Roles y Responsabilidades

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Guía No. 4

MINTIC vive digital Colombia TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0.0	25/04/2016	Versión inicial del documento

TABLA DE CONTENIDO

PÁG

1 DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información son derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, por medio de la Estrategia Gobierno en línea.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001:2013, así como a los anexos son derechos reservados por parte de ISO/ICONTEC, se tomarán algunas definiciones incluidas en la Ley 1581 de 2012.

2. AUDIENCIA

Este documento está elaborado para las entidades públicas de orden nacional, entidades públicas del orden territorial y entidades privadas que deseen una guía para implementar las políticas planteadas en el Modelo de Seguridad y Privacidad de la Información, así como proveedores de servicios para la estrategia de Gobierno en Línea y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la Información en el marco de la estrategia Gobierno en Línea.

3 INTRODUCCIÓN

Cuando la entidad toma la decisión de implementar Seguridad de la Información como un sistema vivo, el primer paso es la definición de una estructura organizacional con funciones y responsabilidades para la ejecución de las actividades que esto conlleve, puesto que la designación del personal a estas tareas es necesario a tal punto que si no se entregan las responsabilidades para ciertos perfiles no se obtendrá la eficacia y efectividad que se requiere. Ahora bien, el personal se puede definir dependiendo del tamaño de la entidad y el alcance definido dentro del proyecto enfocado de acuerdo al Modelo de Seguridad y Privacidad de la Información.

En el momento de asumir un rol, un individuo tiene la responsabilidad de alcanzar ciertos objetivos trazados conforme a unas determinadas funciones y capacidades descritas para ello, es así como el establecer los roles y la asignación de un responsable para cada acción definida dentro de la planeación de seguridad de la información en cada entidad es un aspecto clave para el correcto funcionamiento del Modelo de Seguridad de la Información (en adelante MSPI), de esta manera se busca asegurar que siempre se tenga el panorama claro respecto a la ejecución de las actividades definidas, teniendo un responsable al cual solicitar información sobre la ejecución y funcionamiento de las mismas.

Las responsabilidades determinadas para cada rol dependerán de las metas establecidas para las diferentes actividades, pues éstas van a permitir detallar los roles y responsabilidades de las personas que se van a encargar de establecer y desarrollar cada una de estas actividades asociadas a la implementación del MSPI, por otro lado, para elegir de forma más fácil y adecuada un responsable, debe generarse un análisis de las funciones de cada rol comparándolas con el personal de la entidad.

Teniendo en cuenta lo anterior, una de las preocupaciones de este ejercicio es que en el momento de la asignación de las tareas, se genere un sobredimensionamiento de las actividades, es por eso que se debe garantizar primero en cada una de las asignaciones la preparación para el cargo, así como el análisis juicioso para la definición de sus funciones e independiente de quien sería el encargado de asumir cierto rol.

Otro aspecto a contemplar en esta definición de roles y responsabilidades es la de hacer una segregación de funciones ya que permite detectar errores involuntarios,

y sobre todo evitar fraude interno en el momento en el cual un solo personaje no tiene la capacidad operacional por asignación de privilegios, para generar todas las fases de una transacción.

De esta forma, es necesario que las responsabilidades asignadas en el desarrollo del proyecto del MSPI para cada perfil, sean incorporadas a los manuales de funciones de cada entidad de acuerdo al cargo que desempeñan.

4 PROPÓSITO

El siguiente documento puede ser utilizado como guía para la definición del equipo responsable de seguridad y privacidad de información dentro de las entidades públicas, como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015.

5 GLOSARIO

- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento
- **Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la organización antes de crear nuevas políticas.
- **Guía:** Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.
- **Mejor Práctica:** Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la organización.
- **Política:** Declaración de alto nivel que describe la posición de la organización sobre un tema específico.
- **Procedimiento:** Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico.
- **Responsabilidad:** Cualidad de la persona responsable. "para cubrir ese puesto buscan a una persona con responsabilidad".[1]

- **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.
- **Rol:** Papel, función que alguien o algo desempeña.[1]

[1] Extraído de la RAE

6 DEFINICIÓN DE ROLES Y RESPONSABILIDADES

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.

6.1 IDENTIFICACIÓN DE LOS RESPONSABLES

En primer lugar se genera la necesidad de vincular de forma más efectiva al personal de alto nivel que estará vinculado 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.

6.2 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 del mismo.

6.3 PERFILES Y RESPONSABILIDADES

Con el fin de poder realizar la labor de la manera más eficiente, se sugiere el conjunto de integrantes para el equipo al interior de las entidades, denominados de la siguiente forma:

6.3.1 Responsable de Seguridad de la Información para la entidad:

En aquellas entidades que así lo justifiquen, por ejemplo con insuficiencia de recursos técnicos o experticia, se recomienda la definición de un responsable de seguridad que responda simultáneamente para un conjunto de entidades que acuerden agruparse.

Responsabilidades Responsable de Seguridad de la información:

El Responsable de Seguridad de la información será el líder del proyecto, escogido dentro del equipo mencionado anteriormente en cada entidad y tendrá las siguientes responsabilidades:

- ✓ Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo
- ✓ Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.
- ✓ Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.
- ✓ Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.
- ✓ Gestionar el equipo de proyecto de la entidad, definiendo roles, responsabilidades, entregables y tiempos.
- ✓ Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo
- ✓ Encarrilar el proyecto hacia el cumplimiento de la implementación del Modelo de Seguridad y privacidad de la Información para la entidad.
- ✓ Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.
- ✓ Monitorear el estado del proyecto en términos de calidad de los productos, tiempo y los costos.
- ✓ Trabajar de manera integrada con el grupo o áreas asignadas.
- ✓ Asegurar la calidad de los entregables y del proyecto en su totalidad.

- ✓ Velar por el mantenimiento de la documentación del proyecto, su custodia y protección.
- ✓ Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre el proyecto en cuanto a la documentación de las lecciones aprendidas.
- ✓ Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del proyecto.

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 al Dominio:

Tabla No. 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.

6.3.2 Equipo del Proyecto:

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 a su composición orgánica cuales deben ser los miembros del equipo de seguridad y privacidad de la información, de acuerdo a 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.

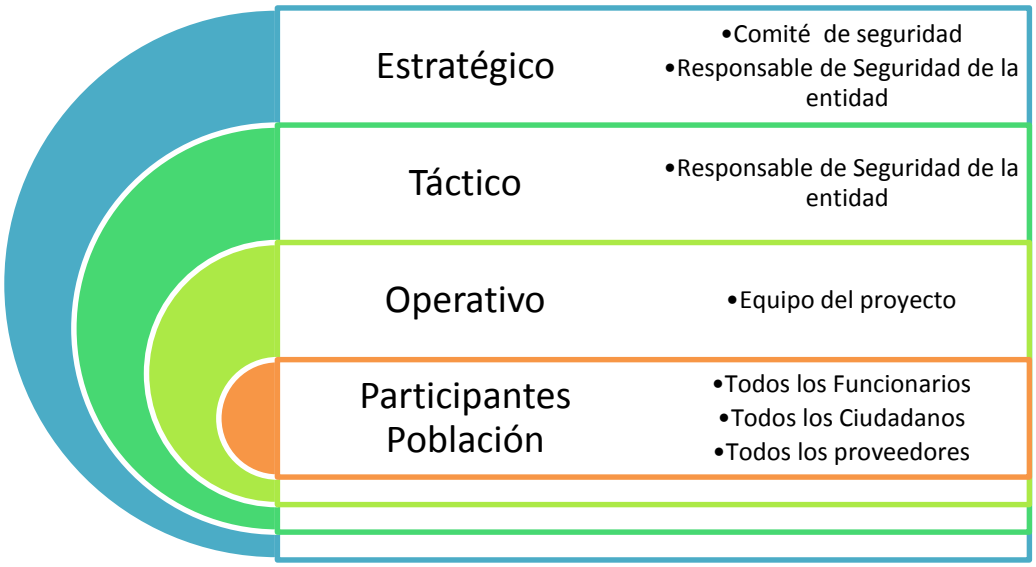

Figura No. 1 – Equipo de Gestión de Seguridad de la Información en las entidades

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 que el proyecto no es de responsabilidad exclusiva del área de TI su papel es fundamental, y de acuerdo a 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.

6.3.3 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 al señalado en el Art. 2.2.9.1.2.4. Responsable de orientar la implementación de la Estrategia de Gobierno en Línea. O 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 1°. 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 soportes.
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 a 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