TIC

Lineamientos de Roles y Responsabilidades

Ministerio de tecnologías de la información y las comunicaciones

MSPI

Julián Molina Gómez – Ministro de Tecnologías de la Información y las Comunicaciones
Yeimi Carina Murcia Yela - Viceministra de Transformación Digital
Lucy Elena Urón Rincón - Directora de Gobierno Digital
Luis Clímaco Córdoba Gómez - Subdirector de Estándares y Arquitectura de TI
Danny Alejandro Garzón Aristizábal – Contratista Subdirección de Estándares y Arquitectura de TI
German García Filoth – Contratista Subdirección de Estándares y Arquitectura de TI
Johanna Marcela Forero Varela - Profesional Especializado Subdirección de Estándares y Arquitectura de TI
Julio Andrés Sánchez Sánchez - Contratista Subdirección de Estándares y Arquitectura de TI
Lourdes María Acuña Acuña - Contratista de la Dirección de Gobierno Digital
Tairo Elías Mendoza Piedrahita - Profesional Especializado Dirección de Gobierno Digital
Andrés Díaz Molina- Jefe de la Oficina de Tecnologías de la Información
Nelson Barrios Perdomo – Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Adriana María Pedraza - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Camilo Andrés Jiménez - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Emanuel Elberto Ortiz - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Angela Janeth Cortés Hernández - Oficial de Seguridad y Privacidad de la Información GIT de Seguridad y Privacidad de la Información.

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

Versión	**Observaciones**
Versión 5 21/04/2025	Lineamientos de 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
Lineamientos de Roles y Responsabilidades V 5.0
Este documento de la Dirección de Gobierno Digital se encuentra bajo una Licencia Creative Commons Atribución 4.0 Internacional.

Tabla de contenido

Listado de tablas

Lineamientos de Roles y Responsabilidades

Este documento busca orientar a la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, en la estructuración y documentación de la Matriz del grupo de Arquitectura Empresarial, el cual es el instrumento base sobre el cual se inicia la documentación del RRHH del área de TI.

La Matriz del grupo de Arquitectura hace parte de la arquitectura de TI de una entidad u organización y a grandes rasgos describe cada una de las personas que hacen parte de estas.

A continuación, se presentan los objetivos y alcance del Instructivo.

1. Objetivo

Definir la estructura organizacional para la gestión y operación MSPI en las entidades mediante una adecuada distribución de roles y responsabilidades.

2. Alcance

El presente documento involucra a todo el personal que forma parte del alcance del MPSI

3. Definicion de roles y responsabilidades

Una de las primeras metas para implementar un modelo de seguridad y privacidad de la información es que en todas las entidades se deben definir internamente las responsabilidades para ejecutar las actividades específicas de seguridad de la información designando a las personas apropiadas, documentando las competencias y formación necesaria para el personal encargado de la seguridad de la información.

La definición de roles dentro del MSPI es fundamental, ya que permite establecer de manera precisa las tareas y responsabilidades de cada miembro del equipo. Esto minimiza las ambigüedades y reduce el riesgo de imprecisiones en la ejecución de sus funciones, garantizando una gestión eficiente y alineada con los principios establecidos en la norma.

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.

4. Identificación de los responsables

Es fundamental garantizar la participación efectiva del personal de alto nivel en el desarrollo e implementación del Modelo de Seguridad de la Información (MSPI) dentro de la entidad. Su vinculación temprana en la planeación del proyecto permite establecer una base sólida para el éxito del modelo, asegurando el liderazgo y respaldo necesarios desde el inicio del proceso.

Los representantes de alto nivel deben identificar, conformar y organizar un grupo de trabajo multidisciplinario, compuesto por integrantes de todas las áreas de la entidad, el cual será responsable de la implementación del MSPI en las entidades del Estado. Este grupo debe ser designado con base en perfiles y roles definidos en el documento de política de seguridad de la información, en concordancia con la normativa aplicable, sin perjuicio de lo establecido en la Ley 489 de 1998. Cada entidad deberá determinar los plazos y mecanismos adecuados para cumplir con esta obligación en el menor tiempo posible.

Al finalizar este proceso, el equipo directivo encargado de la implementación del MSPI deberá formalizar y comunicar los perfiles, funciones y responsabilidades de los integrantes designados, asegurando su correcta alineación con los objetivos estratégicos de seguridad de la información de la entidad.

5. Identificación de los responsables

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

6. Perfiles y responsabilidades

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

6.1. Responsable de Seguridad de la Información para la entidad

El responsable de seguridad y privacidad de la información u oficial de seguridad de la información tendrá a su cargo liderar y gestionar la implementación y mantenimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad y tendrá entre otras las siguientes responsabilidades principales:

- Definir y gestionar la normativa de seguridad y privacidad de la información y seguridad digital.

- Participar y reportar la gestión de seguridad y privacidad de la información en los comités institucionales relevantes.

- Promover la concientización, capacitación y mejora continua en materia de seguridad y privacidad de la información para todo el personal de la entidad.

- Definir, socializar e implementar los procedimientos relacionados con la gestión de seguridad y privacidad de la información al interior de la entidad.

- Asesorar y acompañar a las diferentes áreas de la entidad en la gestión de activos de información, riesgos, implementación de controles y definición de actividades de planes de tratamiento para mejorar la postura de seguridad en la entidad.

Oficial de Protección de Datos Personales (OPD)

La función del OPD en la organización es la de velar por la implementación efectiva de las políticas y procedimientos adoptados por ésta para cumplir el Régimen de Protección de Datos Personales de Colombia. Adicionalmente, es la de velar por la implementación de buenas prácticas de gestión de datos personales dentro de la entidad.

De esta manera, el OPD tendrá a su cargo la función de estructurar, diseñar y administrar el programa que permita a la organización cumplir las normas sobre protección de datos personales, así como establecer los controles de ese programa, su evaluación y revisión permanente.

Como función esencial de un OPD en la organización se encuentra la de supervisar el cumplimiento del Régimen General de Protección de Datos Personales. Acatando y cumpliendo todos los lineamientos que establezca la Superintendencia de Industria y Comercio como Autoridad Nacional de Protección de Datos Personales, en específico se le pueden asignar las siguientes responsabilidades:

- Recabar información para determinar las actividades de Tratamiento.

- Analizar y comprobar la conformidad con la normativa de las actividades de Tratamiento.

- Informar, asesorar y emitir recomendaciones al Responsable o al Encargado del Tratamiento.

- Promover la elaboración e implementación de un sistema que permita administrar los riesgos del Tratamiento de Datos personales.

- Coordinar la definición e implementación de los controles del Programa Integral de Gestión de Datos Personales.

- Servir de enlace y coordinador con las demás áreas de la organización para asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales.

- Impulsar una cultura de protección de Datos personales en poder de la organización y su debida clasificación según su naturaleza.

- Registrar las bases de datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la Superintendencia de Industria y Comercio.

- Obtener las declaraciones de conformidad de la Superintendencia de Industria y Comercio cuando sea requerido.

- Obtener la certificación de las Normas Corporativas Vinculantes por parte de la Superintendencia de Industria y Comercio cuando sea requerido.

- Revisar los contenidos de los contratos de transferencias internacionales de Datos personales que se suscriban con otros Responsables del Tratamiento, ubicados o no en territorio colombiano.

- Revisar los contenidos de los contratos de transmisión internacional de Datos personales que se suscriban con Encargados del Tratamiento, ubicados o no en territorio colombiano.

- Analizar la responsabilidad de cada cargo de la organización, para diseñar un programa de entrenamiento en protección de Datos personales específico para cada uno de ellos.

- Realizar un entrenamiento general en protección de Datos personales para todos los empleados de la compañía.

- Proyectar la documentación relacionada con la recolección y tratamiento de los datos personales.

- Realizar el entrenamiento necesario a los nuevos colaboradores, que tengan acceso por las condiciones de sus contratos a Datos personales gestionados por la organización.

- Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización (talento humano, seguridad, call centers, gestión de proveedores, etc.)

- Medir la participación y calificar el desempeño, en los entrenamientos de protección de datos Personales.

- Requerir que, dentro de los análisis de desempeño de los empleados, se encuentre haber completado satisfactoriamente el entrenamiento sobre Datos personales.

- Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de sus políticas de Tratamiento de información personal.

- Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la Superintendencia de Industria y Comercio.

- Realizar seguimiento al Programa Integral de Gestión de Datos Personales.

Nota: Supervisar la observancia no significa que el OPD sea personalmente Responsable de cualquier caso de inobservancia al Régimen General de Protección de Datos Personales.

Las Leyes Estatutarias 1266 de 2008 y 1581 de 2012 establecen claramente los sujetos obligados ante la ley y quienes están obligados a “ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado las medias apropiadas y efectivas para cumplir con las obligaciones establecidas”.

Por eso, el cumplimiento de las normas en materia de protección de datos es responsabilidad del Responsable / Encargado del Tratamiento, no del OPD.

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

El Comité Institucional de Gestión y Desempeño debe tratar los temas de seguridad y privacidad de la información asegurando 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:

- Aprobar y realizar 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 contribuyan en la implementación del MSPI.
- Promover la gestión de seguridad de la información en los procesos y cultura organizacional.
- Vigilar el cumplimiento de la normatividad relacionada con la implementación de la seguridad de la información.
- Asegurar que se logren los resultados previstos del MPSI, con un enfoque de mejora continua del referido modelo.
- Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información.
- Gestión de crisis y continuidad del negocio con la finalidad asegurar la capacidad de recuperación ante incidentes graves
- Presentación de indicadores de desempeño para medir la efectividad en la gestión de la seguridad de la información y los resultados de monitoreo de la eficacia de las políticas y procedimientos establecidos

Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.

6.3. Oficina Asesora Jurídica

Corresponde a la 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.
- Realizar el seguimiento y la interpretación de las nuevas regulaciones y normativas que impacten el MSPI.
- Asesorar a las áreas de la entidad sobre las obligaciones legales y los requisitos de cumplimiento en materia de seguridad de la información y protección de datos.

- Apoyar los lineamientos de seguridad para la gestión con proveedores.
- Verificar que las políticas y procedimientos del MSPI se ajusten a la normativa vigente.

6.4. Gestión del Talento Humano

Controlar y salvaguardar la información personal de los funcionarios de planta de la entidad, asegurando su tratamiento conforme a 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.
- Implementar procesos de selección que incluyan verificación de antecedentes y evaluaciones de confiabilidad con criterios de seguridad de la información.
- Garantizar la firma de acuerdos de confidencialidad y compromiso con la protección de datos desde la vinculación.
- Integrar el entrenamiento en seguridad de la información dentro del proceso de inducción y reinducción del personal
- Apoyar al responsable de Seguridad de la Información en la implementación del plan de concientización y sensibilización en seguridad y privacidad de la información.

6.5. Control Interno

- En el marco de su Plan Anual de Auditoría, la Oficina de Control Interno o quien haga sus veces debe incluir auditorías técnicas y de gestión de seguridad de la información.
- Se deben definir responsables de planificar, ejecutar y reportar las auditorías de seguridad de la información, asegurando que cuenten con la competencia y formación necesarias para evaluar la efectividad de los controles del MSPI.
- Se debe establecer la efectividad de los controles para asegurar el cumplimiento de la normativa vigente en materia de seguridad de la información y protección de datos personales, a través de sus procesos de seguimiento y evaluación.
- Las responsabilidades principales del encargado de realizar las auditorias técnicas y de gestión de seguridad de la información son:
    - Realizar auditorías internas de seguridad de la información
    - Evaluar la efectividad de los controles de seguridad de la información
    - Identificar no conformidades, desviaciones y oportunidades de mejora del MSPI
    - Informar sobre los resultados de las auditorías

- Coordinar actividades con otras áreas (ej. Oficina Asesora de Planeación)
- Realizar seguimiento al cumplimiento normativo

Su función primordial es la de proporcionar una evaluación independiente y objetiva sobre la eficacia del sistema de gestión de seguridad de la información, identificando áreas de riesgo y proponiendo mejoras para garantizar el cumplimiento de los objetivos y la normativa aplicable.

6.6. Oficina de Infraestructura Tecnológica

Será responsable de:

- Identificar los activos de información de los cuales es Responsable y Encargado.
- Gestionar los riesgos de seguridad de la información de los activos a su cargo.
- Asesorar a las otras dependencias en los procesos de identificación e implementación de controles.
- Implementar los controles de seguridad de la información de la infraestructura a su cargo.
- Apoyar al Responsable de Seguridad de la Información y del Oficial de Protección de Datos en los temas de su competencia.

6.7. Funcionarios y contratistas

A continuación, se detallan las responsabilidades principales de los funcionarios y contratistas de la entidad:

- Aplicar las políticas y procedimientos de seguridad de la información.
- Cumplir con los roles y responsabilidades asignados.
- Gestionar los riesgos de seguridad y privacidad de la información inherentes a los procesos
- Participar activamente en los programas de capacitación y sensibilización sobre seguridad de la información.
- Identificar y clasificar los activos de información bajo su responsabilidad.
- Actuar como propietarios o custodios de la información, garantizando la protección de los activos

7. Arquitectura de seguridad de la información

Dentro de la definición de lineamientos en cada uno de los Dominios entregados en el Marco de Arquitectura Empresarial, está contemplado el Dominio de Arquitectura de Seguridad el cual debe cumplir con lo siguiente:

LINEAMIENTO	NOMBRE	DESCRIPCIÓN	EVIDENCIAS
MAE.LI.AS.01	Catálogo de servicios de seguridad de la información y ciberseguridad	Las entidades de la administración pública deben contar con un catálogo de servicios de seguridad que comprende una lista de servicios que proporcionan e identifican funciones específicas de seguridad para los sistemas de información y una lista de servicios institucionales relacionados con seguridad de la información y ciberseguridad.	Catálogo de servicios de seguridad con base en los requerimientos identificados en los demás dominios.
MAE.LI.AS.02	Análisis de impacto del negocio	Las entidades de la administración pública deben realizar el análisis de impacto de negocio para minimizar los riesgos de indisponibilidad de los servicios e infraestructuras de TI, que afecten las operaciones regulares de las organizaciones. Este análisis debe ser incorporado en el diseño de la o las arquitecturas de seguridad y formar parte del sistema de gestión de riesgos y ser utilizado como mecanismo de control para ejecutar tareas de monitoreo de crisis, planes de contingencia, capacidad de marcha atrás y prevención y atención de emergencias.	Informe de análisis de impacto de negocio de acuerdo con el alcance definido por la entidad.
MAE.LI.AS.03	Arquitectura de Seguridad	Las entidades de la administración pública deben definir, evolucionar y aplicar una arquitectura de seguridad sobre la infraestructura tecnológica, los sistemas de información y los datos durante la ejecución de los ejercicios de arquitectura empresarial	Arquitectura de seguridad que incluya todos los artefactos que faciliten su entendimiento e implementación.
MAE.LI.AS.04	Ciberseguridad	Las entidades de administración pública deben diseñar los controles de seguridad informática para gestionar los riesgos que atenten contra la disponibilidad, integridad y confidencialidad de la información identificados durante la ejecución de los ejercicios de arquitectura empresarial.	Controles de seguridad identificados en la entidad.

Tabla 1 Lineamientos Dominio de Arquitectura de Seguridad y sus evidencias

Según la naturaleza de la entidad, debe conformarse un equipo para desarrollar el proyecto de implementación del MSPI al que deben pertenecer miembros directivos y representantes de las áreas misionales, para asegurar que toda la información más relevante de la entidad esté disponible oportunamente. Así se busca asegurar que sea una iniciativa transversal a la entidad, y que no dependa 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

La necesidad del compromiso de la Alta dirección de la entidad es necesario, así se presenta la figura No. 01, donde se presentan los perfiles de manera genérica el nivel al que pertenecerían según lo propuesto.

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

7.1. Responsabilidades Del Equipo De Proyecto de implementación y gestión del MSPI

- 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 institucional de Gestión y Desempeño.

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 del Oficial de Protección de Datos Personales y el Responsable de seguridad de la información u oficial de seguridad de la información.

Teniendo en cuenta que el responsable u Oficial de Protección 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), adicional a las responsabilidades arriba citadas, se tendrá en cuenta que los deberes y responsabilidades de los responsables y/o encargados del tratamiento de los datos personales de acuerdo a la Ley 1581 de 2012 " Protección de 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 solo los datos personales obtenidos mediante autorización, salvo que no la requieran.

- Respetar las condiciones de seguridad y privacidad de información del titular.

- Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.

7.2. Comité o Mesa técnica de seguridad y privacidad de la información

En caso de considerarlo pertinente, la entidad podrá establecer un Comité o Mesa Técnica de Seguridad y Privacidad de la Información, como instancia de apoyo al Comité Institucional de Gestión y Desempeño. Esta instancia podrá abordar aspectos especializados relacionados con la arquitectura de seguridad de la información, análisis y correlación de logs, gestión de eventos e incidentes, tratamiento de vulnerabilidades, así como aspectos normativos y

técnicos asociados al tratamiento de información pública clasificada, reservada y datos personales. Las decisiones o recomendaciones técnicas de esta mesa deberán ser elevadas al Comité Institucional para su validación y seguimiento, asegurando su alineación con la política institucional, los requisitos legales vigentes y los lineamientos del MSPI y la norma ISO/IEC 27001.

7.3. Otras responsabilidades de Proveedores y Terceros

Teniendo en cuenta la importancia de la gestión de la seguridad de la información en las entidades, es primordial establecer responsabilidades de proveedores externos, especialmente aquellos que interactúan con activos de información críticos de la entidad, como proveedores de servicios en la nube o la cadena de suministro de las TIC. Dentro de las responsabilidades se detallan las siguientes:

- Implementar y mantener los controles de seguridad de la información acordados contractualmente.
- Cumplir con la política de seguridad de la información de la entidad y las políticas específicas del tema que les sean aplicables
- Proteger la confidencialidad, integridad y disponibilidad de la información de la entidad
- Garantizar el uso aceptable de la información y otros activos asociados
- Informar sobre el cumplimiento de los requisitos de seguridad de la información
- Permitir la realización de auditorías para verificar el cumplimiento de los requisitos de seguridad.
- Gestionar de manera segura el acceso a la información y otros activos asociados.
- Notificar de manera oportuna los incidentes de seguridad de la información.
- Cooperar en la gestión y resolución de incidentes de seguridad.
- Asegurar la devolución de todos los activos de la organización al finalizar el contrato o acuerdo.
- Cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales aplicables.
- Tener una gestión adecuada de la seguridad de la información, especialmente si manejan información clasificada o reservada.

- Colaborar en la gestión de incidentes de seguridad y notificar oportunamente cualquier evento adverso

- Para proveedores de servicios en la nube, garantizar la portabilidad de los datos y la interoperabilidad de los servicios-

Responsabilidades de los ciudadanos

- Uso responsable de los servicios digitales ofrecidos por las entidades.