U.A.E. CUERPO OFICIAL BOMBEROS BOGOTÁ D.C.

[Honor, Valor, Disciplina]

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión: 02 -2026

ALCALDÍA MAYOR DE BOGOTÁ D.C.

BOGOTÁ

Tabla de Contenido

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - PESIC

Presentación

LA UAECOB, en el desarrollo de sus actividades ha identificado que uno de los activos más importantes es la información que se encuentra almacenada de forma física o electrónica; en los sistemas de información, servidores, computador, folios entre otros.

El plan estratégico de seguridad de la información determina los objetivos a cumplir para salvaguardar la información en sus pilares de confidencialidad, integridad, disponibilidad, autenticidad y no repudio. A través de las diferentes iniciativas y proyectos estratégicos.

Objetivos

-Definir la estrategia de seguridad de la información y ciberseguridad en adelante PESIC liderada por la alta dirección apoyado y alineado su cumplimiento con el plan estratégico de LA UAECOB, respondiendo a la necesidad de preservar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de los activos de información.

-Disminuir el nivel de riesgos que responda a las necesidades de preservar la confidencialidad, la integridad, la disponibilidad, autenticidad y no repudio sobre los activos de información, priorizando su nivel de criticidad.

Alcance

Conservando el análisis del contexto externo, interno y las partes interesadas establecido en el Modelo de Seguridad y Privacidad de la Información de LA UAECOB se define el alcance del plan estratégico de seguridad de la información y ciberseguridad (PESIC), en términos de las características de la UAECOB, su ubicación y sus activos de información.

Adopta, establece, implementa, opera, verifica y mejora el Modelo de Seguridad y Privacidad de la Información (MSPI) para la UAECOB.

Principios del PESIC

LA UAECOB a través del plan estratégico de seguridad de la información y ciberseguridad debe:

- Facilitar la integración de la seguridad de la información y ciberseguridad a los departamentos, áreas, oficinas y estaciones de LA UAECOB.

- Fortalecer las competencias de seguridad de la información y ciberseguridad.

- Proponer soluciones que aseguren la información y estén a la vanguardia de la tecnología, sean flexibles, adaptables yescalables para las necesidades de la entidad.

Definiciones.

- Activo: En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamientode esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- Confidencialidad: La información no se pone a disposición ni se revela a individuos o procesos no autorizados.

- Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos deseguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguardao contramedida. En una definición más simple, es una medida que modifica el riesgo.
- Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos o procesos autorizados cuando lo requieran.
- Guía: documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas deinformación.
- Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.
- Parte interesada: (Stakeholder) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma comoafectada por una decisión o actividad.
- Política del SGSI: Manifestación expresa de apoyo y compromiso de la alta dirección con respecto a la seguridad de lainformación.
- Política: Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la UAECOB.
- Procedimiento: Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.
- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activode 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).
- Autenticidad: Es el proceso de verificar la identidad de alguien o algo. La autentificación suele tener lugar mediante la comprobación de una contraseña, un token de hardware o algún otro dato que demuestre la identidad.
- No repudio: Es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Existirán por tanto dos posibilidades:

No repudio en origen: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío.

No repudio en destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. La posesión de un documento y su firma digital asociada será prueba efectiva del contenido y del autor del documento.

Marco Normativo

Marco Normativo	Descripción
Decreto 510 de 2023	Por medio del cual se modifica la planta de empleos de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos.
8Decreto Nº 509 de 2023	"Por Medio del cual se Modifica la Estructura Organizacional de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos."
Decreto 359 de 2022	Por medio del cual se modifica el Decreto Distrital 555 de 2011 "Por medio del cual se modifica la estructura organizacional de la Unidad Administrativa Cuerpo Oficial de Bomberos y se dictan otras disposiciones".
Decreto 360 de 2022	Por medio del cual se modifica el Decreto 559 de 2011 "Por el cual se establece la planta de cargos de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos de Bogotá. D.C. li, se dictan otras disposiciones."
Ley 962 de 2005	"Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos."
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1341 de 2009	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.

Marco Normativo	Descripción
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.
Ley 1955 del 2019	Establece que las Entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
Decreto 2150 de 1995	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
Decreto 025 de 2021	Por medio del cual se reglamenta la Comisión Distrital de Transformación Digital.
Decreto 619 de 2007	Se establece la Estrategia de Gobierno Electrónico de los organismos y de las Entidades de Bogotá, Distrito Capital y se dictan otras disposiciones.
Decreto 185 de 2008.	Por el cual se prorroga el plazo para formular la Estrategia Distrital de Gobierno Electrónico de los organismos y de las Entidades de Bogotá, Distrito Capital.
Decreto 296 de 2008.	Por el cual se le asignan las funciones relacionadas con el Comité de Gobierno en Línea a la Comisión Distrital de Sistemas y se dictan otras disposiciones en la materia.
Decreto 316 de 2008.	Por medio del cual se modifica parcialmente el artículo 3° del Decreto Distrital 619 de 2007 que adoptó las acciones para el desarrollo de la Estrategia Distrital de Gobierno Electrónico.
Decreto 1151 de 2008	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.
Decreto 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
Decreto 235 de 2010	Por el cual se regula el intercambio de información entre Entidades para el cumplimiento de funciones públicas.

Marco Normativo	Descripción
Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica 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 2433 de 2015	Por el cual se reglamenta el registro de TIC y se subroga el título 1 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.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1081 de 2015	"Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República."
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las Comunicaciones.
Decreto 728 2016	“Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico”.
Decreto 728 de 2017	“Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico”.

Marco Normativo	Descripción
Decreto 1413 de 2017	"Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales"
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
Decreto 1008 de 2018	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.
Decreto 2106 de 2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
	Cap. II Transformación Digital Para Una Gestión Publica Efectiva
Decreto 620 de 2020	"Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 Y 64 de la Ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"
Decreto 088 de 2022	Por el cual se adiciona el Titulo 20 del libro 2 del Decreto Único Reglamentario del sector de las Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3,5 y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea.
Decreto 338 de 2022	Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de las Seguridad Digital y se dictan otras disposiciones.

Marco Normativo	Descripción
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.
Decreto 1263 de 2022	Por el cual se adiciona el Titulo 22 a la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de las Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Publica.
Resolución 256 de 2008	Por la cual se establece el reglamento interno de la Comisión Distrital de Sistemas – C.D.S.
Resolución 305 de 2008	Por la cual se expiden políticas públicas para las Entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.
Resolución 378 de 2008	Por la cual se adopta la Guía para el diseño y desarrollo de sitios Web de las Entidades y organismos del Distrito Capital
Resolución 473 de 2011	Por la cual se reestructura el Sistema y el comité del sistema Integrado de Gestión de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos.
Resolución 2710 de 2017	Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.
Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.

Marco Normativo	Descripción
Resolución 1117 de 2022	"Por la cual se establecen los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes de las entidades territoriales, en el marco de la Política de Gobierno Digital"
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 No. 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
Norma Técnica Colombiana NTC 5854 de 2012	Accesibilidad a páginas web El objeto de la Norma Técnica Colombiana (NTC) 5854 es establecer los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA.
CONPES 3292 de 2004	Señala la necesidad de eliminar, racionalizar y estandarizar trámites a partir de asociaciones comunes sectoriales e intersectoriales (cadenas de trámites), enfatizando en el flujo de información entre los eslabones que componen la cadena de procesos administrativos y soportados en desarrollos tecnológicos que permitan mayor eficiencia y transparencia en la prestación de servicios a los ciudadanos.

Marco Normativo	Descripción
CONPES 3854 Política Nacional de Seguridad Digital de Colombia, del 11 de abril de 2016	El crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica y el incremento en la oferta de servicios disponibles en línea, evidencian un aumento significativo en la participación digital de los ciudadanos. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo
CONPES 3920 de Big Data, del 17 de abril de 2018	Política Nacional de Explotación de Datos (Big Data) Este documento CONPES busca sentar las bases para una política pública integral que habilita el aprovechamiento de los datos para generar desarrollo social y económico.
CONPES 3975 de 2019	Tiene como objetivo impulsar la productividad y el bienestar de los ciudadanos, a través del uso estratégico de las tecnologías digitales en el sector público y privado.
CONPES 3995 de 2020	Por el cual se establece la Política Nacional de Confianza y Seguridad Digital.
CONPES 4023 de 2021	Política para la Reactivación, la Repotenciación y el Crecimiento Sostenible e Incluyente
CONPES 4070 de 2021	Lineamientos de Política para la Implementación de un Modelo de Estado Abierto.
Circular 02 de 2019	Con el propósito de avanzar en la transformación digital del Estado e impactar positivamente la calidad de vida de los ciudadanos generando valor público en cada una de las interacciones digitales entre ciudadano y Estado y mejorar la provisión de servicios digitales de confianza y calidad.

Marco Normativo	Descripción
Directiva Distrital 002 de 2002	Respeto al derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software).
Directiva 005 de 2005	Por medio de la cual se adoptan las Políticas Generales de Tecnología de Información y Comunicaciones aplicables al Distrito Capital.
Directiva 02 de 2019	Simplificación de la interacción digitalmente los ciudadanos y el estado.
Directiva 005 de 2020	Directrices sobre gobierno abierto de Bogotá de la Alcaldía Mayor de Bogotá.
Directiva 02 de 2022	Las entidades que conforman la administración pública no han sido ajenas a la dinámica propia del incremento de los incidentes en el ámbito cibernético, con el riesgo de producir impactos negativos a partir de la materialización de incidentes de seguridad en el entorno digital. Por ello, la Seguridad Digital es, sin duda alguna, uno de los retos más importantes que enfrentan todo tipo de organizaciones.
Acuerdo 057 de 2002	Por el cual se dictan disposiciones generales para la implementación del sistema Distrital de Información –SDI-, se organiza la Comisión Distrital de Sistemas, y se dictan otras disposiciones.
Acuerdo 130 de 2004	Por medio del cual se establece la infraestructura integrada de datos espaciales para el Distrito Capital y se dictan otras disposiciones.
Acuerdo 279 de 2007	Dicta los lineamientos para la Política de Promoción y Uso del Software libre en el Sector Central, el Sector Descentralizado y el Sector de las Localidades del Distrito Capital.
Acuerdo 409 de 2009	Por el cual se modifica la integración de la Comisión Distrital de Sistemas.

Marco Estratégico

Motivador	Fuente
Estrategia Nacional	Plan Nacional de Desarrollo “Colombia potencia mundial de la vida” Objetivos de Desarrollo Sostenible Plan TIC Nacional:

Motivador	Fuente
	Gobierno digital para la gente. Se diseñará e implementará una estrategia que acelere la digitalización de trámites e impulse el desarrollo de modelos de identidad digital y la masificación de servicios ciudadanos digitales. Asimismo, se adelantarán ajustes normativos e institucionales que favorezcan la compra y uso inteligente y estratégico de las TIC para proveer productos y servicios innovadores que resuelvan problemáticas y generen valor público. ***Estrategia para el fortalecimiento de la Ciberseguridad. "En respuesta al incremento del conjunto de amenazas cibernéticas que actualmente afectan a las personas, se requiere institucionalizar una hoja de ruta de mediano y largo plazo para el fortalecimiento de las capacidades del ecosistema cibernético nacional en materia de ciberseguridad".***
Estrategia Distrital	Plan Distrital de Desarrollo 2024 al 2027 - El cual involucra en este a la UAECOB, en : 1°El obejtivo 5: "**B***ogotá confía en su gobierno: Lograremos una ciudad pujante, donde uno quiera vivir, requiere de un Gobierno que atienda las necesidades, garantice los derechos de las personas y brinde un servicio amable, ágil y oportuno en todo el territorio con un gasto eficiente. Un gobierno, en el que la ciudadanía crea y confíe."* En la Estrategia 1: Bogotá se fortalece con un gobierno abierto, cercano, eficiente, transparente e íntegro. En el Programa 33: Fortalecimiento institucional para un gobierno confiable. Y la meta del Plan de Desarrollo que aplica es un plan para el fortalecimiento de las capacidades institucionales de la UAECOB." "Desarrollar Implementar una red para aumentar la cobertura de capacidades, reducir los tiempos de respuesta y recuperación en la atención emergencias del Cuerpo Oficial de Bomberos en Bogotá Región. 2° Estructurar un sistema integrado de atención a emergencias y desastres naturales que garantice la capacidad de respuesta frente a los desafíos del cambio climático y reduzca las vulnerabilidades de este en la ciudad región, que contribuyen al Plan de manera directa al cumplimiento de su objetivo general frente a la necesidad de la Entidad. Anexo: Anexo 2. Políticas Públicas y POT con el PDDhttps://www.sdp.gov.co/sites/default/files/anexo_2._politicas_publicas_y_pot.xlsx 9Meta PDD 2024 – 2027 Implementar un programa para mejorar la respuesta en la atención a emergencias del Cuerpo Oficial de Bomberos de Bogotá apalancada en redes de conocimiento prevención del riesgo y cobertura en la ciudad y su entorno
Estrategia Sectorial e Institucional	El Plan Estratégico Institucional de la Unidad Administrativa Especial del Cuerpo Oficial de Bomberos Bogotá (UAECOB) para el periodo 2024 al 2027, Involucra las estrategias del Plan Distrital de Desarrollo: Bogotá protege el ambiente y se compromete con la acción climática.

Motivador	Fuente
	Bogotá se fortalece con un gobierno abierto, cercano, eficiente, transparente e íntegro. Los programas que hacen parte de las estrategias para la UAECOB son: Aumento de la resiliencia al cambio climático y reducción de la vulnerabilidad Fortalecimiento institucional para un gobierno confiable. Metas que hacen parte: Implementar un programa para mejorar la respuesta en la atención a emergencias del Cuerpo Oficial de Bomberos de Bogotá, apalancada en redes de conocimiento, prevención del riesgo y cobertura en la ciudad y su entorno. Desarrollar un plan para el fortalecimiento de las capacidades institucionales de la UAECOB.
Lineamientos y Políticas	Política de Gobierno Digital Marco de la Transformación Digital Modelo Integrado de Planeación y Gestión – MIPG Entre otros en el marco de la normativa vigente institucional, Función Pública y MINTIC

Operación

La seguridad de la información opera desde la Dirección de LA UAECOB en el marco dereferencia de la norma ISO/ NTC 27001:2013 la cual tuvo vigencia hasta marzo 2024. Sin embargo, la UAECOB ya está tomando en cuenta la norma ISO / NTC 27001:2022.

Estructura Organizacional UAECOB.

Fuente: Oficina Asesora de Planeación – U.A.E. Cuerpo Oficial de Bomberos de Bogotá

PLANEACION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION Y CIBERSEGURIDAD.

En La UAECOB se trabaja permanentemente en pos de implementar el SGSI siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL con el fin de preservar la integridad, confidencialidad, disponibilidad y privacidad de la información mediante la adecuada gestión del riesgo, la aplicación de la normatividad vigente y la implementación de mejores prácticas relacionadas con seguridad de la información.

PHVA: En efecto, el modelo del SGSI se encuentra basado en el ciclo de mejoramiento continuo PHVA (Planear, hacer, actuar y verificar), el cual asegura que el SGSI esté expuesto a revisiones continuas cuando existe un cambio importante en la infraestructurao se requiera mejorar su efectividad dependiendo de las mediciones de parámetros claves de su operación. Se cuenta, entonces, conun ciclo que permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI.

A continuación, se listan los componentes de cada una de estas fases del ciclo:

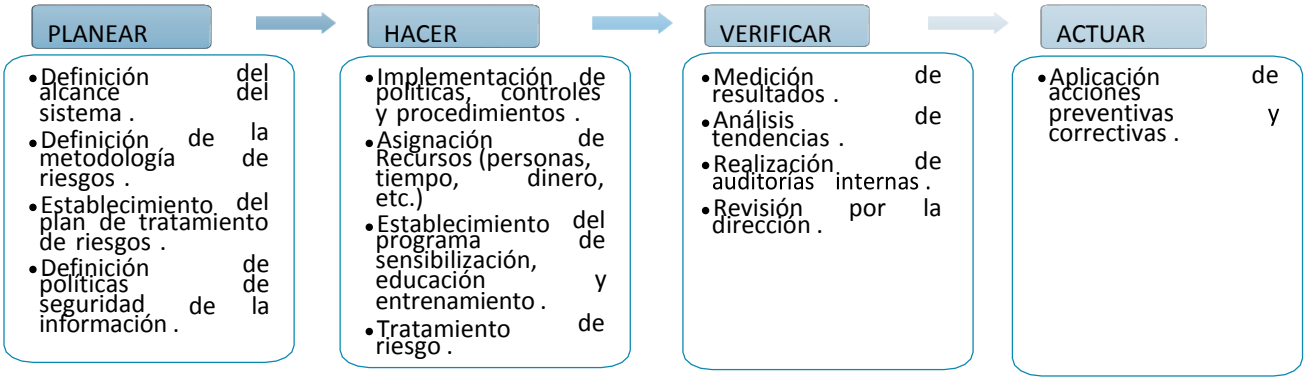


Ilustración . Fases del ciclo PHVA

CONTEXTO INTERNO

FACTORES DE RIESGO OPERATIVO

Son las principales situaciones generadoras de riesgos operativos que pueden o no generar pérdidas. Son factores de riesgo: el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos. Dichos factores se deben clasificar en internos o externos.

FACTORES INTERNOS

Son aquellas situaciones generadoras de eventos de riesgo operativo al interior de LA UAECOB relacionados con: el recurso humano, los procesos, la tecnología y la infraestructura física.

RECURSO HUMANO

Es el conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos de LA UAECOB.

a. Se entiende por vinculación directa, aquella basada en un contrato de trabajo en los términos de la legislación vigente.

b. La vinculación indirecta hace referencia a aquellas personas que tienen con LA UAECOB una relación jurídica de prestación deservicios, diferente a aquella que se origina en un contrato de trabajo.

c. Ciudadanía

TECNOLOGÍA

Es el conjunto de herramientas empleadas para soportar los procesos de LA UAECOB, que incluye: hardware, software y telecomunicaciones.

ANÁLISIS DOFA.

Luego de identificar los actores internos y externos, a continuación, se presenta el análisis DOFA (debilidades, oportunidades,fortalezas y amenazas) identificado por LA UAECOB con relación a la seguridad de la información **y ciberseguridad**

	Componentes Internos		**Componentes Externos**	
	Fortalezas		**Oportunidades**	
Factor Positivo	F1.	Personal altamente calificado, rigurosidad técnica y con habilidades de liderazgo.	O1.	Aprender de los incidentes conocidos ocurridosen otras entidades del sector público y Organizaciones.
	F2.	Programas de sensibilización y transferencia de conocimiento actualizados e implementados.	O2.	Mantener comunicación activa con Organismoso entidades del Gobierno frente a temas de Seguridad y ciberseguridad como por ejemplo elCOLCERT, ACDTIC, MINTIC, entre otras.
	F3.	Se cuenta el diseño y el desarrollo de la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI,el cual se encuentra en el 81% de su implementación total.	O3.	Lograr que los objetivos del Plan Estratégico Institucional se cumplan con un alto nivel de Seguridad en el manejo de la Información.
	F4.	Se implementan soluciones robustas para la ciberseguridad como gestión automática de vulnerabilidades, sistema DLP para prevenir fugas de datos, esquemas apropiados de backup y restauración de datos, así como apropiados esquemas de Plan de Recuperación de Desastres.	O4.	Implementación de un Plan de Continuidad Institucional.

	F5.	La implementación actual de la seguridad del Datacenter en el edificio principal de LA UAECOB. Y centro alterno de datos con proveedor de nube cuyas plataformas se hospedan en Datacenter TIER IV en Tocancipa.	O5.	Diseñar e implementar servicios deciberseguridad innovadores que incorporen medidas robustas según las necesidades de LA UAECOB.
	Debilidades		Amenazas	
	D1.	LA UAECOB debe fortalecer la aprobación de los documentos asociados con la seguridad de la información y ciberseguridad, estableciendo un equipo técnico de seguridad de la información delegado por los Directivos del Comité Institucional de Gestión de Desempeño de la Entidad.	A1.	Ataques cibernéticos a la UAECOB.
	D2.	La UAECOB debe fortalecer los programas de sensibilización, capacitación y divulgación a los funcionarios, contratistas y proveedores frente al MSPI.	A2.	Terremotos o desastres naturales que afectan ladisponibilidad de los servicios.
Factor Negativo	D3.	LA UAECOB debe fortalecer el plan de tratamiento de los riesgos que afecten el MSPI	A3.	Perdida parcial o total de la información crítica para el cumplimiento de la operación.
	D4.	LA UAECOB debe fortalecer y mejorar el seguimiento y monitoreo de los controles implementados para verificar la efectividad y eficacia de estos.	A4.	Daños a infraestructura critica.
	D5.	La UAECOB carece de seguimiento a los proveedores y terceros frente al cumplimiento del MSPI.	A5.	Cambios de las normativas y legislativos vigentes que afecten el MSPI.
	D6.	Garantizar el nivel de seguridad física en las estaciones de la UAECOB, controlando el ingreso y salida del personal, así como los activos de información de la UAECOB.		
	D7.	Constante rotación del personal operativo responsable de los Procesos y de la administración de plataformas tecnológicas.		

INFRAESTRUCTURA FÍSICA

Es el conjunto de elementos de apoyo para el funcionamiento de la UAECOB que incluye entre otros los siguientes: edificios, espacios de trabajo, almacenamiento y transporte.

PROCESOS DE CONTROL

Son los procesos definidos para gestionar los riesgos identificados en las diferentes actividades que realiza la UAECOB, así como la validación al cumplimiento de la normatividad vigente. Proceso de control: Auditoría Interna.

PARTE INTERESADA	DESCRIPCIÓN
Usuarios directos	Ciudadanos
Usuarios Indirectos	Distrito y la ciudadanía.
Entidades públicas.	Autoridades del sector público y entes del Gobierno.
Terceros relacionados	Gremios de la producción, la academia, centros de investigación, proveedores, medios decomunicación, en general sector público y sector privado.
Entidades de Bomberos externas	Dirección Nacional de Bomberos y otros cuerpos de Bomberos a nivel país y organismos del sector de seguridad, justicia y convivencia.

La metodología utilizada para el desarrollo del PESIC se muestra y se explica a continuación:

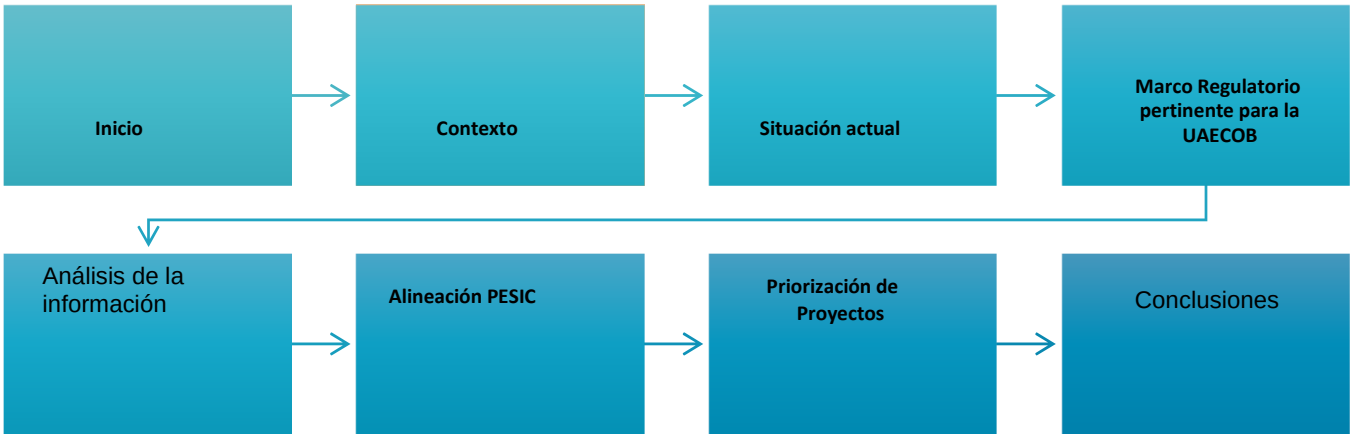


Ilustración 5. Metodología Utilizada

CONTEXTO

En esta fase inicial del desarrollo del PESI, se busca entender las características principales de LA UAECOB con el fin de que los objetivos de este Plan estén alineados con los objetivos estratégicos de la entidad. Entre los aspectos que se deben considerar para lograr este entendimiento están:

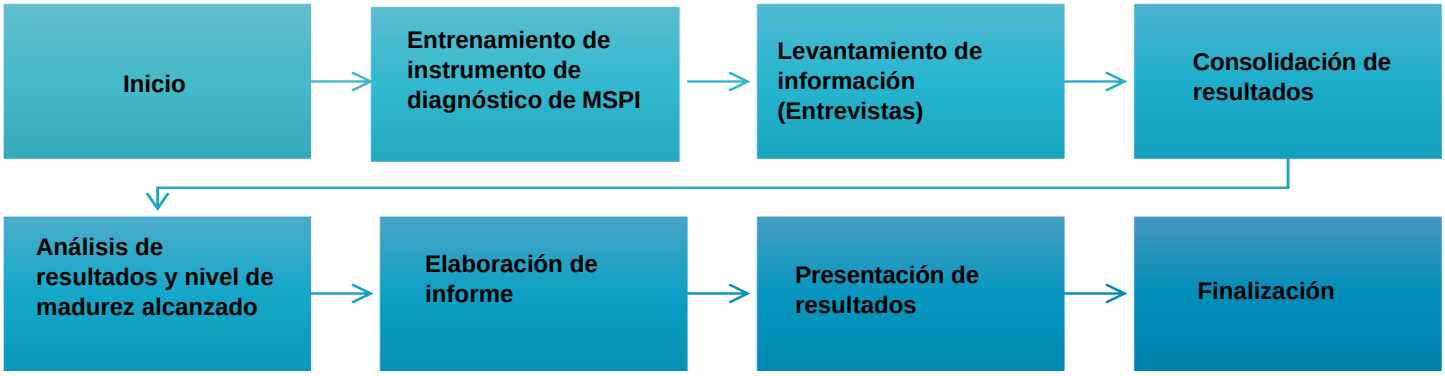
- La misión
- La visión
- Historia y antecedentes
- Estructura organizacional
- Procesos
- Cultura y valores
- Legislación pertinente

SITUACIÓN ACTUAL

Por situación actual se entiende el nivel de madurez que posee en este momento LA UAECOB con relación al Modelo de Seguridad y Privacidad de la Información. El proceso por el cual se lleva a cabo esta estimación del nivel de madurez se denomina Instrumento de diagnóstico del MSPI de MINTIC. Para poder realizar el PESI es indispensable que se tenga en cuenta los niveles de madurez alcanzados por cada uno de los dominios con el fin de plantear prioridades sobre su implementación (ver figura a continuación).

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**Nivel de Madurez**
A.5	CONTROLES ORGANIZACIONALES (37controles)	81	100	**OPTIMIZADO**
A.6	CONTROLES DE PERSONAS (8 controles)	83	100	**OPTIMIZADO**
A.7	CONTROLES FÍSICOS (14 controles)	91	100	**OPTIMIZADO**
A.8	CONTROLES TECNOLÓGICOS (34 controles)	70	100	**GESTIONADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**81**	**100**	**OPTIMIZADO**

La metodología utilizada para realizar el GAP se presenta a continuación:



El nivel de madurez permite establecer las bases para la mejora continua del proceso de Seguridad de la Información y Ciberseguridad de LA UAECOB, e identificar las iniciativas de seguridad de la información, los cuales deben estar alineadas a las necesidades que se identificaron en Plan Estratégico de tecnologías de información y comunicaciones y la estrategia de información (PETI). En seguida, se presenta el nivel demadurez del modelo de seguridad y privacidad de la información y el porcentaje de cumplimiento de la UAECOB frente a los dominios de la norma ISO/IEC 27001:2022 y ISO/IEC 27002:2022.

Esto nos deja en el nivel de optimizado, que significa:

Tabla de Escala de Valoración de Controles		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

U.A.E. CUERPO OFICIAL BOMBEROS BOGOTÁ D.C.

En el framework de ciberseguridad se obtiene:

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	**CALIFICACIÓN ENTIDAD**	**NIVEL IDEAL CSF**
GOVERNAR	76	100
IDENTIFICAR	87	100
PROTEGER	67	100
DETECTAR	80	100
RESPONDER	80	100
RECUPERAR	79	100
PROMEDIO	**78,17**	

ANALISIS Y PRIORIZACION DE INICIATIVAS DE SEGURIDAD DE LA INFORMACION

Teniendo en cuenta el resultado anterior, se identifican las iniciativas de seguridad de la información, los cuales deben estar alineadas al plan estratégico de LA UAECOB, y a los resultados de la calificación actual del instrumento de diagnóstico del Modelo de seguridad yprivacidad de la información. De otra parte, es importante que las iniciativas estén enmarcadas dentro de los controles sugeridos para garantizar una adecuada arquitectura de seguridad de la información y un esquema de defensa a profundidad utilizando soluciones y tendencias de seguridad de la información y de tecnología. Estas iniciativas fueron seleccionadas de acuerdo con el nivel de madurez de cada Dominio de controles teniendo como referencia la calificación actual obtenida.

DEFINICIÓN DEL PORTAFOLIO DE PROYECTOS DE SEGURIDAD DE LA INFORMACIÓN

En esta etapa se define el portafolio de proyectos del plan estratégico PESI:

INICIATIVAS DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD

No.	PROYECTO	DESCRIPCION	AVANCES	REQUIERE INVERSIÒN
I01	Elaboración plan estratégico de seguridad de la información.	Planificación y control operacional, Elaborar el plan estratégico de seguridad de la información y ciberseguridad	EN PROCESO	NO
I02	Implementación del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Continuidad de Negocio	El SGSI no ha tenido continuidad en su implementación desde el año 2022, existe toda la documentación de políticas y procedimientos (nuevos y actualizaciones requeridas por el Modelo de Seguridad y Privacidad de la Información), pero algunos no han sido aprobados por la Dirección y por ende no han sido comunicados a los funcionarios y contratistas y partes interesadas. Fortalecer la toma de conciencia, sensibilización y capacitación en seguridad de la información y ciberseguridad.	EN PROCESO	SI
I03	Integrar los componentes del sistema de gestión de seguridad de la información en el ciclo de vida de los proyectos de LA UAECOB	Definir e integrar la seguridad de la información y ciberseguridad en el ciclo de vida de los proyectos para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto.	EN PROCESO	NO

No.	PROYECTO	DESCRIPCION	AVANCES	REQUIERE INVERSIÒN
I04	Desarrollar el programa de capacitación y sensibilización en seguridad de la información para funcionarios, contratistas, proveedores y terceros.	Diseñar y documentar un programa anual de sensibilización y capacitación en seguridad de la información para funcionarios, contratistas, proveedores y terceros de LA UAECOB. Implementar el programa anual de sensibilización y capacitación en seguridad de la información para funcionarios, contratistas, proveedores y terceros de LA UAECOB	**EN PROCESO**	**SI**
I05	Sistema de control de acceso para dispositivos móviles e implementación de VPN's en Teletrabajo.	Verificar el procedimiento actual de entrega de dispositivos e información a la cual tienen acceso al mismo. Definir, desarrollar y adoptar una política y procedimiento para dispositivos móviles e implementación de VPN en teletrabajo. Verificar la necesidad de implementar una herramienta de MDM- Mobile Device Management	**EN PROCESO**	**SI**
I06	Fortalecimiento del sistema de seguridad adaptativa. (analiza el perfil de riesgo de un usuario en función de su comportamiento histórico, por ejemplo, demasiados intentos de conexión incorrectos y demasiados intentos de autenticación multifactor (MFA) incorrectos.	Identificar un esquema de defensa en profundidad de acuerdo a las necesidades de LA UAECOB. Implementar un esquema de defensa en profundidad que cuente con análisis de comportamiento, inteligencia artificial, escaneo para aprendizaje (machine learning), que permitan reducir la vulnerabilidad a las amenazas que puedan presentarse en estaciones de trabajo. Acompañar al departamento de tecnología en la implementación del XDR y colaborar en las tareas asignadas a seguridad de la información y ciberseguridad.	**IMPLEMENTADO SE DEBE MANTENER**	**SI**

No.	PROYECTO	DESCRIPCION	AVANCES	REQUIERE INVERSIÓN
I07	Fortalecimiento de la gestión del riesgo de seguridad de la información y ciberseguridad.	Actualizar los activos de información y realizar su valoración según la criticidad para la compañía, igualmente identificar los riesgos de seguridad de la información asociados. Identificar los riesgos de seguridad de la información para cada uno de los procesos. Gestionar el Tratamiento de riesgos de seguridad de la información de los riesgos identificados en cada uno de los procesos. Las actividades relacionadas con la herramienta de riesgos son: 1) Identificar herramientas para la gestión de riesgos de seguridad de la información y ciberseguridad. 2) Evaluar su funcionalidad 3) Cuantificar recursos, tiempo y costos asociados 4) Implementar demostración de la solución para LA UAECOB 5) Generar informe ejecutivo a la Alta Dirección. 6) Aprobación de la gerencia. 7) Contratar, capacitar, socializar, sensibilizar, desarrollar capacidades en gestión de riesgos digitales. 8) Mantener actualizados y evaluados permanentemente los riesgos asociados con la seguridad de la información y ciberseguridad.	**EN PROCESO**	**NO**
I08	Implementación del plan de continuidad del Negocio	Implementar el plan de continuidad del negocio de LA UAECOB que contemple los procesos críticos basado en los requerimientos del Modelo de Seguridad y Privacidad de la Información y de la Norma ISO 27001:2022, así mismo revisar y aprobar el plan de continuidad de negocio por la Dirección para luego ser llevado al comité institucional de Gestión y Desempeño de la UAECOB. Implementar y Documentar los planes de continuidad de negocio basado en la Norma ISO 22301:2019 Sistema de Gestión de Continuidad del Negocio- Marco de requisitos, así mismo Aprobar los planes de continuidad por la alta dirección. Diseñar y documentar el programa de pruebas del plan de recuperación ante desastres, ante escenarios de fallas de las tecnologías, garantizando que se mantengan los controles de seguridad.	**EN PROCESO**	**SI**

No.	PROYECTO	DESCRIPCION	AVANCES	REQUIERE INVERSIÓN
I09	Actualización del plan de recuperación de desastres.	Diseñar planes de recuperación ante desastres que contemplen los procesos críticos de LA UAECOB basado en los requerimientos del Modelo de Seguridad y Privacidad de la Información. Si es aprobado por la Dirección realizar la implementación del plan de recuperación de desastres basado en la Norma ISO 22301:2019 Sistema de Gestión de Continuidad del Negocio- Marco de requisitos. Implementar y Documentar los planes de recuperación ante desastres basado en la Norma ISO 22301:2019 Sistema de Gestión de Continuidad del Negocio- Marco de requisitos, así mismo aprobar los planes de continuidad por la alta dirección. Diseñar y documentar el programa de pruebas del plan de recuperación ante desastres, ante escenarios de fallas de las tecnologías, garantizando que se mantengan los controles de seguridad.	**IMPLEMENTADO SE DEBE MANTENER**	**SI**
I10	Adquisición de herramientas para soportar esquemas de alta disponibilidad para dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core.	El responsable de redes y comunicaciones verificará la implementación de esquemas de alta disponibilidad para dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core.	**EN PROCESO**	**SI**
I11	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	Definir y establecer un procedimiento formal para el tratamiento de información de producción en ambientes de desarrollo y prueba, en el cual se establezcan controles para proteger la confidencialidad de la información.	**INICIADO**	**SI**
I12	Desarrollar la metodología para el ciclo de desarrollo de software seguro para cumplimento de los proveedores.	Definir y establecer la metodología de desarrollo seguro para LA UAECOB y sus proveedores de software.	**INICIADO**	**SI**
I13	Monitoreo de accesos y privilegios de TI	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios. Gestionar el cumplimiento del ciclo de vida de gestión de usuarios (creación, modificación, activación, desactivación, eliminación, entre otros) verificando que se cumple para todas las aplicaciones.	**INICIADO**	**SI**
I14	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	Definir e implementar una política sobre el uso de controles criptográficos para la protección de la información en la organización.	**INICIADO**	**NO**

No.	PROYECTO	DESCRIPCION	AVANCES	REQUIERE INVERSIÒN
I15	Evaluación y desempeño de proveedores y terceras partes.	Monitorear a los terceros periódicamente para verificar que los controles de seguridad, los acuerdos de servicio definidos y demás requerimientos de seguridad que se contrataron están siendo implementados, operados y mantenidos.	**INICIADO**	**SI**
I16	Gestión de accesos	Revisar la implementación de la gestión centralizada de usuarios para todos los aplicativos de LA UAECOB de parte del departamento de Tecnología. Implementación de Single Sign On.	**NO INICIADO**	**SI**
I17	Revisar e investigar una solución para la implementación de una solución para aseguramiento y gestión de cuentas privilegiadas (Modulo IAM)	Revisar e investigar una solución para la implementación de la gestión para usuarios privilegiados. Asegurar y monitorear las acciones de las cuentas privilegiadas en las plataformas tecnológicas críticas de LA UAECOB, según los privilegios otorgados por el departamento de Tecnología. Las actividades relacionadas con la herramienta o solución son: 1) Identificar herramientas para la gestión de usuarios privilegiados en el mercado. 2) Evaluar su funcionalidad 3) Cuantificar recursos, tiempo y costos asociados 4) Implementar demostración de la solución para LA UAECOB 5) Generar informe ejecutivo a la Alta Dirección. 6) Aprobación de la gerencia. 7) Contratar, capacitar, socializar, sensibilizar, desarrollar capacidades en gestión de riesgo corporativo. 8) Mantener actualizados y evaluados permanentemente los riesgos asociados con la seguridad de la información y ciberseguridad.	**INICIADO**	**SI**

No.	PROYECTO	DESCRIPCION	AVANCES	REQUIERE INVERSIÓN
I18	Revisar e investigar una solución para la implementación de Software para borrado seguro de Información	Revisar e investigar una solución para la implementar una solución de borrado seguro de información Las actividades relacionadas con la herramienta o solución son: 1) Identificar herramientas para borrado seguro en el mercado. 2) Evaluar su funcionalidad 3) Cuantificar recursos, tiempo y costos asociados 4) Implementar demostración de la solución para LA UAECOB 5) Generar informe ejecutivo a la Alta Dirección. 6) Aprobación de la gerencia. 7) Contratar, capacitar, socializar, sensibilizar, desarrollar capacidades en gestión de riesgo corporativo. 8) Mantener actualizados y evaluados permanentemente los riesgos asociados con la seguridad de la información y ciberseguridad.	EN PROCESO	SI
I19	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información.	Verificar o acompañar según corresponda, la implementación por parte del departamento de Tecnología, una solución de antimalware avanzado para la protección contra amenazas avanzadas persistentes (APT).	EN PROCESO	SI
I20	Asesoría en la Adquisición de Servicio de análisis de vulnerabilidades, hacking Ético pentesting, revisión de código seguro.	Desarrollar un RFI para que el departamento de Tecnología lo envíe a los Proponentes seleccionados. Revisar las propuestas recibidas y generar un cruce de información entregada para su presentación al departamento de tecnología. Acompañar las pruebas de Hacking Ético sobre los aplicativos críticos. Proponer, esperar autorización de la Dirección de TI para establecer e implementar pruebas de análisis de vulnerabilidades y Ethical Hacking.	NO INICIADO	SI
I21	Validar herramientas de cifrado de información automatizados, Repositorio centralizado de información cifrada.	Revisar, investigar o monitorear una solución para la implementación que permita la transferencia segura de archivos, mediante protocolos de cifrado.	INICIADO	SI
I22	Revisar e investigar una solución DLP (Data Loss Prevention) para el correo Electrónico y equipos críticos.	Revisar e investigar una solución de DLP (Data Loss Prevention), con el fin de controlar y monitorear el intercambio de información confidencial y/o sensible para las Bases de Datos que lo requiera.	INICIADO	SI
I23	Revisar e investigar una solución automatizada para la hardenización o endurecimiento de infraestructura tecnológica.	Revisar e investigar una solución automatizada para la hardenización o endurecimiento de infraestructura tecnológica. Monitorear la gestión de plantillas de seguridad en la plataforma tecnológica con el fin de conseguir, endurecer, monitorear y configurar los sistemas informáticos de manera segura y eliminar aplicaciones, puertos, protocolos y servicios innecesarios.	INICIADO	SI

No.	PROYECTO	DESCRIPCION	AVANCES	REQUIERE INVERSIÓN
I24	Evaluación y desempeño del sistema de Gestión de seguridad de la información.	Implementar y monitorear los indicadores de gestión y desempeño del sistema de gestión de seguridad de la información. Revisar con el departamento de Tecnología cuales indicadores podemos generar relacionados con el MSPI.	**INICIADO**	**NO**
I26	Doble factor de autenticación	Revisar la implementación con el departamento de Tecnología de las conexiones seguras entre los usuarios y los servicios en línea.	**EN PROCESO**	**SI**
I27	Fortalecimiento de capacidades en gestión de incidentes	Capacitar a los usuarios sobre el registro de incidentes en la herramienta de mesa de ayuda e implementar y validar funcionalidades de la herramienta	**INICIADO**	**NO**
I28	Revisión independiente de la gestión de la seguridad de la información	Realizar revisiones independientes sobre las políticas, lineamientos y implementación de la seguridad de la información. Realizar visitas a las sedes y estaciones de Bomberos a fin de validar el cumplimiento de las políticas de seguridad de la Información.	**INICIADO POR CONTROL INTERNO**	**SI**

ALINEACIÓN PESI

La alineación del PESI busca sincronizar los objetivos estratégicos de TI, el cual define lineamientos para el mejoramiento del nivel de madurez institucional en la implementación de soluciones tecnológicas que generen valor y promuevan el cumplimiento de la misión con sostenibilidad tecnológica. Así mismo el PESI define objetivos que permiten asegurar la confidencialidad, integridad y disponibilidad delos activos de información. para ello se establecen los objetivos de TI que están directamente involucrados en el plan estratégico de seguridad de la información.

El objetivo principal que busca el Plan Estratégico Institucional -PEI- 2024-2027 de la UAECOB es otorgar los lineamientos institucionales y orientadores de la planificación para el presente cuatrienio, basado en 3 ejes estructurales “Proteger-Potenciar-Participar” P3, estableciendo para ello las diferentes acciones estratégicas concertadas año por año en las actividades del Plan de Acción Institucional.

Teniendo en cuenta el P.E.I 2024-2027 el objetivo estratégico del segundo eje estructural “POTENCIAR” y el cual va alineado con tecnología es la Modernizar la gestión y el desempeño institucional a través de la articulación efectiva de los procesos, con innovación pública, transparencia y seguridad de la información para garantizar el equipamiento tecnológico y de infraestructura requerido por la misionalidad.

No.	Objetivo
1.	Alinear la estrategia de TI con la estrategia de LA UAECOB.
2.	Maximizar el aporte de las TIC a los procesos internos para la transformación de LA UAECOB.
3.	Ejercer el Gobierno de las TIC de LA UAECOB.
4.	Posicionarse como aliado estratégico de todos los procesos internos de LA UAECOB.
5.	Mejorar la satisfacción de los usuarios, así como la del ciudadano que utiliza los servicios de LA UAECOB.
6.	Proveer información oportuna y de calidad para la toma de decisiones en los procesos internos de LA UAECOB.
7.	Entregar oportunamente sistemas de información de calidad, funcionales, eficientes y confiables fortaleciendo los procesos internos de LA UAECOB.
8.	Fortalecer la Gestión de las TIC y de la seguridad de la información en los procesos internos de LA UAECOB.
9.	Fortalecer las competencias y desarrollo profesional del equipo de TI de LA UAECOB.
10.	Desarrollar la capacidad de innovación y prospectiva tecnológica.

Dominio	Objetivo del PESI
Políticas de la seguridad de la información	La adopción de políticas de seguridad de la información debe obedecer a una decisión estratégica, las cuales servirán de directrices para proteger la información de propiedad de LA UAECOB.
Organización de la seguridad de la información	La definición de los roles y responsabilidades para la seguridad de la información es el aspecto fundamental para iniciar y controlar la implementación y la operación de lo relacionado con la protección de la información propiedad de LA UAECOB.

Dominio	Objetivo del PESI
Seguridad de los recursos humanos	Las personas son el componente más importante en todo el modelo de seguridad de la información, por lo tanto, antes de su contratación, durante su permanencia yen el proceso de finalización o cambios de cargo, la UAECOB debe asegurar que los funcionarios y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
Gestión de activos	Identificar los activos de información y definir las responsabilidades de protección apropiadas, asegurar que la información recibe un nivel apropiado de protección, deacuerdo con su importancia para la organización y evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios; son las principales razones de la UAECOB para garantizar la gestión adecuada de los activos y la asignación de las respectivas responsabilidades sobre los mismos.
Control de acceso	Las técnicas de control de acceso permiten proteger la información en términos de la confidencialidad, la integridad y la disponibilidad.
Criptografía	Las técnicas de cifrado ayudan a proteger la información de acuerdo con su nivel de clasificación, la implementación de éstas, el uso apropiado y eficaz de la criptografía permiten proteger la confidencialidad, la autenticidad y/o la integridad de la información propiedad de la UAECOB.
Seguridad física y del entorno	La debida protección de los centros de datos, archivos documentales, equipos,oficinas, entre otros, es un aspecto que se debe considerar cuando se trate de la seguridad de la información.
Seguridad de las operaciones	Lograr que las operaciones protejan la información debe ser un compromiso de laUAECOB.
Seguridad de las comunicaciones	La transferencia de información está expuesta a múltiples riesgos, por ello la UAECOB debe implementar medidas preventivas para evitar su divulgación o modificación.
Adquisición, desarrollo y mantenimiento de sistemas	Mantener la seguridad de la información durante el ciclo de desarrollo requiere contar con una metodología de desarrollo seguro. Las aplicaciones normalmente mantienen información importante de la UAECOB, por esta razón se deben implementar controles de seguridad dentro de ellas.
Relación con los proveedores	Gestión de proveedores y evaluación
Gestión de incidentes de seguridad de la información	La adecuada gestión de los incidentes de seguridad de la información permite proteger los tres pilares de la seguridad: la confidencialidad, la integridad y la disponibilidad de la información. La implementación de estos controles permite asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
Aspectos de seguridad de la información de la gestión de continuidad de negocio	Poder contar con planes para la continuidad del negocio y la recuperación ante desastres es importante para preservar la disponibilidad de la información. La UAECOB debe adoptar estos controles para asegurar la disponibilidad de las instalaciones de procesamiento de información durante una situación adversa, adicionalmente debe verificar a intervalos regulares dichos controles con el fin de asegurar que son válidos y eficaces.

Cumplimiento	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad es importante para no incurrir en demandas, multas u otra clase de afectación a la imagen o reputación de la UAECOB.

PRIORIZACION DEL PORTAFOLIO DE PROYECTOS

Una vez identificadas las iniciativas y los proyectos con base en el resultado de diagnóstico de la situación actual del instrumento del MSPI de MINTIC, es necesario priorizar los proyectos, para lo cual se tuvo en cuenta la estrategia de seguridad de la información.

(Gobierno o Modelo de seguridad de información, Gestión de riesgos de Seguridad, Desarrollo y gestión del programa de seguridad de la información y Gestión de incidentes de seguridad de la información). Para ello se construyeron las siguientes categorías de prioridad que permiten evaluar y determinar una secuencia sistemática para el desarrollo del Plan Estratégico de seguridad de la Información y ciberseguridad (PESIC):

PRIORIDAD	
PRIORIDAD	**DESCRIPCION**
0	Elaboración del presente Plan Estratégico de Seguridad de la Información.
1	Gobierno o Modelo de seguridad de información, el cual Incluye las iniciativas que soportan el desarrollo del modelo de seguridad de la información.
2	Gestión de Riesgos Operacionales: Hace referencia a los proyectos y actividades que mitigan los riesgos de seguridad de la información catalogados como relevantes, garantizando salvaguardar la información en su confidencialidad,disponibilidad e integridad.
3	Desarrollo y gestión del programa de seguridad de la información; hace referencia aquellos proyectos que permiten la Operación y mantenimiento del Sistema de Gestión de Seguridad de la información.
4	Desempeño: Soportan aquellos proyectos que permiten la evaluación del desempeño y mejora continua del SGSI.

Evaluación de Desempeño

MARCO CONCEPTUAL DEL PESI:

Para LA UAECOB, son muy importantes los resultados obtenidos en el PESI con el fin de apoyar la implementación del SGSI. El PESIse apoya en el Plan Estratégico De LA UAECOB. Esta metodología tiene en cuenta las siguientes fases: el análisis revisión de Misión, objetivos y estrategias, análisis de la propuesta de Valor, recursos financieros, clientes, procesos, crecimiento y aprendizaje; Reporte, Revisión y Comunicación de resultados, cambio y mejoramiento de las Estrategias laborales de cada miembro de la Entidad, actualización y adaptación permanente frente a cambios internos y externos del entorno. Asimismo, los objetivos y metas son evaluables y medibles, generando sus propios indicadores, que deberán ser utilizados como herramienta para el seguimiento, control, evaluación y gestión de LA UAECOB.

Actualmente el sistema de seguridad de la información opera con cinco indicadores. Durante las fases de mejora, estos indicadores se refinan y se introducen nuevos para respaldar la estrategia general de seguridad de la información. Dentro de LA UAECOB estos indicadores están diseñados para recoger datos de forma clara y a tiempo, asegurando que se hagan mediciones periódicas y se analicen de acuerdo con las tendencias en la consecución de objetivos y metas establecidas.

Si los resultados esperados no se logran, es necesario implementar ajustes y medidas correctivas adecuadas para garantizar que el proceso se ajuste a los estándares establecidos. Es aconsejable que, al menos anualmente, los encargados de los procesos revisende manera exhaustiva los indicadores para garantizar que estén alineados con las políticas y metas definidas

dentro de LA UAECOB.

Es esencial establecer un objetivo que simplifique el análisis y la decisión sobre la introducción de medidas para gestionar riesgos y realizar acciones correctivas o de mejora. Esta meta se puede determinar utilizando uno de los siguientes criterios:

- Atendiendo a las demandas de los stakeholders.
- Basándose en el rendimiento pasado (historial).
- Teniendo en cuenta la trayectoria y aspiraciones de LA UAECOB

En LA UAECOB, poseemos directrices y procedimientos para la planificación y realización de auditorías internas al Sistema Integrado de Gestión. A continuación, algunas consideraciones clave:

- La factibilidad de realizar auditorías se define según la disponibilidad de:

  a) Información adecuada y pertinente para la planificación de las auditorías.

  b) Cooperación activa de aquellos que serán auditados.

  c) Suficiente tiempo y recursos para llevarla a cabo.

- Es vital recopilar evidencias confiables y exhaustivas a través de análisis, inspecciones, observaciones, entrevistas, verificaciones y otros métodos de auditoría, buscando fundamentar sólidamente las conclusiones de la auditoría.
- Es obligatorio ejecutar, al menos, una auditoría interna anual al Modelo de Seguridad y Privacidad de la Información.
- Las auditorías deben apegarse a los lineamientos descritos en las directrices y procedimientos para la realización de auditorías internas del Modelo de Seguridad y Privacidad de la Información.
- Cualquier anomalía detectada en la auditoría se cataloga como una no conformidad real, mientras que cualquier sugerencia se ve como una oportunidad de mejora. La implementación de soluciones varía según la evaluación del auditado y el criterio del auditor designado.
- Para resolver cualquier acción correctiva o mejora identificada en una auditoría interna, es esencial seguir el procedimiento predeterminado.
- Los auditores internos no deben examinar sus propias tareas o procedimientos.

Al planificar el programa de auditoría interna, quienes están a cargo deben considerar la definición del alcance del programa de auditoria lo que incluye:

✓ Establecer las metas del programa de auditoría para guiar su planificación y ejecución.

✓ La finalidad de la auditoría.

✓ El ámbito o rango de acción.

✓ La periodicidad con la que se realizarán las auditorías.

✓ Hallazgos y conclusiones de auditorías anteriores.

✓ Evaluaciones de programas de auditorías pasadas.

✓ Alteraciones relevantes en la estructura de la entidad o en sus funciones.

✓ Evaluaciones previas realizadas por la dirección.

✓ Resultados de análisis de riesgos asociados a los procesos de la entidad.

Identificar los recursos requeridos para el programa de auditoría, como:

✓ Presupuesto para diseñar, aplicar, supervisar y perfeccionar las actividades de auditoría.

✓ Mecanismos para garantizar y mejorar la habilidad de los auditores.

✓ El alcance del programa de auditoría.

Mejoramiento

Actualmente LA UAECOB, cuenta con un procedimiento para la gestión de la mejora donde se establece una metodología para determinar y seleccionar las oportunidades de mejora e implementar cualquier acción necesaria para cumplir los requisitos previstos en el Modelo de Seguridad y Privacidad de la Información.

Las fuentes potenciales de oportunidades de mejora para el sistema de seguridad de la información son:

1. Revisión de Controles, políticas o procedimientos del sistema de seguridad de la información.
2. Incidentes de Seguridad de la Información
3. El grado de satisfacción de las partes interesadas
4. Experiencias obtenidas de las No Conformidades y de las acciones correctivas relacionadas
5. Estudios comparativos externos de las mejoras practicas
6. Nueva legislación o los cambios propuestos a la legislación vigente para el MSPI
7. Resultados de las auditorías internas
8. Evaluación y análisis de los resultados de seguimiento y medición
9. Opiniones de las partes interesadas
10. Resultados de la Revisión por la Dirección

PROYECTOS DE SEGURIDAD Y CIBERSEGURIDAD DE LA INFORMACIÓN PARA IMPLEMENTAR UN NIVEL DE MADUREZ APROPIADO PARA EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

PROYECTO	**P1. Fortalecimiento del MSPI (Modelo de Seguridad y Privacidad de la Información) Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Continuidad de Negocio**
JUSTIFICACION	El MSPI no ha tenido continuidad en su implementación, se identifican políticas aprobadas pero no existen procedimientos establecidos para los procesos de seguridad preventiva para la ciberseguridad, el comité de seguridad de la información no se ha establecido, existe un comité tecnológico, pero ocasionalmente se tratan temas de riesgos digitales y de seguridad de la información. Es necesario incluir el componente de ciberseguridad, así como ajustar los procedimientos asociados. No se cuenta actualmente con una declaración de aplicabilidad donde se refleje el nivel de madurez de los controles establecidos basado en Anexo ISO 27002.

OBJETIVO DEL PROYECTO	Tomar las acciones correspondientes con respecto a marcos individuales y hacer las inversiones de servicios profesionales y consultorías de mejores prácticas para cerrar la brecha de una manera progresiva en el marco de la seguridad de la información y ciberseguridad.
ALCANCE	Todos los años: 1) Revisión, actualización, adaptación e implementación de las políticas y procedimientos de seguridad de la información, privacidad de la información y ciberseguridad, basado en los lineamientos de las buenas prácticas IS0 27001, ISO 27032, ISO 22301 e ISO 27701. 2) Hacer revisión del sistema actual, realizar las consultorías de verificación según los procesos de información crítica para certificar el sistema de gestión de seguridad de la información enfocado en procesos misionales y de apoyo que manejen información sensible. 3) Gestionar la Declaración de aplicabilidad - SOA de SGSI. 4) Definir y conformar el equipo de respuesta a incidentes que abarque proveedores críticos. 5) Fortalecer el Uso y apropiación de las políticas y procedimientos de seguridad y privacidad de la información, Protección de datos. 7) Robustecer las auditorias al Sistema de gestión de seguridad de la información y ciberseguridad, extendiéndola a los proveedores o terceros de servicios críticos. 8) Establecer la estructura y recursos necesarios para la gestión de la seguridad de la información, ciberseguridad, privacidad y protección de datos. 9) Diseñar y establecer los indicadores que permitan evaluar la eficacia y eficiencia de la gestión de ciberseguridad, seguridad de la información y protección de datos. 10) Establecer un procedimiento para la recolección de evidencia digital on premise. 11) Implementar los procesos relacionados con la gestión y el gobierno de los servicios TI para la gestión de los riesgos asociados con la aplicación de cambios en los negocios críticos o clientes que afecten a las aplicaciones, las interfaces de los sistemas (APIs), las configuraciones y diseños, así como a la infraestructura de red y a los componentes del sistema, integrando a los proveedores de nube o aplicaciones SaaS. 12) Integrar el procedimiento de gestión de cambios, basados en una validación de los resultados esperados en el entorno, que se establezca una preautorización de la dirección adecuada, y que se produzca la notificación, así como la autorización de los clientes, según el acuerdo de nivel de servicio (OLA). 13) Articular el plan de gestión de incidentes con el plan de recuperación de desastres - DRP en caso de que sea un incidente catastrófico. 14) El plan de gestión de seguridad de la información y el plan de tratamiento de riesgos pueden tener actividades comunes no necesariamente cruzadas, la gestión de riesgos debe dar la prioridad de implementación de esas actividades de control.
TIEMPO	24 meses

PROYECTO	P2. Fortalecimiento del sistema de seguridad adaptativa.

JUSTIFICACION	Con el fin de aplicar acciones que apoyen la mitigación de riesgos de seguridad y ciberseguridad de la información, se requiere implementar un esquema de defensa en profundidad que cuente con inteligencia artificial, escaneo de vulnerabilidades, que permitan reducir la vulnerabilidad a las amenazas de manera automática en la plataforma tecnológica de la UAECOB, así como realizar continuamente requerimientos de hardenización sobre plataformas críticas.
OBJETIVO DEL PROYECTO	Automatizar y mejorar la postura de seguridad con herramientas y soluciones de protección de amenazas emergentes a nivel de servidores y a nivel de estaciones de trabajo.
ALCANCE	Algunas de las soluciones propuestas para este fortalecimiento son: 1) Herramienta que permita realizar escaneo de vulnerabilidades a toda la plataforma tecnológica. 2) Herramienta que permite remediación automática en un alto porcentaje de componentes de la plataforma tecnológica. 3) Herramienta que permita actualizaciones controladas sobre componentes críticos de la plataforma tecnológica 4) Herramienta que permita mejorar la postura de seguridad en componentes críticos a través de la hardenización.
TIEMPO	24 meses

PROYECTO	P3. Mantener el DRP (Plan de Recuperación de Desastres Tecnológico) para asegurar que la UAECOB pueda gestionar de manera efectiva las crisis y desastres, protegiendo sus operaciones, activos y reputación mientras mantiene la continuidad del negocio.
JUSTIFICACION	Un Plan de Recuperación de Desastres (DRP) es fundamental en la ciberseguridad y en la gestión de TI por varias razones: **Minimiza el Tiempo de Inactividad:** Un DRP bien diseñado ayuda a reducir el tiempo de inactividad en caso de un desastre, ya sea un ataque cibernético, un fallo de hardware, un desastre natural o cualquier otro incidente que pueda interrumpir las operaciones. Esto es crucial para mantener la continuidad del negocio y minimizar la pérdida de productividad. **Protege la Información Crítica**: Los datos personales de los ciudadanos son uno de los activos más valiosos de la UAECOB. Un DRP incluye estrategias para la protección, recuperación y restauración de la información crítica, asegurando que los datos importantes no se pierdan o se corrompan durante un incidente. **Garantiza la Continuidad del Negocio:** Un DRP proporciona un marco para que las operaciones esenciales continúen funcionando incluso en medio de una crisis. Esto es vital para mantener la confianza de los ciudadanos y cumplir con los compromisos misionales de la entidad. **Reduce el Impacto Financiero:** Los desastres y los incidentes de seguridad pueden ser costosos. Tener un DRP ayuda a mitigar estos costos al permitir una recuperación más rápida y eficiente, lo que reduce el impacto financiero en la UAECOB. **Cumple con Requisitos Regulatorios:** Muchas industrias y sectores tienen requisitos regulatorios específicos sobre la gestión de riesgos y la recuperación ante desastres. Tener un DRP ayuda a garantizar el cumplimiento con estas normativas y evita posibles sanciones legales.

	Mejora la Resiliencia Organizacional: La preparación y planificación para desastres fortalece la resiliencia general de la UAECOB, haciendo que sea más adaptable y capaz de manejar eventos inesperados. **Facilita la Comunicación en Crisis**: Un DRP incluye planes de comunicación que aseguran que todos los miembros del equipo, así como los ciudadanos y proveedores, estén informados de manera adecuada durante y después de un incidente.
OBJETIVO DEL PROYECTO	Asegurar que la UAECOB pueda continuar operando y recuperar sus operaciones normales de manera rápida y eficiente después de un incidente crítico o desastre.
ALCANCE	Infraestructura de TI: Servidores, redes, sistemas de almacenamiento, bases de datos, aplicaciones y servicios críticos. Datos: Información sensible, bases de datos y archivos importantes para la operación de la UAECOB. Recursos Humanos: Personal clave y roles críticos necesarios para la recuperación. Equipos y Tecnología: Hardware, software y otros equipos esenciales para la operación.
TIEMPO	24 meses

PROYECTO	P4. Implementación de herramientas de análisis de comportamiento en el uso de las redes y el comportamiento de los usuarios en el acceso a los servicios de tecnología
JUSTIFICACION	Ante la constante situación de amenazas persistentes, la complejidad del malware y el tráfico malicioso se hace necesario implementar herramientas de análisis de comportamiento (machine learning) que le permitan a la entidad tomar acciones contra estos patrones anómalos no identificados.
OBJETIVO DEL PROYECTO	Bloquear comportamientos anómalos en la red y en los sistemas la UAECOB
ALCANCE	Como mínimo se debe implementar las siguientes soluciones: 1) 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, el monitoreo sobre anomalías, altos consumos, mayores aplicaciones usadas, e Indicador de compromiso (IoC) que conlleve hacia un fraude o malware avanzado. 2) Establecer un servicio o mecanismos de Análisis de comportamiento del usuario (User behavior analytics) que permita monitorear y detectar anomalías, las cuales pueden llevar a fraude o robo de información para beneficio propio, bien sea intencionales o por algún ente externo que esté usando una credencial de usuario de la entidad
TIEMPO	24 meses

PROYECTO	P5. Implementación de herramientas y procedimientos para desarrollo seguro
JUSTIFICACION	Fortalecer la seguridad en el ciclo de vida de sistemas de información.

OBJETIVO DEL PROYECTO	Asegurar los sistemas de información de la UAECOB publicados en la WEB (intranet e internet) están utilizando metodologías de desarrollo seguro.
ALCANCE	Las actividades mínimas para desarrollar son: 1) Actividades precontractuales 2) Aseguramiento de pruebas no funcionales a través de (análisis de vulnerabilidades, análisis de stress o carga, EH, verificación de código seguro). Se plantea una solución similar a Fortify para análisis de código estático. 3) Se plantea solución similar a GITLAB para gestión de código fuente y manejo de versionamientos. 3) Establecer procedimientos y herramientas para la construcción, adquisición, mantenimiento y desarrollo seguro de aplicaciones, APPS, APIS y Sistemas de Información 4) Evaluar prácticas de ingeniería DevOps y DevSecOps para contemplar la tolerancia al riesgo y realizar el análisis de beneficio, se debe capacitar y exigir el uso de esta metodología.
TIEMPO	24 meses

PROYECTO	P6. Implementación de solución automatizada para la hardenización o endurecimiento de infraestructura tecnológica.
JUSTIFICACION	Se requiere asegurar la gestión de plantillas de seguridad en la plataforma tecnológica con el fin de conseguir configurar un sistema informático de manera segura y eliminar aplicaciones y servicios innecesarios.
OBJETIVO DEL PROYECTO	Asegurar la plataforma tecnológica con el fin de encontrar fallas en el sistema para priorizar los ajustes y parcheo de vulnerabilidades.
ALCANCE	El alcance mínimo se enmarca en: 1) Establecer estándares de seguridad (hardening). 2) Configuraciones recomendadas por el fabricante en la aplicación o dispositivo, con el objetivo de no dejar parámetros con valores que deja el fabricante por defecto. 3) Cada sistema operativo deberá ser fortalecido para proporcionar sólo los puertos necesarios, protocolos y servicios para satisfacer las necesidades del negocio y tener vigentes los controles técnicos de apoyo tales como: antivirus, integridad de los ficheros de monitorización y el inicio de sesión como parte de su línea base de operativa estándar o plantilla. 4) Realizar el endurecimiento de infraestructura a nivel de: servidores, bases de datos, aplicaciones, elementos activos de red. (ej. Tripwire).
TIEMPO	24 meses

PROYECTO	P7. Implementar Gestión de Identidad y Accesos (IAM) para proteger los activos de información, mejorar la gestión de identidades y accesos e Implementación de solución para aseguramiento y gestión de cuentas privilegiadas. Esta solución debe

	integrarse como parte del IAM y permitir Single Sign On para autenticación única en los diferentes aplicativos.
JUSTIFICACION	No se tiene control sobre las acciones de cuentas privilegiadas, por lo cual no se puede realizar la trazabilidad o rastreo sobre los eventos reportados frente a un incidente de seguridad informática.
OBJETIVO DEL PROYECTO	Asegurar y monitorear las acciones de las cuentas privilegiadas en las plataformas tecnológicas críticas la UAECOB
ALCANCE	Las actividades mínimas para desarrollar son: 1) Monitorear la gestión de usuarios privilegiados de las plataformas tecnológicas (Key Power Management) 2) Implementar el uso de las herramientas para gestionar usuarios privilegiados en plataformas On Premise o nube o herramientas propias de los proveedores Software as a Service
TIEMPO	24 meses

PROYECTO	P8. Licenciamiento Microsoft Office 365 durante 2 años. Se abarca en este proyecto necesidades de aseguramiento como: 1)Microsoft Defender para Office 365: Protección contra amenazas avanzadas como phishing, malware, ransomware y ataques de spoofing. 2) Azure Active Directory Premium: Gestión avanzada de identidades y accesos, que incluye funciones como autenticación multifactor (MFA), inicio de sesión único (SSO). 3) Protección de datos: Herramientas avanzadas de prevención de pérdida de datos (DLP), cifrado de correo electrónico, y administración de derechos de información (IRM). 4) Microsoft Information Protection: Soluciones para clasificar, etiquetar y proteger datos sensibles dentro de la organización. 5) Windows Virtual Desktop: Virtualización completa de escritorios y aplicaciones, permitiendo que los empleados trabajen de manera remota de forma segura. Y 6) Enterprise Mobility + Security (EMS): Ofrece capacidades avanzadas de administración y seguridad de dispositivos móviles (MDM) y administración de aplicaciones móviles (MAM).
JUSTIFICACION	Adquirir licenciamiento microsoft con los máximos esquemas de seguridad para cargos críticos que manejen información sensible de la UAECOB.
OBJETIVO DEL PROYECTO	Establecer soluciones robustas de aseguramiento en la plataforma Microsoft.

ALCANCE	Las actividades mínimas para realizar son: Implementar: 1)Microsoft Defender para Office 365: Protección contra amenazas avanzadas como phishing, malware, ransomware y ataques de spoofing. 2) Azure Active Directory Premium: Gestión avanzada de identidades y accesos, que incluye funciones como autenticación multifactor (MFA), inicio de sesión único (SSO). 3) Protección de datos: Herramientas avanzadas de prevención de pérdida de datos (DLP), cifrado de correo electrónico, y administración de derechos de información (IRM). 4) Microsoft Information Protection: Soluciones para clasificar, etiquetar y proteger datos sensibles dentro de la organización. 5) Windows Virtual Desktop: Virtualización completa de escritorios y aplicaciones, permitiendo que los empleados trabajen de manera remota de forma segura. Y 6) Enterprise Mobility + Security (EMS): Ofrece capacidades avanzadas de administración y seguridad de dispositivos móviles (MDM) y administración de aplicaciones móviles (MAM).
TIEMPO	24 meses

HOJA DE RUTA

PROYECTO No.	PROD/SERV	TITULO DEL PROYECTO	OBJETIVO	RECURSOS
1	SERVICIO	P1. Fortalecimiento del MSPI (Modelo de Seguridad y Privacidad de la Información) Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Continuidad de Negocio	Tomar las acciones correspondientes con respecto a marcos individuales y hacer las inversiones de servicios profesionales y consultorías de mejores prácticas para cerrar la brecha de una manera progresiva en el marco de la seguridad de la información y ciberseguridad.	Presupuesto Equipo de trabajo de la UAECOB (Responsable de Seguridad de la Información, Líderes de proceso) Equipo de Consultoría SGSI-SGCS-SGCN
2	PRODUCTO	P2. Fortalecimiento del sistema de seguridad adaptativa.	Automatizar y mejorar la postura de seguridad con herramientas y soluciones de protección de amenazas emergentes a nivel de servidores y a nivel de estaciones de trabajo.	Presupuesto Equipo de trabajo la UAECOB (administradores de sistemas de información, líderes funcionales, Administradores de infraestructura (proveedor)) Expertos en Consultoría de cada solución
3	SERVICIO	P3.Mantener un DRP (Plan de Recuperación de Desastres Tecnológico) para asegurar que la UAECOB pueda gestionar de manera efectiva las crisis y desastres, protegiendo sus operaciones, activos y reputación mientras mantiene la continuidad del negocio.	Asegurar que la UAECOB pueda continuar operando y recuperar sus operaciones normales de manera rápida y eficiente después de un incidente crítico o desastre.	Presupuesto Equipo de trabajo la UAECOB (Responsables de Riesgos de la Entidad, Líderes Funcionales, Oficial de Seguridad de la Información, Equipo de TI)
4	PRODUCTO	P4. Implementación de herramientas de análisis de comportamiento en el uso de las redes y el comportamiento de los usuarios en el acceso a los servicios de tecnología	Bloquear comportamientos anómalos en la red y en los sistemas la UAECOB	Presupuesto Equipo de trabajo la UAECOB (Equipo de TI, Administradores de Infraestructura (Proveedor), Expertos en Consultoría de la solución
5	PROD/SERV	P5. Implementación de herramientas y procedimientos para desarrollo seguro	Asegurar los sistemas de información de la UAECOB publicados en la WEB (intranet e internet) están utilizando metodologías de desarrollo seguro.	Presupuesto Equipo de trabajo de TI. Equipo de Desarrollo de la UAECOB
6	PRODUCTO	P6. Implementación de solución automatizada para la hardenización o endurecimiento de infraestructura tecnológica.	Asegurar la plataforma tecnológica con el fin de encontrar fallas en el sistema para priorizar los ajustes y parcheo de vulnerabilidades.	Presupuesto Equipo de trabajo de TI, Administradores de Infraestructura (Proveedor)
7	PROD/SERV	P7. Implementar Gestión de Identidad y Accesos (IAM) para proteger los activos de información, mejorar la gestión de identidades y accesos e Implementación de solución para aseguramiento y gestión de cuentas privilegiadas . Esta solución debe integrarse como parte del IAM y permitir Single Sign On para autenticación única en los diferentes aplicativos.	Asegurar y monitorear las acciones de las cuentas privilegiadas en las plataformas tecnológicas críticas la UAECOB	Presupuesto Equipo de trabajo la UAECOB: (Desarrolladores, administradores de sistemas de información, líderes funcionales, Administradores de infraestructura (proveedor))
8	PROD/SERV	P8. Licenciamiento Microsoft Office 365 durante 3 años. Se abarca en este proyecto necesidades de aseguramiento como: 1)Microsoft Defender para Office 365: Protección contra amenazas avanzadas como phishing, malware, ransomware y ataques de spoofing. 2) Azure Active Directory Premium: Gestión avanzada de identidades y accesos, que incluye funciones como autenticación multifactor (MFA), inicio de sesión único (SSO). 3) Protección de datos: Herramientas avanzadas de prevención de pérdida de datos (DLP), cifrado de correo electrónico, y administración de derechos de información (IRM). 4) Microsoft Information Protection: Soluciones para clasificar, etiquetar y proteger datos sensibles dentro de la organización. 5) Windows Virtual Desktop: Virtualización completa de escritorios y aplicaciones, permitiendo que los empleados trabajen de manera remota de forma segura. Y 6) Enterprise Mobility + Security (EMS): Ofrece capacidades avanzadas de administración y seguridad de dispositivos móviles (MDM) y administración de aplicaciones móviles (MAM).	Establecer soluciones robustas de aseguramiento en la plataforma Microsoft.	Presupuesto Equipo de trabajo de TI, Administradores de Infraestructura (Proveedor)

CRONOGRAMA

PROYECTO No.	PROD/SERV	TITULO DEL PROYECTO	2026				2027			
			IQ	IIQ	IIIQ	IVQ	IQ	IIQ	IIIQ	IVQ
1	SERVICIO	P1. Fortalecimiento del MSPI (Modelo de Seguridad y Privacidad de la Información) Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Continuidad de Negocio								
2	PRODUCTO	P2. Fortalecimiento del sistema de seguridad adaptativa.								
3	SERVICIO	P3.Mantener un DRP (Plan de Recuperación de Desastres Tecnológico) para asegurar que la UAECOB pueda gestionar de manera efectiva las crisis y desastres, protegiendo sus operaciones, activos y reputación mientras mantiene la continuidad del negocio.								
4	PRODUCTO	P4. Implementación de herramientas de análisis de comportamiento en el uso de las redes y el comportamiento de los usuarios en el acceso a los servicios de tecnología								
5	PROD/SERV	P5. Implementación de herramientas y procedimientos para desarrollo seguro								
6	PRODUCTO	P6. Implementación de solución automatizada para la hardenización o endurecimiento de infraestructura tecnológica.								
7	PROD/SERV	P7. Implementar Gestión de Identidad y Accesos (IAM) para proteger los activos de información, mejorar la gestión de identidades y accesos e Implementación de solución para aseguramiento y gestión de cuentas privilegiadas . Esta solución debe integrarse como parte del IAM y permitir Single Sign On para autenticación única en los diferentes aplicativos.								
8	PROD/SERV	P8. Licenciamiento Microsoft Office 365 durante 3 años. Se abarca en este proyecto necesidades de aseguramiento como: 1)Microsoft Defender para Office 365: Protección contra amenazas avanzadas como phishing, malware, ransomware y ataques de spoofing. 2) Azure Active Directory Premium: Gestión avanzada de identidades y accesos, que incluye funciones como autenticación multifactor (MFA), inicio de sesión único (SSO). 3) Protección de datos: Herramientas avanzadas de prevención de pérdida de datos (DLP), cifrado de correo electrónico, y administración de derechos de información (IRM). 4) Microsoft Information Protection: Soluciones para clasificar, etiquetar y proteger datos sensibles dentro de la organización. 5) Windows Virtual Desktop: Virtualización completa de escritorios y aplicaciones, permitiendo que los empleados trabajen de manera remota de forma segura. Y 6) Enterprise Mobility + Security (EMS): Ofrece capacidades avanzadas de administración y seguridad de dispositivos móviles (MDM) y administración de aplicaciones móviles (MAM).								

NOTA PROYECTO DE INVERSIÓN:

Estos proyectos se realizarán con el proyecto de inversión 8126 “Fortalecimiento Institucional de la UAECOB para un gobierno confiable Bogotá D.C.”.

RIESGOS EN LA EJECUCIÓN DEL PLAN

Estos riesgos están enunciados en el mapa institucional de riesgos, dentro de estos tenemos:

- ✓ No asignación o recorte presupuestal para seguridad digital. contar con las competencias necesarias por partes del recurso humano para la seguridad digital.
- ✓ No lograr niveles de madurez apropiadas en la gestión de la seguridad de la información por alta rotación del personal de Tecnología.
- ✓ Modificación de la información para beneficio propio por dadivas ofrecidas a funcionarios o contratistas de la entidad.

CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la Modificación
1	29/01/2026	Versión del Plan de Seguridad y Privacidad de la información 2025 para ser aprobado al comité Institucional del 2025 para el 2026.
2	29/01/2026	Actualización del Plan de Seguridad y Privacidad de la Información 2025, Se actualiza documento basándose en proyectos ya realizados y que se deben mantener, así como evolución en temas de Seguridad de la Información de acuerdo a nueva herramienta de MINTIC que se actualizo de la versión ISO 27001:2013 a la ISO 27001:2022.

CONTROL DE FIRMAS

Elaboró	Revisó	Aprobó
Original Firmado **José Hernán Morales Muñoz** Contratista – Dirección -TIC	Original Firmado **Cristian Leonardo Cala Torres** Profesional Especializado Dirección -TIC Original Firmado **Darío Alexander Méndez Beltrán** Contratista – Dirección -TIC Original Firmado **María Claudia Gonzalez** Profesional Contratista OAP	29/01/2026 **Comité Institucional de Gestión y Desempeño**