

TIC-PL03

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

**TABLA DE CONTENIDO**

[1. INTRODUCCIÓN 3](#_Toc125628592)

[2. OBJETIVO 4](#_Toc125628593)

[3. ALCANCE 4](#_Toc125628594)

[4. RESPONSABLE 4](#_Toc125628595)

[5. MARCO NORMATIVO 4](#_Toc125628596)

[6. GLOSARIO 6](#_Toc125628597)

[7. NIVELES DE MADUREZ DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 10](#_Toc125628598)

[8. SITUACIÓN ACTUAL SEGURIDAD DE LA INFORMACIÓN 11](#_Toc125628599)

[8.1 EVALUACIÓN DE EFECTIVIDAD DE CONTROLES 12](#_Toc125628600)

[8.2 BRECHA ANEXO A ISO 27001:2013 13](#_Toc125628601)

[8.3 AVANCE DEL CICLO PHVA (PLANEAR-HACER-VERIFICAR-ACTUAR) 14](#_Toc125628602)

[8.4 NIVEL DE MADUREZ 16](#_Toc125628603)

[9. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 17](#_Toc125628604)

[9.1 INDICADOR 26](#_Toc125628605)

[10. DOCUMENTOS RELACIONADOS 27](#_Toc125628606)

[**CONTROL DE CAMBIOS** 27](#_Toc125628607)

# INTRODUCCIÓN

La Política de Gobierno Digital 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.

Asimismo, establece como habilitador transversal la seguridad y privacidad de la información, mediante el cual se definen de manera detallada la implementación de controles de seguridad físicos y lógicos con el fin de asegurar de manera eficiente los trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física y del entorno de las entidades públicas, gestionando de manera eficaz, eficiente y efectiva los activos de información, infraestructura critica, los riesgos e incidentes de seguridad y privacidad de la información y así evitar la interrupción en la prestación de los servicios de la Entidad enmarcados en su modelo de operación por procesos[[1]](#footnote-1).

Teniendo en cuenta lo anterior, el MinTIC a través del Modelo de Seguridad y Privacidad de la Información – MSPI[[2]](#footnote-2) define los lineamientos para la implementación de la estrategia de seguridad de la información, con el objetivo de formalizar al interior de la entidades un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento.

La Unidad Administrativa Especial Cuerpo Oficial de Bomberos de Bogotá adopta el Modelo de Seguridad y Privacidad de la Información – MSPI, paralelo a esto se diseñó un documento de lineamientos “Manual de Seguridad y Privacidad de la Información[[3]](#footnote-3)” basado en la norma técnica que le sirve de sustento: ISO 27001:2013, las mejores prácticas y los requerimientos normativos que tengan impacto sobre el mismo.

Dado lo anterior, la Unidad Administrativa Especial Cuerpo Oficial de Bomberos de Bogotá asume compromisos en relación con la Seguridad y Privacidad de la información y diseña el Plan Estratégico de Seguridad y Privacidad de la Información, trazando la ruta para alcanzar en la vigencia 2021-2024 la situación objetivo que le permita tener un adecuado nivel de madurez en seguridad de la información, y a partir de este estado poder garantizar la sostenibilidad aplicando el ciclo PHVA de manera constante, con el fin de apoyar el cumplimiento de los objetivos estratégicos de la UAE Cuerpo Oficial Bomberos Bogotá.

# OBJETIVO

Definir las actividades necesarias para implementar y apropiar 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 seguridad y privacidad con el fin de proteger, preservar y administrar la confidencialidad, integridad, disponibilidad de la información.

# ALCANCE

El Plan Estratégico de Seguridad y Privacidad de la Información —PESI— describe el estado del arte frente al componente de Seguridad de la Información enmarcados en el Sistema de Gestión de Seguridad de la Información -SGSI, así como la situación objetivo que debe alcanzar la Entidad durante el periodo 2021 - 2024, con el fin de apoyar el cumplimiento de los objetivos estratégicos de la UAE Cuerpo Oficial Bomberos Bogotá

De igual forma, se traza la ruta para continuar con la implementación de la política de Seguridad Digital y lograr el estado de madurez de seguridad con el fin de proteger, preservar y administrar la confidencialidad, integridad, disponibilidad de la información.

# RESPONSABLE

El responsable de la Seguridad y Privacidad de la información es el Comité Institucional de Gestión y Desempeño, creado mediante la Resolución 376 de 2014.

La Oficina Asesora de Planeación es la dependencia responsable de la formulación, estructuración y seguimiento del Modelo de Seguridad y Privacidad de la Información, quien se apoya en el equipo técnico de Tecnología y Comunicaciones.

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

# MARCO NORMATIVO

|  |  |
| --- | --- |
| **Marco Normativo** | **Descripción** |
| Resolución 1519 de 2020 | Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos |
| 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 |
| 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 en lo que 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 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. Desarrollado por el Decreto 4487 de 2009 – Reglamentado parcialmente por el Decreto 1747 de 2000. |
| Decreto 1263 de 2022 | Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública" |
| Decreto 338 de 2022 | Por medio del cual se establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital. |
| Decreto 767 de 2022 | Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones'" |
| Resolución 746 de 2022 | Por la cual se fortalece el modelo de seguridad y privacidad de la información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021. |
| Resolución 1978 de 2023 | Por la cual se adopta la Versión 3 del Marco de Referencia de Arquitectura Empresarial para el Estado Colombiano como el instrumento para implementar el habilitador de arquitectura de la Política de Gobierno Digital y se dictan otras disposiciones |

Adicionalmente se tendrá en cuenta las siguientes doctrinas administrativas:

|  |  |
| --- | --- |
| 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. |
| 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. |

# GLOSARIO

* 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.

# NIVELES DE MADUREZ DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN[[4]](#footnote-4)

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**

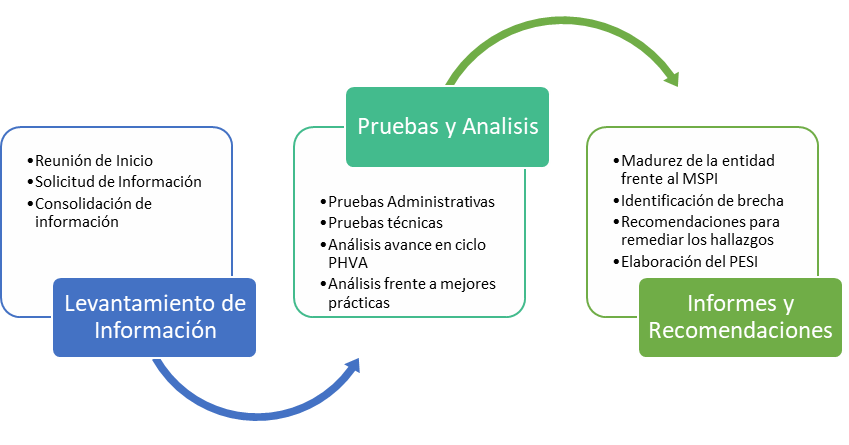
* Revisa y monitorea periódicamente los activos de información de la Entidad.
* Utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información.
* Evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su 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.

# SITUACIÓN ACTUAL SEGURIDAD DE LA INFORMACIÓN

Por situación actual se entiende el nivel de madurez que posee en este momento la **UAECOB** con relación a la seguridad de la información, para lo cual se recolectó información mediante el diligenciamiento de la herramienta de diagnóstico del Modelo de Seguridad y Privacidad de la Información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones[[5]](#footnote-5), la cual se documentó con corte al primer semestre de 2023, utilizando para la ejecución de la evaluación las siguientes fases:



**Figura 1. Fases de ejecución evaluación MPSI**[[6]](#footnote-6)

# EVALUACIÓN DE EFECTIVIDAD DE CONTROLES

El diligenciamiento de la herramienta permitió obtener una calificación calculada para cada dominio y está totalizada a partir del valor registrado y promediado sobre la cantidad de objetivos de control que se establecen. El resultado obtenido para la evaluación del estado actual nos refleja los controles y su efectividad según la Normatividad ISO 27001 del 2013 y lo planteado dentro del desarrollo del Modelo de Seguridad y Privacidad de la Información -MPSI que ha establecido el MinTIC para las entidades públicas, así como el avance del ciclo PHVA (Planear-Hacer-Verificar-Actuar).

Con el diligenciamiento de la herramienta MSPI, se obtuvieron los siguientes resultados de los dominios para la evaluación de efectividad de los controles:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Evaluación de Efectividad de controles** | | | | | | | |
| **DOMINIO** | | **Calificación a Feb 28 de 2022** | **Calificación a Jun 30de 2022** | **Calificación a Dic9 de 2022** | **Calificación a Junio de 2023** | **Calificación Objetivo** | **EVALUACIÓN DE EFECTIVIDAD DE CONTROL** |
| A.5 | POLITICAS DE SEGURIDAD DE LA INFORMACIÓN | | 90 | 100 | 100 | 100 | 100 | **OPTIMIZADO** |
| A.6 | ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | | 65 | 78 | 78 | 78 | 100 | **GESTIONADO** |
| A.7 | SEGURIDAD DE LOS RECURSOS HUMANOS | | 82 | 86 | 86 | 89 | 100 | **OPTIMIZADO** |
| A.8 | GESTIÓN DE ACTIVOS | | 46 | 62 | 75 | 75 | 100 | **GESTIONADO** |
| A.9 | CONTROL DE ACCESO | | 65 | 77 | 77 | 77 | 100 | **GESTIONADO** |
| A.10 | CRIPTOGRAFÍA | | 60 | 80 | 80 | 80 | 100 | **GESTIONADO** |
| A.11 | SEGURIDAD FÍSICA Y DEL ENTORNO | | 67 | 84 | 84 | 84 | 100 | **OPTIMIZADO** |
| A.12 | SEGURIDAD DE LAS OPERACIONES | | 55 | 68 | 68 | 68 | 100 | **GESTIONADO** |
| A.13 | SEGURIDAD DE LAS COMUNICACIONES | | 27 | 58 | 58 | 58 | 100 | **EFECTIVO** |
| A.14 | ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS | | 37 | 61 | 61 | 61 | 100 | **GESTIONADO** |
| A.15 | RELACIONES CON LOS PROVEEDORES | | 20 | 50 | 50 | 52 | 100 | **EFECTIVO** |
| A.16 | GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | | 29 | 57 | 57 | 57 | 100 | **EFECTIVO** |
| A.17 | ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO | | 43,5 | 63,5 | 63,5 | 63,5 | 100 | **GESTIONADO** |
| A.18 | CUMPLIMIENTO | | 48,5 | 59 | 59 | 80 | 100 | **EFECTIVO** |
| **PROMEDIO EVALUACIÓN DE CONTROLES SGSI** | | **39** | **53** | **70** | **71** | **73** | **100** | **GESTIONADO** |

**Tabla 1. Evaluación de efectividad de Controles - ISO 27001:2013[[7]](#footnote-7)**

De acuerdo con el análisis y los resultados obtenidos, la calificación promediada de los controles dentro de la entidad fue de 73, lo cual evidencia que la **UAECOB** se encuentra en un proceso “GESTIONADO ” de implementación de medidas para la seguridad y privacidad de la información, evidenciando oportunidades de mejora que se encuentra en proceso de revisión y mejora de los controles existentes.

Sin embargo, se precisan los dominios que deben ser incluidos entre las acciones de la actual vigencia para su fortalecimiento, en especial los que quedaron evaluados en estado efectivo.

En estos dominios se evidencia que la calificación obtenida está por debajo del promedio total de la evaluación de controles, por lo que se tendrán en cuenta los niveles de madurez alcanzados por cada uno de los dominios, con el fin de plantear las acciones y actividades prioritarias en el plan de seguridad de la información que permita de manera rápida y significativa mejorar el nivel de madurez de la entidad.

# BRECHA ANEXO A ISO 27001:2013

En este componente se muestra de manera gráfica el resultado del análisis de brecha frente a los controles del Anexo A, del estándar ISO 27001:2013, y la G[uía 8 - Controles de Seguridad de la Información](https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf) del Modelo de Seguridad de Privacidad de la Información[[8]](#footnote-8). Aquí se puede evidenciar la calificación de cada dominio frente a la escala de evaluación definida y también en comparación con la calificación objetivo.

Gráfico, Gráfico radial

Descripción generada automáticamente

**Figura 3. Fases de ejecución evaluación MPSI**

De acuerdo con la evaluación realizada y los resultados obtenidos, la **UAECOB** se encuentra en un proceso “GESIONADO” con respecto a la implementación de medidas y controles destinados a garantizar la seguridad de la información, así mismo, como la protección de los activos que la contienen.

# AVANCE DEL CICLO PHVA (PLANEAR-HACER-VERIFICAR-ACTUAR)

El aspecto que determina la evaluación del estado actual en la entidad es el correspondiente al ciclo del modelo de operación PHVA. A continuación, se presenta el resultado del avance del ciclo de funcionamiento del Modelo de Operación (PHVA).

|  |  |  |  |
| --- | --- | --- | --- |
| **AVANCE PHVA** | | | |
| **AÑO** | **COMPOENTE** | **% De avance actual entidad** | **%Avance Esperado** |
| 2023 | Planificación | 28,90% | 40% |
| Implementación | 12% | 20% |
| Evaluación de Desempeño | 13,33% | 20% |
| Mejora Continua | 10% | 20% |
| **TOTAL** | | **64,23%** | **100%** |

**Tabla 2. Avance del Ciclo PHVA**

El resultado presenta un porcentaje de avance del 64,23% a corte 30 de junio de 2023. Según el análisis realizado la UAECOB se encuentra en un proceso “GESTIONADO” de cumplimiento con respecto al PHVA y lo referente a la implementación de la Política de Gobierno Digital mediante el MSPI.

Para el ítem de planificación la entidad se encuentra en un 28% del 40% que debería presentar, para el ítem de Implementación la entidad se encuentra en un 12% de un total de un 20%, para el ítem de evaluación de desempeño la entidad se encuentra cumpliendo actualmente con un 13% de un total del 20% que debería presentar y para el ítem de mejora continua la entidad ha completado un 10% de un total del 20%.

Lo anterior se puede visualizar de manera precisa en el siguiente grafica de Avance Ciclo de Funcionamiento del Modelo de Operación) la cual representa el avance actual en la entidad y lo esperado, mostrando las diferencias de cada fase del ciclo PHVA.

La gráfica presenta una comparación entre el avance logrado por la entidad, el avance objetivo y el avance total posible.

**Figura 4. Avance Ciclo de Funcionamiento del Modelo de Operación**

# NIVEL DE MADUREZ

La madurez de la seguridad y privacidad de la información incluye los controles tanto administrativos como técnicos, la competencia técnica de los recursos informáticos, los procesos y las prácticas sostenibles, así como la eficiencia de los controles establecidos al interior de la entidad.

La madurez de la seguridad se puede medir únicamente a través de la capacidad en que la entidad utiliza de forma eficaz y eficiente los recursos disponibles para el apoyo de las funciones de forma que se cree un nivel de seguridad sostenible. Para ello debe establecerse una línea de partida de la madurez de la seguridad y usarse para definir los procesos en las que centra las actividades de seguridad de la información de la entidad, el nivel de madurez se identificó mediante el diligenciamiento del Instrumento de Evaluación MSPI evidenciado en la componente denominada madurez MSPI, que permitió identificar el estado actual que cuenta la entidad con respecto al Modelo de Seguridad y Privacidad de la Información y se identificaron requisitos que en su mayoría han sido previamente evaluados en los componentes Administrativas, Técnicas y PHVA.

En el resultado obtenido al diligenciar la herramienta Instrumento de Evaluación MSPI, la **UAECOB** evidencia que la entidad se encuentra en un nivel “GESTIONADO” de madurez y de cumplimiento de acuerdo con la implementación del Modelo de Seguridad y Privacidad de la Información.

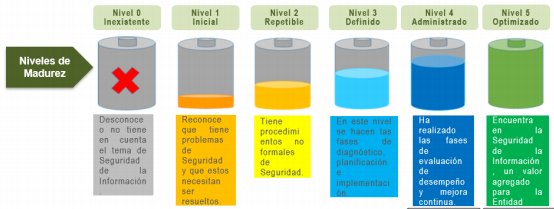
Para alcanzar el nivel de optimizado se debe diseñar un plan de trabajo con las brechas identificadas y así actualizar, diseñar y revisar los controles que actualmente se encuentran en operación para la vigencia 2021 – 2024.

2022 - 2023

2024

2021

2020



**Figura 5. Estado actual y proyección del nivel de madurez**

# 9. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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.

El plan de trabajo será revisado de manera anual y las iniciativas estarán alineadas con el plan estratégico de la entidad y de acuerdo con los cambios y prioridades del negocio permitiendo mejorar el nivel de madurez del sistema de gestión de seguridad de la información.

**ACTIVIDADES PARA EL AÑO 2024**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Actividad** | | **Fecha fin Estimada** | **Producto o entregable** |
| **1** | **PLANEACIÓN SGSI** | | | |
| 1.1 | Se establecerán las políticas y los procedimientos adicionales y se implementarán las medidas técnicas de apoyo a los procesos de negocio que permitan un gobierno de TI adecuado y una gestión de servicios que garanticen una adecuada planificación, entrega y apoyo de las capacidades de TI, dando soporte a las funciones de negocio, la mano de obra, y/o a los ciudadanos, basados en normas aceptadas por la industria (como ITIL y COBIT 5). Además, las políticas y procedimientos deberán incluir roles y responsabilidades definidos, apoyados por una formación regular de la mano de obra. | | I Trimestre 2024 | Uso y apropiación de las políticas y procedimientos de seguridad y privacidad de la información. |
| 1.2 | Articular el plan de gestión de incidentes con el plan de recuperación de desastres - DRP | | II Trimestre 2024 | Pruebas del procedimiento de gestión de incidentes alineado con procedimiento de gestión de crisis. |
| 1.3 | Actualización de riesgos digitales en todos los procesos | | I Trimestre 2024 | Matriz de riesgos digitales de todos los procesos de la UAECOB. |
| 1.4 | Establecer presupuesta de Seguridad de la Información y Ciberseguridad | | II Trimestre 2024 | PESI cuantificado. |
| **2** | **AUTODIAGNOSTICO MSPI** | | | |
| 2.1 | Realizar actualización de los niveles de madurez en los controles establecidos en la herramienta MSPI de MINTIC | | I/II/III/IV Trimestre 2024 | GAP análisis actualizado en herramienta MSPI del SGSI y GAP de Ciberseguridad. |
| **3** | **ACTIVOS DE INFORMACIÓN** | | | |
|  |  | |  |  |
| 3.1 | Realización de campañas de clasificación de activos de información en los procesos. | | II Trimestre 2024 | Matrices de clasificación de activos de los procesos. |
| **4** | **IMPLEMENTACIÓN DEL SGSI** | | | |
| 4.1 | Diseñar e Implementar el programa anual de capacitación especializada en Ciberseguridad para los colaboradores que son responsables de Ciberseguridad en la UAECOB. | | III Trimestre 2024 | Certificados de asistencia a capacitaciones en seguridad de la información y ciberseguridad. |
| 4.2 | Implementar una herramienta tipo GRC (Governance, Risk and Compliance) que permita la administración del sistema de gestión de seguridad de la información y del marco de trabajo de ciberseguridad, la administración de los activos de información, la gestión de los riesgos de ciberseguridad, la gestión de vulnerabilidades. | | II Trimestre 2024 | Riesgos Digitales y avances del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Continuidad de Negocio en herramienta de apoyo. |
| **5** | **OPERACIÓN DEL SGSI** | | | |
| 5.1 | Elaborar el programa de auditoría técnica anual a los terceros críticos para verificar el cumplimiento de las medidas y obligaciones establecidas en los contratos con el fin de verificar la adecuada gestión de los riesgos de seguridad de la información y ciberseguridad. | | III Trimestre 2024 | Informes de auditorias a terceiros. |
| 5.2 | Implementar como servicio una solución de anti malware avanzado para la protección contra amenazas avanzadas persistentes (APT) On premise y la nube. Antivirus con funcionalidad EDR (Endpoint Defense and Response) | | I Trimestre 2024 | Indicadores de amenazas materializadas. |
| 5.3 | Establecer un Servicio o mecanismos de análisis de comportamiento de red (Network Behavior analytics), que permiten definir y monitorear líneas base de comportamiento de red, obteniendo así el monitoreo sobre anomalías y comportamiento fuera de esta línea base en la red, tales como altos consumos, mayores aplicaciones usadas, posible comportamiento que definan un Indicador de compromiso (IoC) que lleve hacia un fraude o malware avanzado. | | I Trimestre 2024 | Mantener el servicio de SOC / SIEM.  Contratar servicio de Centro de operaciones de seguridad (SOC) que permita identificar de manera temprana y contener los ciberataques, mediante la realización de monitoreo inteligente y la correlación de eventos e integración de fuentes (aplicaciones, App, seguridad, entre otros) para plataformas On premises y Nube. Brindando cobertura a los sistemas más críticos de la UAECOB |
| 5.4 | Documentar planes de acción ante diferentes ciberataques, donde se especifiquen que acciones de contención se deben adoptar (Ej. desconexión automática de equipos, cambios de contraseñas, actualizar la base de firmas del antivirus, bloqueo de direcciones IP, entre otros). | | II Trimestre 2024 | Playbook de diferentes escenarios de ciberataques. |
| 5.5 | Realizar el proyecto de endurecimiento de infraestructura: servidores, bases de datos, aplicaciones, elementos activos de red | | I Trimestre 2024 | Llevar a cabo el ejercicio de análisis de vulnerabilidades y red team con frecuencia, mínimo una vez al mes.  Establecer e implementar pruebas de Hacking Ético de manera periódica sobre los aplicativos críticos expuestos en el ciberespacio. |
| 5.6 | Ejecutar el programa de ejercicios al plan de recuperación ante desastres, para los escenarios de ataques cibernéticos. | | III Trimestre 2024 | Informes de resultados de pruebas realizadas. |
| 5.7 | Establecer métodos de autenticación fuerte. - Es el proceso en el cual se verifica la identidad de un cliente, entidad o usuario, en función de uno o varios factores de autenticación y consiste en verificar que el usuario es quien dice ser. Ejemplos de estos métodos son la autenticación de doble factor con token (de software o hardware) o pin a celular. | | I Trimestre 2024 | Verificar los mecanismos implementados de cifrado sobre la información confidencial en tránsito y en reposo con el fin de mitigar los riesgos asociados a fuga de información. |
| 5.8 | Probar el Plan de Continuidad de Negocio de la UAECOB. | | II Trimestre 2024 | Plan de Continuidad de Negocio. |
| **6** | **PLAN DE SENSIBILIZACIÓN SEGURIDAD DE LA INFORMACIÓN** |  | | |
| 6.1 | Diseñar e implementar un programa anual de sensibilización y concientización en Seguridad de la Información y Ciberseguridad para funcionarios y contratistas y proveedores críticos. | | I Trimestre 2024 | Plan de Sensibilización y capacitación en seguridad de la información y ciberseguridad. |
| 6.2 | Realización de campañas de sensibilización en seguridad y privacidad de la información | | I Trimestre 2024 | Encuestas y evaluaciones de las charlas de sensibilización. |
| 6.3 | Asegurar que se atiendan las recomendaciones generadas en los informes y reportes entregados por los grupos de interés como: ColCERT y CISRT sectorial, sobre amenazas y vulnerabilidades explotadas a nivel nacional o mundial. Monitorear su implementación. | | II Trimestre 2024 | Evidencias de aplicación de recomendaciones de CSIRT sectorial y ColCERT. |

# 9.1 INDICADOR

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| MADUREZ SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN | | | | | | | |
| **RESPONSABLE** | Oficial de Seguridad de la Información | | | | | | |
| **DEFINICIÓN:** | | | | | | | |
| El indicador permite medir el nivel de madurez del SGSI | | | | | | | |
| **OBJETIVO** | | | | | | | |
| Establecer el nivel de madurez de la implementación del modelo de seguridad y privacidad de la información para establecer el estado de la gestión y adopción de controles. | | | | | | | |
| **FORMULA** | | | | | | | |
| Nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información - MPSI | | | | | | | |
| **DESCRIPCIÓN DE VARIABLES** | | | **UNIDAD DE MEDIDA** | | **FUENTE DE INFORMACIÓN** | | |
| Resultado de la implementación frente a la guía de controles MSPI y el anexo A de la ISO 27001:2013 | | | % | | Autodiagnóstico Instrumento de evaluación MSPI | | |
| **COBERTURA** | **ESCALA** | **TENDENCIA** | **TIPO** | | **FRECUENCIA** | | |
| **RECOLECCIÓN** | | **REVISIÓN** |
| Modelo de Seguridad y Privacidad de la Información | Porcentaje | Decreciente | Eficacia | | Semestral | | Semestral |
| **METAS** | | | | | | | |
| MÍNIMA | 60% | SATISFACTORIA | | 70% | | SOBRESALIENTE | 100% |
| **OBSERVACIONES** | | | | | | | |
| N/A | | | | | | | |

# DOCUMENTOS RELACIONADOS

|  |  |
| --- | --- |
| **CÓDIGO** | **DOCUMENTO** |
|  |  |

**CONTROL DE CAMBIOS**

|  |  |  |
| --- | --- | --- |
| **VERSIÓN** | **FECHA** | **DESCRIPCIÓN DE LA MODIFICACIÓN** |
| 01 | 08/06/2021 | Creación de documento |
| 02 | 29/01/2021 | Se adicionan actividades para años 2023 y 2024 |
| 03 | 30/11/2022 | Se actualizan actividades para año 2023. |
| 04 | 15/12/2023 | Se actualiza actividades para el 2024 |

**CONTROL DE FIRMAS**

|  |  |  |
| --- | --- | --- |
| Elaboró  **Luz Mery Sarmiento Rodriguez** | Cargo:  **Contratista OAP** | Firma: |
| Revisó  **Oswaldo García Rincón** | Cargo:  **Líder de Gestión TIC** | Firma |
| Aprobó  **Olga Soraida Silva Albarran** | Cargo:  **Jefe Oficina Asesora de Planeación** | Firma |

1. Tomado del Documento Maestro del Modelo de Seguridad y Privacidad de la Información Versión 4.0 [↑](#footnote-ref-1)
2. https://gobiernodigital.mintic.gov.co/692/articles-162625\_recurso\_1.pdf [↑](#footnote-ref-2)
3. https://www.bomberosbogota.gov.co/sites/default/files/planeacion/TIC-MN01%20Manual%20de%20Pol%C3%ADticas%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informaci%C3%B3n.docx [↑](#footnote-ref-3)
4. <https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf> Página 36 [↑](#footnote-ref-4)
5. https://www.mintic.gov.co/gestionti/615/articles-5482\_Instrumento\_Evaluacion\_MSPI.xlsx [↑](#footnote-ref-5)
6. https://www.mintic.gov.co/gestionti/615/articles-5482\_Instructivo\_instrumento\_Evaluacion\_MSPI.pdf [↑](#footnote-ref-6)
7. Fuente: Herramienta-Instrumento de Evaluación MSPI-Portada [↑](#footnote-ref-7)
8. https://www.mintic.gov.co/gestionti/615/articles-5482\_G8\_Controles\_Seguridad.pdf [↑](#footnote-ref-8)