

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

TIC-PL03

**TABLA DE CONTENIDO**

[1. INTRODUCCIÓN 3](#_Toc62814694)

[2. OBJETIVO 3](#_Toc62814695)

[3. ALCANCE 3](#_Toc62814696)

[4. RESPONSABLE 3](#_Toc62814697)

[5. MARCO NORMATIVO 4](#_Toc62814698)

[6. DEFINICIONES 5](#_Toc62814699)

[7. NIVELES DE MADUREZ DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 8](#_Toc62814700)

[8. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN UAECOB 10](#_Toc62814701)

# INTRODUCCIÓN

La Política de Gobierno en línea en Colombia ha venido siendo implementada de manera sistemática y coordinada en todas las entidades públicas. En los últimos años, se han evidenciado cambios y avances en el uso y apropiación de la tecnología como herramienta que permite mejorar la gestión pública, la provisión de servicios y la transparencia.

La Unidad Administrativa Especial Cuerpo de Bomberos de Bogotá en este proceso de implementación se encuentra en nivel de madurez 1 por lo que debe detallar las líneas de acción para implementar el Modelo de Seguridad y Privacidad de la Información (MSPI), basándose en el ciclo PHVA. Para el desarrollo del componente de Seguridad y Privacidad de la Información, se realizó un diagnóstico preliminar según lo indica la metodología propuesta por MINTIC, paralelo a esto se diseñó un documento de lineamientos “Manual de Seguridad y Privacidad de la Información” basado en la norma técnica que le sirve de sustento: ISO 27001, las mejores prácticas y los requerimientos normativos que tengan impacto sobre el mismo.

Dado lo anterior, la Unidad Administrativa Especial Cuerpo de Bomberos de Bogotá asume compromisos en relación con la Seguridad y Privacidad de la información y diseña el Plan de Seguridad y Privacidad de la Información, trazando la ruta para alcanzar en la vigencia 2021 el nivel 3 de madurez y para el 2022 el nivel 5, y a partir de este estado poder garantizar la sostenibilidad aplicando el ciclo PHVA de manera constante.

# OBJETIVO

Implementar el Modelo de Seguridad y privacidad de la información para brindar confianza a los grupos de valor en cuanto al tratamiento de la información basado en la gestión de riesgos de la información relacionados con la disponibilidad, confidencialidad e integridad.

# ALCANCE

El Modelo de Seguridad y Privacidad de la Información está estructurado con base en la norma ISO 27001 e integrado al Modelo Integrado de Planeación y Gestión MIPG y se aplica a la información física y digital de la Unidad Administrativa Especial Cuerpo de Bomberos de Bogotá.

# RESPONSABLE

La Oficina Asesora de Planeación es la dependencia Responsable de la formulación, estructuración y seguimiento del Modelo de Seguridad y Privacidad de la Información.

Todos los funcionarios, contratistas y terceros con accesos a la información de la entidad son responsables de la implementación del del Modelo de Seguridad y Privacidad de la Información.

# MARCO NORMATIVO

| **Marco Normativo** | **Descripción** |
| --- | --- |
| Política de seguridad y privacidad de la información de Función Pública -2018. | La Política de Seguridad de la Información de (MIPG - administración Pública), con respecto a la protección de los activos de que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información. |
| Manual de política de seguridad y privacidad de la información de función pública -2018. | Compendio de políticas aplican para todos los servidores públicos y contratistas de las entidades que procesan y/o manejan información de las entidades. Política pública de Seguridad Digital. |
| Decreto 103 de 2015. | Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones |
| Manual Gobierno Digital. | Para la Implementación de la Estrategia de Gobierno Digital, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno Digital. |
| Ley 1712 de 2014; | Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones |
| Decreto 2573 de 2014 | Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones |
| Decreto 1377 de 2013 | Por el cual se reglamenta parcialmente la Ley 1581de 2012. |
| Decreto 2609 de 2012. | Por el cual se reglamenta el Título V de la Ley 594 de 2000 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado". |
| Decreto 2693 de 2012 | Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones |
| Ley estatutaria 1581 de 2012, | Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República |
| Ley 1474 de 2011 | “Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública”. Disponible en Línea |
| Decreto 4632 de 2011 | Por medio del cual se reglamenta parcialmente la Ley |
| 1474 de 2011 | Se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones. |
| Ley 1273 de 2009, | Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado |
| Ley 1266 de 2008 | Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales. |
| Ley 527 de 1999 | Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. |

# DEFINICIONES

* Acceso a la Información Pública: Derecho fundamental que consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
* Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
* Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
* Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)
* Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
* Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
* Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
* Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
* Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
* Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
* Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
* Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Un control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el nivel de riesgo.
* Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).
* Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
* Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
* Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).
* Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)
* Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
* Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
* Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
* Encargado del Tratamiento de Datos: 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. (Ley 1581 de 2012, art 3)
* 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).
* Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
* Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
* Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.
* Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.
* Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
* 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).
* Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
* Privacidad: En el contexto de este documento, 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.
* Registro Nacional de Bases de Datos: Directorio público de las bases de datos que contienen datos personales sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
* Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
* Responsable del Tratamiento de Datos: 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. (Ley 1581 de 2012, art 3).
* Riesgo: 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).
* 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).
* Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
* Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
* Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
* Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
* Partes interesadas: (Stakeholder) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

# 7. NIVELES DE MADUREZ DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN[[1]](#footnote-1)

De acuerdo con la metodología planteada en la Guía de implementación del modelo de seguridad y privacidad de la información, para lograr el nivel de madurez 5 se requiere cumplir con un numero de requisitos específicos los cuales están asociados a cada nivel de madurez y están alineados al ciclo PHVA, es por esta razón que el plan de acción se encuentra estructurado por niveles de madurez y las actividades asociadas a cada nivel corresponden a los entregables o productos que se deben tener en cada nivel para avanzar en la implementación del habilitador transversal “Seguridad de la Información” de la política de gobierno digital.

A continuación, se describen de manera condensada los requisitos para cada nivel de madurez.

1. **Inexistente**

 Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo, no están alineados a un Modelo de Seguridad.

 No se reconoce la información como un activo importante para su misión y objetivos estratégicos.

 No se tiene conciencia de la importancia de la seguridad de la información en la entidad.

1. **Inicial**

 Se han identificado las debilidades en la seguridad de la información.

 Los incidentes de seguridad de la información se tratan de forma reactiva.

 Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.

1. **Repetible**

 Se identifican en forma general los activos de información.

 Se clasifican los activos de información.

 Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información.

 Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión.

1. **Definido**

 La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información.

 La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información.

 La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas.

 La Entidad tiene procedimientos formales de seguridad de la Información

 La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información.

 La Entidad ha realizado un inventario de activos de información aplicando una metodología.

 La Entidad trata riesgos de seguridad de la información a través de una metodología.

 Se implementa el plan de tratamiento de riesgos.

 Se revisa y monitorea periódicamente los activos de información de la Entidad.

 Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información.

 Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro.

1. **Administrado**

Revisa y monitorea periódicamente los activos de información de la Entidad.

Utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información.

Evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro.

La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6

1. **Optimizado**

 En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización.

 Utilizan indicadores de efectividad para establecer si la entidad encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales.

 La entidad genera tráfico en IPv6.

# 8. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN UAECOB

En la tabla siguiente, se presentan las características de cada uno de los niveles de madurez del Modelo de Seguridad y Privacidad de la Información sumando en las dos últimas columnas el tiempo estimado en meses y la correspondiente vigencia en la que se adelantaran las actividades asociadas a cada nivel de madurez.

| **NIVEL DE MADUREZ** | | **PHVA** | **ACTIVIDAD** | **DESCRIPCIÓN** | **TIEMPO**  **(meses)** | **AÑO** |
| --- | --- | --- | --- | --- | --- | --- |
| NIVEL 0 | INEXISTENTE | PLANEAR | ESTRUCTURACIÓN | Políticas | 4 | 2020 |
| NIVEL 1 | INICIAL | LEVANTAMIENTO DE INFORMACIÓN | Definición de cronograma, registro de entrevistas, actividades, bases de datos, riesgos y posibles controles. | 6 | 2021 |
| NIVEL 2 | REPETIBLE | DOCUMENTACIÓN | Inventarios, procedimientos, instructivos, guías, formatos, registros e indicadores. | 6 |
| NIVEL 3 | DEFINIDO | HACER | IMPLEMENTACIÓN | Socialización de documentación, implementación de controles. | 18 | 2022-2023 |
| NIVEL 4 | ADMINISTRADO | VERFICAR | SEGUIMIENTO | elaboración de informes de seguimiento | 6 |
| NIVEL 5 | OPTIMIZADO | ACTUAR | CONTROL | Aseguramiento y mejora del proceso | 12 | 2024 |

1. <https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf>. Página 36 [↑](#footnote-ref-1)