El futuro digital es de todos

MinTIC

Roles y Responsabilidades

Modelo de Seguridad y Privacidad de la Información

Ministerio de Tecnologías de la Información y las Comunicaciones

OCTUBRE 2021

MSPI

Carmen Ligia Valderrama Rojas - ministra de Tecnologías de la Información y las Comunicaciones

Iván Mauricio Durán Pabón - viceministro de Transformación Digital

Aura María Cifuentes Gallo - directora de Gobierno Digital

Gersson Jair Castillo Daza- subdirector de Estándares y Arquitectura de TI

Angela Janeth Cortés Hernández – líder del equipo de Seguridad y Privacidad de la Información

Danny Alejandro Garzón Aristizabal – asesor del equipo de Seguridad y Privacidad de la Información

Andrés Díaz Molina - oficial de Seguridad y Privacidad de la Información

Melisa Pacheco Flórez – líder del equipo de Política

Marco Sánchez Acevedo – abogado del equipo de Política

Ministerio de Tecnologías de la Información y las Comunicaciones

Viceministerio de Transformación Digital

Dirección de Gobierno Digital

Versión	**Observaciones**
Versión 4 28/10/2021	**Roles y Responsabilidades** Dirigida a las entidades del Estado

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Modelo de Seguridad y Privacidad de la Información

Roles y Responsabilidades V 4.0

Esta guía de la Dirección de Gobierno Digital se encuentra bajo una Licencia Creative Commons Atribución 4.0 Internacional.

Contenido

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

Guía - Roles y responsabilidades

1. Definición de roles y responsabilidades

Todas las entidades deben definir internamente las responsabilidades para ejecutar las actividades específicas de seguridad de la información designando a las personas apropiadas.

El mayor aporte que genera una definición de roles es que se tendrán establecidas las tareas que realizará cada uno de los miembros del equipo del MSPI, dejando un campo muy pequeño a que se presenten imprecisiones en referencia a las responsabilidades que cada personaje tiene.

Partiendo de este punto, las entidades tendrán asegurado que cada actividad establecida dentro de la etapa de planeación del MSPI, tenga un responsable claro y de igual forma que cada uno de los miembros del equipo responsable de la ejecución entiendan claramente sus roles y responsabilidades.

2. Identificación de los responsables

En primer lugar, se genera la necesidad de vincular de forma más efectiva al personal de alto nivel que estará asociado al proceso de desarrollo del MSPI en las entidades para que el apoyo se vaya garantizando desde el principio de la planeación del proyecto e ir marcando un punto de partida de éxito con la implementación del modelo de gestión de seguridad de la información planteado para la entidad.

Los representantes de alto nivel de la entidad deben identificar y establecer, sin perjuicio de lo establecido en la Ley 489 de 1998, en el menor tiempo posible (cada entidad establecerá los términos en los cuales se puede cumplir con esta obligación) organizar el grupo de trabajo responsable para implementar el Modelo de seguridad de la información en las entidades del Estado, definiendo el perfil y rol de conformidad con lo establecido en su documento de política.

Teniendo en cuenta lo anterior, al final del ejercicio el equipo directivo que lidera la implementación del MSPI, debe dar a conocer el perfil y responsabilidades de los responsables.

3. Equipo de gestión al interior de cada una de las entidades

El equipo de gestión del proyecto en cada una de las entidades se encarga de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades necesarias para adoptar el Modelo de Seguridad de la Información al interior de su entidad, así como planear las actividades necesarias para una adecuada administración y sostenibilidad de este.

4. Perfiles y responsabilidades

A continuación, se proponen los siguientes roles y responsabilidades asociados a seguridad y privacidad de la información:

5. Responsable de Seguridad de la Información para la entidad

La responsabilidad de Seguridad de la información será el liderar la implementación del Modelo de seguridad y privacidad de la información en la entidad y tendrá las siguientes responsabilidades:

- Fomentar la implementación de la Política de Gobierno Digital
- Asesorar a la entidad en el diseño, implementación y mantenimiento del Modelo de Seguridad y privacidad de la Información para la entidad de conformidad con la regulación vigente.
- Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación actual de la entidad.
- Realizar la estimación, planificación y cronograma de la implementación del MSPI.
- Liderar la implementación y hacer seguimiento a las tareas y cronograma definido.
- Definir, elaborar e implementar las políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del MSPI.
- De acuerdo con las solicitudes realizadas por los proyectos y/o procesos, realizar el acompañamiento correspondiente en materia de seguridad y privacidad de la información.
- Liderar y brindar acompañamiento a los procesos de la entidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia.
- Proponer la formulación de políticas y lineamientos de seguridad y privacidad de la información.
- Definir e implementar en coordinación con las dependencias de la entidad, las estrategias de sensibilización y divulgaciones de seguridad y privacidad de la información para servidores públicos y contratistas.
- Apoyar a los procesos de la entidad en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad y privacidad de la información.
- Definir, socializar e implementar el procedimiento de Gestión de Incidentes de seguridad de la información en la entidad.
- Efectuar acompañamiento a la alta dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los líderes de los procesos en seguridad y privacidad de la información.
- Poner en conocimiento de las dependencias con competencia funcional cuando se detecten irregularidades, incidentes o prácticas que atentes contra la seguridad y privacidad de la información de acuerdo con la normativa vigente.

6. Comité Institucional de Gestión y Desempeño Institucional – Comité de Seguridad y privacidad de la información

- Asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información, mediante el cumplimiento de las siguientes actividades:
    - Aprobación seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarias para la implementación interna de las políticas de seguridad y privacidad de la información.
    - Socializar la importancia de adoptar la cultura de seguridad y privacidad de la información a los procesos de la entidad.
    - Aprobar acciones y mejores prácticas que en la implementación del MSPI.
    - Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información.
- Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.

7. Oficina asesora Jurídica

- Brindar asesoría a los procesos de la entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.
- Brindar asesoría al Comité Institucional de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.
- Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los procesos, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso.
- Representar a la entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información.
- Apoyar y asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.

8. Gestión del Talento Humano

- Controlar y salvaguardar la información de datos personales del personal de planta de la entidad, en concordancia con la normatividad vigente.
- Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.

9. Control Interno

Dentro de la definición de responsables en cada uno de los Dominios entregados en el Marco de Arquitectura Empresarial, está contemplado el papel del responsable de seguridad y privacidad de la información de la entidad, de esta forma se tienen las siguientes responsabilidades específicas de acuerdo con el Dominio:

Tabla 1: Responsabilidades – Marco de Arquitectura Empresarial

DOMINIO	RESPONSABILIDADES
SERVICIOS TECNOLÓGICOS	- Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución. - Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. - Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. - Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias. - Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. - Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
ESTRATEGIA TI	- Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la institución. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información.
GOBIERNO TI	- Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI. Encargado monitorear y gestionar la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información.

SISTEMAS DE INFORMACIÓN	- Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad. - Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano. - Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. - Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados. - Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.
DE INFORMACIÓN	- Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados. - Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información.
USO Y APROPIACIÓN	- Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles. - Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora. - Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.

Teniendo en cuenta la naturaleza de la entidad, debe conformarse un equipo para el desarrollo del proyecto al cual deben pertenecer miembros directivos y representantes de las áreas misionales, con el propósito de asegurar que toda la información más relevante de la entidad esté disponible oportunamente. De esta forma se busca asegurar que sea una iniciativa de carácter transversal a la entidad, y que no dependa exclusivamente de la oficina o área de TI.

Una de las tareas principales del líder del proyecto es entregar y dar a conocer los perfiles y responsabilidades de cada personaje al grupo de trabajo e identificar las personas idóneas para tomar cada rol. De esta forma, y de manera general se pone a consideración el siguiente listado para que las entidades analicen de acuerdo con su composición orgánica cuales deben ser los miembros del equipo de seguridad y privacidad de la información, de acuerdo con los siguientes perfiles:

- Personal de seguridad de la información.
- Un representante del área de Tecnología.
- Un representante del área de Control Interno.
- Un representante del área de Planeación.
- Un representante de sistemas de Gestión de Calidad.
- Un representante del área Jurídica.
- Funcionarios, proveedores, y ciudadanos

Es importante resaltar nuevamente la necesidad del compromiso de la Alta dirección de la entidad, de esta forma se presenta la figura No. 01, en la cual se presentan los perfiles de manera genérica el nivel al cual pertenecerían según lo propuesto.

Ilustración 1: Equipo de Gestión de Seguridad de la Información en las entidades

RESPONSABILIDADES DEL EQUIPO DEL PROYECTO:

- Apoyar al líder de proyecto al interior de la entidad.
- Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto.

- Ayudar al líder de proyecto designado, en la gestión de proveedores de tecnología e infraestructura.
- Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el líder de proyecto.
- Las que considere el líder del proyecto o el comité de seguridad de la entidad.

De manera particular se resaltan dos perfiles que deben estar participando de manera activa durante el desarrollo del proyecto, a pesar de que el proyecto no es de responsabilidad exclusiva del área de TI su papel es fundamental, y de acuerdo con la Ley de Protección de Datos Personales se debe tener muy presente el rol de **responsable del tratamiento** de los datos personales.

Teniendo en cuenta que el responsable del tratamiento de datos personales en la entidad, es quien tiene decisión sobre las bases de datos que contengan este tipo de datos y que el responsable es quien direcciona las actividades de los encargados de los datos personales (quien realiza el tratamiento directamente), como se mencionaba anteriormente, adicional a las responsabilidades arriba citadas se tendrán en cuenta que de acuerdo a la Ley 1581 de 2012 Protección de Datos Personales los deberes y responsabilidades de los responsables y/o encargados del tratamiento de los datos personales son:

- Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales.
- Tramitar las consultas, solicitudes y reclamos.
- Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran.
- Respetar las condiciones de seguridad y privacidad de información del titular.
- Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.

COMITÉ DE SEGURIDAD:

Las funciones de este comité pueden ser incluidas por el comité Institucional de desarrollo administrativo, como instancia orientadora de la implementación de la estrategia de Gobierno en línea de acuerdo con el señalado en el Art. 2.2.9.1.2.4. Responsable de orientar la implementación de la Estrategia de Gobierno en Línea; ó si la entidad así lo estima conveniente, se debe crear un comité de Seguridad de la Información para la entidad.

A continuación, se presenta un ejemplo de plantilla que podría servir como base para la generación de la resolución para la creación del comité de seguridad de la información para las entidades, se reitera que está sujeta a las condiciones orgánicas y misionales de cada entidad.

RESOLUCIÓN XX DE XXXX

"Por la cual se conforma el Comité de Seguridad de la Información de nombre de la entidad y se definen sus funciones"

EL CARGO DE DIRECTIVO DE QUIEN TIENE LA FACULTAD DE LA NOMBRE DE LA ENTIDAD,

en ejercicio de sus facultades legales, en especial las conferidas por ..., y

CONSIDERANDO

Que....

...Que, en mérito de lo expuesto,

RESUELVE:

Artículo 1º. Conformación del Comité de Seguridad de la Información. Créase el Comité de Seguridad de la Información de Nombre de la entidad. El Comité estará integrado así:

1. El Directivo del área de informática o su delegado.

2. El Directivo del área de Planeación o su representante.

3. El Directivo del área Jurídica (según corresponda por distribución Orgánica de la entidad) o su delegado.

4. El Directivo encargado de los sistemas de Gestión de Calidad (según corresponda por distribución Orgánica de la entidad) o su delegado

5. El Directivo encargado de la Gestión Documental (según corresponda por distribución Orgánica de la entidad) o su delegado.

6. El Directivo encargado (según corresponda por distribución Orgánica de la entidad) de Control Interno o su delegado.

7. El responsable de Seguridad de la información de la entidad.

Parágrafo 1º.El Comité podrá invitar a cada sesión, con voz y sin voto, a aquellas personas que considere necesarias por la naturaleza de los temas a tratar.

Artículo 2º. Objetivo del Comité de Seguridad de la Información. El Comité deberá asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el

organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo.

Artículo 3°. Funciones del comité. El Comité de Seguridad de la Información de la Nombre de la entidad tendrá dentro de sus funciones las siguientes:

1. Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.
2. Revisar los diagnósticos del estado de la seguridad de la información en Nombre de la entidad.
3. Acompañar e impulsar el desarrollo de proyectos de seguridad.
4. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de Nombre de la entidad.
5. Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
6. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
7. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
8. Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
9. Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
10. Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.
11. Las demás funciones inherentes a la naturaleza del Comité.

Parágrafo. Una vez conformado el Comité de Seguridad de la Información, este podrá expedir su reglamento, en el cual fijará el alcance de cada una de las funciones operativas señalas en el presente artículo.

Artículo 5°. Secretaria Técnica: La Secretaría Técnica del Comité se definirá al interior del Comité y el secretario elegido será remplazado cada XXXX (X) meses.

Artículo 6°. Funciones de la Secretaría Técnica. Las funciones de la Secretaría Técnica serán las siguientes:

1. Elaborar las actas de las reuniones del Comité y verificar su formalización por parte de sus miembros.
2. Citar a los integrantes del Comité a las sesiones ordinarias o extraordinarias
3. Remitir oportunamente a los miembros la agenda de cada comité.
4. Llevar la custodia y archivo de las actas y demás documentos soporte.
5. Servir de interlocutor entre terceros y el Comité.
6. Realizar seguimiento a los compromisos y tareas pendientes del Comité.
7. Presentar los informes que requiera el Comité.
8. Las demás que le sean asignadas por el Comité.

Artículo 7°. Reuniones del Comité de Seguridad de la Información. El Comité de Seguridad de la Información – deberá reunirse (según periodicidad definida por la entidad), previa convocatoria del secretario técnico del Comité.

Artículo 8°. Sesiones Extraordinarias. Los miembros que conforman el Comité podrán ser citados a participar de sesiones extraordinarias de trabajo cuando sea necesario, de acuerdo con temas de riesgos, incidentes o afectaciones de continuidad dentro del Sistema de Gestión de Seguridad de la Información.

Artículo 9°. Vigencia y Derogatoria: La presente Resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE Y CÚMPLASE

Dado en XXXX, a los X días del mes de XXXX de XXXX

Directivo Responsable de la entidad

Cargo