 definió la seguridad de la información como principio de la Política de Gobierno Digital. En consideración de esto, las entidades públicas deben adoptar medidas apropiadas, efectivas y verificables que den cumplimiento al modelo de seguridad emitido por el MinTic, con el fin de satisfacer los principios de confidencialidad, integridad y disponibilidad de la información. De igual manera, en el artículo 2.2.9.1.2.1 definió la estructura de los componentes TIC para el Estado y TIC para la sociedad y los habilitadores: seguridad de la información, arquitectura y servicios ciudadanos digitales, que permiten el desarrollo de los componentes y el logro de los propósitos de la Política de Gobierno Digital.

Así mismo, el Decreto 1499 de 2017 modificó el Decreto 1083 de 2015 (Decreto Único Reglamentario del Sector de Función Pública), y adoptó el Modelo Integrado de Planeación y Gestión - MIPG. El Decreto define al modelo en su artículo 2.2.22.3.2 como "*... un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y Organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio*". El MIPG estableció 18 políticas, entre ellas la Política de Gobierno Digital y la Política de Seguridad Digital.

El Conpes 3854 de 2016 y la Política de Seguridad Digital se desarrollan con la implementación del "Modelo de Gestión de Riesgos de Seguridad Digital-MGRSD". El modelo debe ser aplicado por los organismos que conforman la rama ejecutiva del poder público y por los demás organismos y entidades de naturaleza pública que de manera permanente tienen a su cargo el ejercicio de las actividades y funciones administrativas o la prestación de servicios públicos del Estado Colombiano, asi como por los particulares que cumplen funciones administrativas. El MGRSD suministra los requisitos para incorporar la gestión de riesgos digitales con el enfoque de mejora continua.

El Departamento Administrativo Nacional de Estadística – DANE, mediante la Resolución No 0447 de 2019, adoptó las políticas de Gobierno Digital y Seguridad Digital. Así mismo, en mayo de 2019 estableció la Política General de Seguridad de la Información.

Del marco jurídico expuesto anteriormente se desprende la obligación para el DANE y el FONDANE de adoptar una Política de Seguridad y Privacidad de la información. La política debe integrar el Modelo propuesto por el MinTic en el marco de la Política de Gobierno Digital y la Política de Seguridad Digital.

En consecuencia, se hace necesario establecer el marco en el cual el DANE y el FONDANE hagan efectivo el derecho al acceso a la información pública de los ciudadanos y la protección de aquella que se considera reservada o clasificada. En este contexto, se deben establecer los parámetros mediante los cuales se protegerá la información sometida a reserva legal que el DANE y el FONDANE en el ejercicio de sus funcionales misionales administran.

3. Política general de seguridad y privacidad de la información

La Política General de Seguridad y Privacidad de la información del DANE y del FONDANE comprende el compromiso de la Alta Dirección, los principios y la definición de las políticas complementarias. Esta Política se desarrolla en un plan de acción anual que será definido por el Comité de Seguridad de la Información.

La Política General de Seguridad y Privacidad de la información del DANE y del FONDANE, se revisará y de ser necesario se actualizará cada dos años o antes, si ocurren cambios significativos, para asegurar su pertinencia, adecuación y mejora continua.

3.1 Objetivos

La presente política busca el logro de los siguientes objetivos:

- Conservar, salvaguardar y proteger la información administrada por el DANE y el FONDANE, para preservar la confidencialidad, integridad y disponibilidad de la información.
- Asegurar el cumplimiento de los requerimientos legales y regulatorios vigentes en materia de seguridad y privacidad de la información, para evitar sanciones, daños a los particulares y la pérdida de imagen del DANE y del FONDANE.
- Minimizar los riesgos de seguridad de la información, acorde con las necesidades institucionales, para asegurar que los activos cumplan con los atributos de integridad, confidencialidad y disponibilidad.

3.2. Alcance

Esta política aplica a todos los servidores públicos, contratistas, terceros y partes interesadas del DANE y del FONDANE que en el ejercicio de las actividades utilicen información y servicios de tecnologías de la información de las citadas entidades.

3.3. Compromiso de la Alta Dirección

La Alta Dirección del DANE y del FONDANE adopta e implementa el Modelo de Seguridad y Privacidad de la Información para proteger, preservar y administrar la confidencialidad, integridad y disponibilidad de la información en los procesos institucionales. Lo anterior, mediante la administración de los riesgos de seguridad de la información, previniendo incidentes y dando cumplimiento a los requisitos legales y reglamentarios con la implementación de los controles establecidos en el estándar internacional ISO 27001 Anexo A.

3.4. Principios

Los principios están orientados a cumplir con los tres atributos de la seguridad de la información como son: la integridad, la disponibilidad y la confidencialidad. Estos principios se describen a continuación:

- Uso apropiado de los activos para los fines previstos y para cumplir con los objetivos institucionales.
- Protección de la información generada, transmitida, procesada y resguardada en los procesos de negocio y su infraestructura tecnológica de los riesgos que se puedan generar por los accesos

otorgados o el uso indebido de la información. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- Protección de las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos, mediante la implementación de controles de acceso a la información, sistemas y recursos de red.
- Control de la operación de los procesos de negocio, garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Garantía para que la seguridad sea parte integral de los procesos, mediante la aplicación de políticas, análisis de riesgos y buenas prácticas en temas de seguridad y privacidad de la información.
- Promoción de la gestión adecuada de incidentes, eventos y debilidades de seguridad para lograr el mejoramiento continuo del modelo de seguridad.
- Garantía en cuanto a la disponibilidad de los procesos de negocio y la continuidad de su operación, basada en el impacto que pueden generar los eventos e incidentes de seguridad.
- Cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

3.5. Políticas complementarias de seguridad y privacidad de la información

La Alta Dirección del DANE y del FONDANE define las políticas complementarias de seguridad y privacidad de la información que se describen a continuación; el detalle de cada una se incluirá en el manual de políticas de seguridad y privacidad de la información:

3.5.1. Organización de la seguridad y privacidad de la información

La Entidad establece un esquema de seguridad de la información y define roles y responsabilidades. Así mismo, crea el Comité de Seguridad de la Información para su desarrollo e implementación. El equipo de seguridad mantiene el contacto con los grupos de interés del ámbito de la seguridad de la información, para aplicar buenas prácticas en la materia.

3.5.2. Seguridad del recurso humano

La Secretaría General establece mecanismos para que los servidores públicos y contratistas comprendan sus responsabilidades frente a la seguridad y privacidad de la información en los roles que desempeñan. La Secretaría General define planes anuales de comunicación, sensibilización y capacitación de manera conjunta con la Dirección de Difusión, Mercadeo y Cultura Estadística. En el plan se incluyen actividades especializadas dirigidas a las personas que gestionan para el DANE y el FONDANE asuntos de seguridad y privacidad de la información.

Los acuerdos contractuales establecen las responsabilidades del contratista y las del DANE y del FONDANE, en cuanto a la seguridad y privacidad de la información. El manual de funciones contiene responsabilidades de los servidores públicos relacionadas con la seguridad y privacidad de la información.

3.5.3. Gestión de activos

El Comité de Seguridad de la Información valida la metodología para la identificación, clasificación y valoración de activos de información del DANE y el FONDANE, de acuerdo con su criticidad y a su nivel de confidencialidad. El equipo de seguridad de la información y los líderes de proceso deben

aplicar dicha metodología. El equipo de seguridad establece un procedimiento para el manejo de los activos de información.

Los servidores públicos, contratistas y partes interesadas deben devolver todos los activos de información del DANE y del FONDANE que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

3.5.4. Control de acceso

La Oficina de Sistemas administra el acceso a la información, permitiendo el acceso sólo a los usuarios autorizados por los líderes de proceso. La Oficina de Sistemas establece las políticas complementarias para el ingreso seguro a los sistemas de información, así como el acceso a redes y servicios de red.

Los dispositivos móviles de captura adquiridos en la Entidad deben cumplir con las políticas, los procedimientos y los protocolos de seguridad y privacidad de la información.

La Entidad debe disponer de mecanismos de conexión segura para el teletrabajo, que permitan la protección de sus activos de información.

3.5.5. Criptografía

La Oficina de Sistemas establece una política complementaria que define controles criptográficos para garantizar la disponibilidad, integridad y confidencialidad de la información. Determina las condiciones de uso de las llaves criptográficas durante todo su ciclo de vida (creación, uso, recuperación, distribución, retiro y destrucción).

3.5.6. Seguridad física y del entorno

Esta política establece la obligación de generar mecanismos de protección para el acceso físico sólo a las personas autorizadas por los líderes de proceso, reduciendo el riesgo al daño y la interferencia en las instalaciones de procesamiento de información. La Secretaría General establece una política complementaria relacionada con la prevención del acceso a áreas no autorizadas, el daño a la infraestructura, a las instalaciones o de la información, así como lineamientos para: (i) garantizar el control de acceso seguro a las instalaciones al personal autorizado; (ii) asegurar la protección de los activos de tecnología, indicando cómo se determina la ubicación de los equipos que procesan información confidencial, cómo se aseguran dichas instalaciones y los controles que se aplican para minimizar riesgos; y (iii) especificar cómo se ejecutan los mantenimientos preventivos y correctivos dentro de la Entidad. Por último, establece un procedimiento y sus controles para el retiro de activos fuera de la Entidad y su manejo externo.

3.5.7. Seguridad de las operaciones

La Oficina de Sistemas establece una política complementaria para asegurar que las operaciones de procesamiento de información sean correctas y seguras dentro de las instalaciones. Dicha política contempla aspectos como: (i) gestión de cambios; (ii) gestión de capacidad; (iii) separación de ambientes; (iv) protección contra códigos maliciosos; (v) copias de respaldo; (vi) registro y seguimiento de eventos de seguridad y privacidad de la información; (vii) control de software operacional y (viii) gestión de vulnerabilidad técnica.

3.5.8. Seguridad de las comunicaciones

Esta política establece la obligación de asegurar la protección de la información en las redes e instalaciones de procesamiento de información de soporte y de mantener la seguridad de la información transferida dentro y fuera del DANE y del FONDANE. La Oficina de Sistemas establece una política complementaria que asegure la protección de la información a través de los diferentes servicios de comunicaciones que contenga el aseguramiento de servicios en la red y los protocolos utilizados para la transferencia de información.

3.5.9. Adquisición, desarrollo y mantenimiento de sistemas de información

Esta política regula la seguridad en los sistemas de información durante todo el ciclo de vida. La Oficina de Sistemas establece una política complementaria para dar lineamientos sobre los criterios necesarios de seguridad de la información para la adquisición, desarrollo y mantenimiento y control de software en los aspectos tales como: (i) uso o instalación de software; (ii) quienes están autorizados para realizar la instalación de software, (iii) cómo se realiza la gestión de solicitudes de instalación de software y (iv) cómo se realiza el inventario de software.

3.5.10. Relaciones con los proveedores

Esta política establece la obligación de proteger los activos de información que sean accesibles a los proveedores. La Oficina de Sistemas establece una política complementaria para dar lineamientos sobre el tratamiento de la seguridad y privacidad en los acuerdos con los proveedores, lo que incluye la gestión de proveedores de datos.

3.5.11. Gestión de incidentes de seguridad de la información

Esta política determina la obligación de asegurar, con un enfoque coherente y eficaz, la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades. La Oficina de Sistemas establece una política complementaria que indica cómo responde el DANE y el FONDANE en caso de presentarse algún incidente que afecte alguno de los atributos de la información: disponibilidad, integridad o confidencialidad.

La Oficina de Sistemas documenta la organización para el manejo de incidentes de seguridad de la información. Especifica los roles, las responsabilidades y las acciones requeridas para identificar, contener, documentar, recolectar evidencias y mejorar la respuesta ante un incidente de seguridad de la información. Así mismo, indica en qué casos sería necesario pasar a la activación de los planes de BCP (Planes de Continuidad) dependiendo de la criticidad de la información. Describe también los respectivos flujos para el reporte de incidentes de seguridad de la información del centro de datos del DANE[2] a las entidades establecidas por el Gobierno Nacional.

3.5.12. Aspectos de seguridad de la información de la gestión de continuidad de negocio y plan de continuidad

[2] El centro de datos del DANE, es considerado Infraestructura crítica cibernética nacional, en el (Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia PSPICCN V 1.0. 2019). Por lo tanto, se debe reportar los incidentes de seguridad a entidades establecidas por el gobierno nacional.

La Oficina de Sistemas define un plan en el cual se indica la manera en que el DANE y el FONDANE garantizan la continuidad de los procesos críticos de negocio. Dicho plan establece la priorización para las fases de recuperación ante algún desastre o incidente crítico, los pasos a seguir cuando existan situaciones adversas, quienes deberán actuar (incluyendo las terceras partes o proveedores), los tiempos a cumplir y los procesos alternos que permitan continuar con el proceso de manera temporal.

3.5.13. Cumplimiento

Esta política establece la obligación de realizar la evaluación independiente en materia de seguridad y privacidad de la información. La Oficina de Control Interno incluirá anualmente un plan de seguimiento o de auditoria, que verifique el cumplimiento de las obligaciones legales, reglamentarias o contractuales relacionadas con la seguridad y privacidad de la información; así como el cumplimiento de las políticas, procedimientos y protocolos de seguridad y privacidad de la información.

4. Roles y responsabilidades

Para asegurar la aplicación de la política de seguridad y privacidad de la información se hace necesario definir los roles con sus respectivas responsabilidades. A continuación se describen:

Alta Dirección

- Aprobar la política de seguridad y privacidad
- Asignar los recursos para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información atendiendo a las necesidades institucionales.

Comité de seguridad de la información

- Revisar y validar las políticas generales, complementarias, procedimientos y protocolos en materia de seguridad y privacidad.
- Coordinar la implementación de las políticas generales, complementarias, procedimientos y protocolos en materia de seguridad y privacidad.
- Evaluar y coordinar la implementación de controles específicos de seguridad y privacidad de la información para los sistemas o servicios del DANE y del FONDANE, sean preexistente o nuevos.
- Revisar y validar los informes o reportes de actividades en el marco de la Seguridad y Privacidad de la Información para ser presentados a la Alta Dirección.

Proceso gestión jurídica

- Asegurar que lo establecido en las políticas generales, complementarias, procedimientos y protocolos den cumplimiento a la normatividad relacionada a la seguridad y privacidad de la información.

Proceso de comunicación

- Garantizar que las políticas generales, principios, políticas complementarias, procedimientos y protocolos de seguridad y privacidad de la información se comuniquen y apropien adecuadamente.
- Garantizar que la seguridad y privacidad de la información sean parte de la cultura organizacional.

Proceso aprendizaje institucional

- Evaluar de manera independiente el cumplimiento de las políticas generales, principios, políticas complementarias, procedimientos y protocolos de seguridad y privacidad de la información.

Responsables de los procesos

- Participar activamente en la definición de las políticas, procedimientos y protocolos en materia de seguridad y privacidad de la información, de su competencia.
- Implementar las políticas, procedimientos y protocolos en materia de seguridad y privacidad de la información.
- Asegurar que el personal a cargo y sus partes interesadas cumplan con las políticas, procedimientos y protocolos en materia de seguridad y privacidad de la información.
- Generar retroalimentación sobre la efectividad de las políticas, procedimientos y protocolos en materia de seguridad y privacidad de la información.

5. Cumplimiento

Todos los servidores públicos, contratistas, terceros y partes interesadas del DANE y del FONDANE, que en el ejercicio de sus actividades utilicen información y servicios de Tecnologías de la Información de las citadas entidades deben cumplir con la política, principios, políticas complementarias, sus procedimientos y protocolos. Su incumplimiento traerá consigo las consecuencias legales previstas en la normativa vigente.

6. Glosario

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).

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (ISO/IEC 27000:2016).

Control: Medida que modifica el 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. (MGRSD 2018).

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una Entidad. (DAFP 2018).

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

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).

Integridad: Propiedad de exactitud y completitud. (DAFP 2018).

Partes interesadas: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad. (MSPI).

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Privacidad: Por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de Gobierno en Línea la correlativa obligación de proteger dicha información en observancia del marco legal vigente. (MSPI).

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

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 2016, pág. 29).

Sistema de Gestión de Seguridad de la Información- SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Vulnerabilidad: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas. (Basado en DAFP 2018).

7. Referentes nacionales e internacionales

- Política General de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones.
- ISO 27001: 2013 y su anexo A. Objetivos de control y controles de referencia.
- Modelo de Seguridad y Privacidad de la Información establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (2016).

8. Bibliografía

Departamento Administrativo de la Función Pública (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas.

NTC – ISO/IEC- 27001 (2013), anexo A. Objetivos de control y controles de referencia.

Ministerio de Tecnologías de la Información y las Comunicaciones (2016). *Modelo de Seguridad y Privacidad de la Información versión 3.0.2.* Recuperado de https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. Política General de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones. Recuperado de https://www.mintic.gov.co/portal/604/articles-62124_Politica_Seguridad_Privacidad_Informacion.pdf