Especificaciones esenciales:

- **Componente 1: Fortalecimiento en la Operación.**

  - Revisión Centro de Operaciones de Seguridad SOC
    - Revisión del SOC para dar cumplimiento a lo dispuesto en el artículo 17 de la resolución 0500 de 2021 capacidades y servicios de SOC institucionales
      - Propuesta de estructura, proceso, procedimiento, formatos, manuales, perfiles, recomendación de herramientas.
      - Propuesta de especificaciones técnicas para la tercerización del servicio de acuerdo con la oferta disponible en el mercado actual.
    - Fortalecimiento de seguridad FIRST
      - Plan de acción.
  - Revisión de solución SIEM
    - Evaluación de fuentes y Eventos de Seguridad
      - Revisión de documentación asociada a políticas, procedimientos, manuales, instructivos o prácticas asociadas a gestión de usuarios, gestión de logs, gestión de eventos, gestión de accesos, gestión de la actualización de las plataformas tecnológicas.
      - Generación de Catálogo descriptivo para el fortalecimiento de actividades de detección y caracterización de eventos de seguridad.
  - Ciberinteligencia y apoyo.
    - Implementación de SIEM.
      - Suministro de la solución Splunk Enterprise Security suscripción por 2 años, capacidad de ingesta 50GB/d con almacenamiento en la nube 3 meses. Enterprise Support. (1 contact)
      - Implementación de cinco (5) conectores.
      - Documento de configuración e implementación
      - Documento de operación.
      - Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual.
    - Integración Splunk con MISP
      - Documento de configuración e implementación MISP.
      - Documento de operación.
      - Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual.
    - Parametrizaciones Splunk
      - Configuración de 5 alertas base y creación de 1 acción para la notificación de incidentes.
      - Configuración de 5 Dashboards & reports
      - Documento de configuración
      - Documento de operación.
      - Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual.
    - Recomendaciones de seguridad basadas en hallazgos encontrados durante el servicio.

- **Componente 2: Gestión continua de Vulnerabilidades (ver detalle en el numeral**

  - Revisión del proceso de gestión de vulnerabilidades de la entidad.
    - Revisión de Procesos, procedimientos, formatos, instructivos, documentos que soportan el proceso de gestión de vulnerabilidades.
    - Revisión de capacidades asociadas al proceso. (Personas, herramientas)
    - Revisión de la estructura actual para la gestión continua de vulnerabilidades.

  - Pruebas de Seguridad:
    - Pruebas de vulnerabilidad para cien (100) direcciones internas.
    - Informe ejecutivo, informe técnico.

  - Suministro de licenciamiento SaaS:
    - Suministro de una suscripción de Tenable por 24 meses. a continuación, se detalle los componentes a entregar:
      - Tenable.sc Security Center Suscripción, IP Bands: 1650
      - Tenable.io Web Application Scanning, Web Apps: 30
      - Transferencia de conocimiento
        - Documento de configuración
        - Documento de operación.
        - Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual
    - Capacitación: Pruebas de seguridad en plataformas críticas.
      - Grupo máximo: diez (10) funcionarios
      - Diez (10) horas
      - Modalidad: Virtual.

- **Componente 3: Solución de Gestión de Accesos Privilegiados-PAM**

  - Suministro de la solución de Gestión de Accesos Privilegiados-PAM CyberArk para la Entidad. Para 30 usuarios privilegiados. a continuación, se detalle los componentes a entregar:
    - Credential Protection, Session Isolation, Recording, Detection,Remote Access, and Strong Authentication. Price per user permonth Cantidad: 30
  - Para implementar la solución PAM en la Entidad con sus módulos base, se ofrecen los servicios profesionales de diseño, implementación, configuración de la solución con el siguiente alcance:
    - Integración con el dominio
    - Parametrización de los módulos PSM, CPM y PVWA
    - Configuración de 16 accesos a servidores
    - Transferencia de conocimiento
    - Documento de configuración
    - Documento de operación.
    - Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual
    - Capacitación: Privileged Access Management
    - Grupo máximo: diez (10) funcionarios
    - Diez (10) horas

- Modalidad: Virtual.
- Suscripción por 24 meses

- **<u>Componente 4: Solución de seguridad para bases de datos Database Activity Monitoring (DAM) (ver detalle en el numeral 3.2.2.4)</u>**

  - Suministro de la solución Database Activity Monitoring (DAM) por 24 meses Imperva-DAM para la Entidad, a continuación, se detalle los componentes a entregar:

- Imperva *SF-SUB-DBF-X452-GWCL-GWCL-TBL *Suscripción de software X4520 para Firewall de base de datos (cantidad 3).
- Imperva *SS-REPUESTO-X452-H1 *X4520 Gateway Appliance (cantidad 3)
- Imperva *SS-REPUESTO-X452-SL3 *X4520, repuesto in situ para Gateway Appliance. (cantidad 3)
- Imperva -*SF-SUB-M17-TBL *Suscripción de software M170 para el software Management Server, suscripción mejorada. (cantidad 1)
- Imperva -*SS-REPUESTO-M17-H1 *Servidor de gestión M170, Appliance. (cantidad 1)
- Imperva - *SS-REPUESTO-M17-SL3 *M170 Management Server, repuesto in situ para Appliance. (cantidad 1)
- Imperva - SKU: *U-DBURM-SUB-100-R-TBL *Actualización: licencia de administración de derechos de usuario para 100DBis, suscripción mejorada. (cantidad 1)

  - Implementación de Imperva-DAM en la Entidad con sus módulos base. Para un máximo de 10 bases de datos
    Transferencia de conocimiento.
    - Transferencia de conocimiento
      - Documento de configuración
      - Documento de operación.
      - Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual
    - Capacitación: Seguridad en base de datos y aplicaciones.
      - Grupo máximo: Diez (10) funcionarios
      - Diez (10) horas
      - Modalidad: Virtual.

- **<u>Componente 5: Solución de Control de Acceso a la red (Next Generation NAC) (ver detalle en el numeral 3.2.2.5)</u>**

  - Suministro de la solución CISCO ISE por 24 meses así:
    - Cisco ISE Virtual Machine Common PID Cantidad 3.
    - SOLN SUPP SWSS Cisco ISE Virtual Machine Common PID Cantidad 3.
    - Cisco Identity Service Engine Essentials Subscription Cantidad: 5100
    - Cisco Identity Service Engine Premier Subscription Cantidad: 7400

- Cisco ISE Device Admin Node License Cantidad: 3
- Cisco AnyConnect Apex License, Users: Cantidad: 400

- Implementación de CISCO-ISE en la Entidad con sus módulos base. Para un máximo de 50 dispositivos.
  - Transferencia de conocimiento
    - Documento de configuración
    - Documento de operación.
    - Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual
  - Capacitación: 10 horas- Seguridad en redes bajo la filosofía Zero Trust. Control de Acceso a la red.
    - Grupo máximo: 10 personas
    - Modalidad: Virtual.

Las fases propuestas son:

- **FASE I** - Inicio del Proyecto - Entendimiento Situación – Construcción Plan Gestión Proyecto
- **FASE II** - Revisión y Fortalecimiento de seguridad Informatica.

- **FASE III –** Cierre del proyecto

Horario de los servicios

La de ejecución de los servicios será en horario laboral, de lunes a viernes, 8 horas diarias y se establecerá un punto de contacto entre **ESU** y el **SECRETARIA DE INNOVACION DIGITAL DE MEDELLIN** con el fin de hacer un seguimiento a las actividades. De esta forma se podrá tener una visibilidad completa de lo que está ocurriendo en el proyecto vía telefónica o por medio de correo y tendrán la posibilidad de direccionar su ejecución. En caso de requerir la ejecución de actividades fuera de este horario, **ESU** y la **SECRETARIA DE INNOVACION DIGITAL DE MEDELLIN** coordinarán las actividades a ejecutar en ventanas programadas y mediante procedimientos de control de cambios del proyecto.

1 FASES DEL PROYECTO

FASE I - Inicio del Proyecto - Entendimiento Situación – Construcción Plan Gestión Proyecto

En esta etapa se define con exactitud el alcance del proyecto, se ajusta el cronograma de trabajo y responsables; de manera adicional, se define y firma del plan de calidad del proyecto que se convierte su carta de navegación.

Para cumplir con el objetivo de esta etapa, se recopila toda la información necesaria para la ejecución del proyecto. Esta información es, entre otra, la siguiente:

- Pliegos, ofertas y demás documentos de definición y formalización del proyecto
- Requerimientos y necesidades iniciales, vs. implementación actual
- Metodologías utilizadas
- Nivel de apoyo de la alta dirección
- Cultura de la Organización
- Metodología existente para gestión de activos de información
- Metodología existente para gestión de riesgos
- Responsables y demás involucrados (Stakeholders)
- Terceros involucrados
- Contratos
- Clientes de la solución
- Requerimientos normativos, legales que aplican al objeto del Proyecto
- Identificación y formalización de expectativas del cliente.

Entregables

- ✓ Alcance y Objetivos del Proyecto (Según contrato y lo acordado con las partes)
- ✓ Acuerdo de criterios de aceptación y niveles de servicio acordados
- ✓ Plan de Gestión del Proyecto y entregables asociados (PMI) como:
    - Plan de Riesgos del Proyecto
    - Plan de Calidad del Proyecto
    - Plan de Comunicaciones del Proyecto
- ✓ Cronograma detallado de actividades actualizado del proyecto y línea base de definitivos.

FASE II – Revisión y Fortalecimiento de seguridad Informática.

Descripción del servicio

En esta fase se evaluará el estado de seguridad informática de la **SECRETARIA DE INNOVACION DIGITAL DE MEDELLIN** siguiendo las buenas prácticas de seguridad y estándar de la industria. Se desarrollarán cada uno de los componentes definidos en el alcance.

Para cumplir con este objetivo, se utilizará la siguiente estructura de referencia:

- Contexto de la Organización
- Gestión de incidentes de seguridad de la información.
- Controles de seguridad informática base.
- Mejora Continua

Entregables

- ✓ Requisitos de técnicos para la ejecución del servicio.
- ✓ Cronograma detallado de actividades del proyecto por componente conforme al alcance.

Características de la prestación del servicio:

A continuación, se detalla el detalle de cada uno de los componentes del servicio.

Fortalecimiento de la Operación (Componente 1)

A través de entrevistas y revisión de la documentación existente se identificarán las necesidades de la Entidad, en detalle se ejecutarán las siguientes actividades:

- Revisión de la documentación existente.
- Entrevistas con personal de la Entidad responsable de los procesos y controles de seguridad informática asociados.
- Diagnóstico y analisis del proceso.

Criterios de valor para identificar las actividades relevantes:

- Tamaño de la entidad, estructura organizacional de seguridad de la información y de seguridad informática, referencias a estándares de seguridad para la gestión de incidentes y cumplimiento legal.

Específicamente se desarrollará:

A. Revisión Centro de Operaciones de Seguridad SOC

- Revisión de estructura actual del proceso
- Revisión del SOC para dar cumplimiento a lo dispuesto en el artículo 17 de la resolución 0500 de 2021 capacidades y servicios de SOC institucionales
- Propuesta de especificaciones técnicas para la tercerización del servicio de acuerdo con la oferta disponible en el mercado actual.
- Fortalecimiento de seguridad FIRST

Entregables:

- Documento de Informe de madurez de la operación SOC bajo el framework de SOC-GAP
- Documento de estructura del proceso, procedimiento, formatos, manuales, especificación de capacidades requeridas para soportar la operación del SOC (perfiles), recomendación de herramientas.
- Documento de propuesta de especificaciones técnicas para la tercerización del servicio de acuerdo con la oferta disponible en el mercado actual.
- Documento de actividades requeridas y recomendaciones para postular equipo de respuesta de incidentes ante el FIRST

B. Revisión de solución SIEM

- Evaluación de fuentes y Eventos de Seguridad
  - Revisión de documentación asociada a políticas, procedimientos, manuales, instructivos o prácticas asociadas a:
    - ✓ Gestión de usuarios
    - ✓ Gestión de logs
    - ✓ Gestión de eventos,
    - ✓ Gestión de accesos,

- ✓ Gestión de la actualización de las plataformas tecnológicas

Entregables:

- Documento Catálogo descriptivo para el fortalecimiento de actividades de detección y caracterización de eventos de seguridad que contiene:
  - Dispositivos críticos conforme al contexto de Arquitectura tecnológica de la entidad.
  - Recomendación de eventos de seguridad a monitorear por tecnología conforme al contexto tecnológico de la entidad.
- Recomendaciones de reglas de filtrado y detección de eventos de seguridad que se deben de configurar en el SIEM.

C. Ciberinteligencia y apoyo.

- Implementación de SIEM.
  - Splunk Enterprise Security suscripción por 2 años, capacidad de ingesta 50GB/d con almacenamiento en la nube 3 meses. Enterprise Support. (1 contact)
    - Implementación de cinco (5) conectores
    - Documento de configuración e implementación
    - Documento de operación.
    - Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual
- Integración Splunk con MISP
  - Documento de configuración e implementación.
  - Documento de operación.
  - Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual
- Parametrizaciones Splunk
  - Configuración de 5 alertas base y creación de 1 acción para la notificación de incidentes.
  - Configuración de 5 Dashboards & Reports
  - Documento de configuración
  - Documento de operación.
  - Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual.

Entregables:

- Documento de implementación de herramienta y Arquitectura:
  - Splunk Enterprise Security (Habilitación de Servicio nube)
  - Integración MISP
  - Parametrización Splunk.
- Documento de configuración e implementación de:
  - Splunk y cinco (5) conectores
  - Integración MISP
  - Parametrización Splunk
- Documento de operación.
  - Splunk Enterprise Security
  - MISP

- Acta de Capacitación para diez (10) funcionarios
  - 4 horas en administración por cada solución para un total de doce (12) horas:
    - Enterprise Security
    - MISP
    - Parametrización Splunk

*****Se entregará acta de asistencia, diapositivas y evaluación de la capacitación.

Nota: LA SECRETARÍA DE INNOVACIÓN DIGITAL proporcionará los recursos de Hardware y software base necesarios para la implementación de las soluciones ofertadas en el presente componente. En la primera fase del proyecto se entregará el documento de requerimientos técnicos requeridos por cada solución: Características de hardware, S.0, permisos, puertos, protocolos, etc.

Gestión continua de Vulnerabilidades (Componente 2)

A través de entrevistas y revisión de la documentación existente se identificarán las necesidades de la Entidad, en detalle se ejecutarán las siguientes actividades:

- Revisión de la documentación existente.
- Entrevistas con personal de la Entidad responsable de los procesos y controles de seguridad informática asociados.
- Diagnóstico y analisis del proceso.

Criterios de valor para identificar las actividades relevantes:

Tamaño de la entidad, estructura organizacional de seguridad de la información y de seguridad informática, referencias a estándares de seguridad para la gestión de incidentes y cumplimiento legal.

Específicamente se desarrollará:

- **<u>Revisión de Proceso de Gestión de Vulnerabilidades.</u>**

Análisis, diseño, capacitación e implementación del proceso operativo de Gestión de Vulnerabilidades para la Entidad.

La revisión, diseño y ajustes (optimización) del proceso de Gestión de Vulnerabilidades iniciará con talleres de trabajo y/o entrevistas donde se recolectará toda la información asociada con los procesos, procedimientos, puntos de control, herramientas, responsables y documentación asociada con la gestión actual de la Entidad frente a las vulnerabilidades, de manera que sea posible identificar la situación actual (GAP) frente aspectos operativos de seguridad, requisitos normativos y negocio.

A continuación, se detallan las actividades que se van a realizar para este componente:

- Realización de talleres de trabajo que incluyen entrevistas y evaluación del estado actual (Actividades, Personas, Políticas y Herramientas) de la Gestión de Vulnerabilidades.

  El propósito fundamental es conocer detalladamente cómo funciona la operación de la Entidad, los roles y participantes, la interacción con las áreas usuarias y la articulación actual de estos elementos en todo el proceso.

- Se procederá a evaluar lo encontrado para incluir mejoras operativas respecto al cumplimiento de normas, buenas prácticas, estándares internacionales, y políticas-normas-estándares propios que apliquen a la operación de la Entidad.

- Diseño y definición del proceso de Gestión de Vulnerabilidades parar la Entidad, donde se incluye descripción del proceso, KPIs, Tableros de Control, Roles y Responsabilidades

- Realización de talleres de trabajo que incluyen entrevistas y descripción de la situación propuesta donde se detalle lo siguiente:

  - Actividades del nuevo proceso
  - Roles, responsabilidades y aptitudes
  - Niveles de seguridad
  - Riesgos
  - Modelos de Amenazas
  - Cronogramas esperados de solución

  Entregables

  - Informe de situación actual (Gap inicial) del proceso de Gestión de Vulnerabilidades
  - Plan de Mejora del Proceso de Gestión de Vulnerabilidades
  - Acta de entrega del Proceso de Gestión de Vulnerabilidades
  - Acta de divulgación y socialización del Proceso de Gestión de Vulnerabilidades

- **Pruebas de Seguridad:**

  - Identificación de IPs objeto de la auditoría.
    - Pruebas de vulnerabilidad para cien (100) direcciones internas.

  Entregables:

  - Plan de pruebas de seguridad
  - Resumen Ejecutivo donde se centralizan los resultados de las pruebas de seguridad realizadas
  - Informe técnico con el detalle de las pruebas detallando las vulnerabilidades y los resultados obtenidos, recomendaciones de mitigación.
  - Acta de socialización de resultados.

- **Suministro de licenciamiento:**

- Licenciamiento durante 24 meses de:
  - Tenable.sc Security Center Suscripción, IP Bands: 1650
  - Tenable.io Web Application Scanning , Web Apps: 30
  - Transferencia de conocimiento
    - Documento de configuración
    - Documento de operación.
    - Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual
- Capacitación: Pruebas de seguridad en plataformas críticas.
  - Grupo máximo: diez (10) funcionarios
  - Diez (10) horas
  - Modalidad: Virtual.

Entregables:

- Acta de implementación de herramienta (Habilitación de Servicio nube) y Arquitectura:
  - **Tenable.sc y Tenable.io**
- Documento de configuración de:
  - **Tenable.sc y Tenable.io**
- Documento de operación.
  - **Tenable.sc y Tenable.io**
- Acta de Capacitación de **Tenable.sc y Tenable.io** para diez (10) funcionarios, cuatro (4) horas por cada solución para un total de ocho (8) horas. Modalidad Virtual.
- Acta de Capacitación Pruebas de seguridad en plataformas críticas para diez (10) funcionarios, diez (10) horas. Modalidad Virtual.

Solución de Gestión de Accesos Privilegiados PAM (Componente 3)

A través de entrevistas y revisión de la documentación existente se identificarán las necesidades de la Entidad, en detalle se ejecutarán las siguientes actividades:

- Entendimiento de requisitos de la entidad frente a Gestión de Accesos Privilegiados.
  - Entrevistas con personal de la entidad responsable de los procesos y controles de seguridad informática asociados.
- Entendimiento de los activos y Sistemas más Críticos.
- Estrategia de despliegue de la solución de Gestión de Accesos Privilegiados PAM.

Específicamente se desarrollará:

- **Suministro de la solución de Gestión de Accesos Privilegiados-PAM CyberArk por 24 meses para la Entidad.**
  - Para 30 usuarios privilegiados por 24 meses. a continuación, se detalle los componentes a entregar:

- Credential Protection, Session Isolation, Recording, Detection, Remote Access, and Strong Authentication. Cantidad: 30

- Implementación de la solución PAM en la Entidad con sus módulos base, se ofrecen los servicios profesionales de diseño, implementación, configuración de la solución con el siguiente alcance:

  - Ejecución de CyberArk Discovery & Audit (CyberArk DNA®) para escanear los sistemas basados en Active Directory.
    - Revisión de informe.
    - Análisis de resultados.
    - Priorización de Cuentas privilegiadas a proteger.
  - Integración con el dominio
  - Parametrización de los módulos PSM, CPM y PVWA
  - Configuración de 16 accesos a servidores

    - Transferencia de conocimiento
      - Documento de configuración
      - Documento de operación.
      - Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual
    - Capacitación: Seguridad en base de datos y aplicaciones.
      - Grupo máximo: diez (10) funcionarios
      - Diez (10) horas
      - Modalidad: Virtual.
      - Suscripción por 24 meses

Entregables:

- Reporte de CyberArk Discovery & Audit
- Documento de implementación de herramienta CyberArk y Arquitectura:
  - CyberArk (PSM, CPM y PVWA)
- Documento de configuración:
  - CyberArk (PSM, CPM y PVWA)
- Documento de operación.
  - CyberArk (PSM, CPM y PVWA)
- Acta de Capacitación para diez (10) funcionarios, 4 horas en administración por cada solución. Modalidad Virtual. para un total de doce (12) horas:
  - PSM
  - CPM
  - PVWA
- Acta de Capacitación Privileged Access Management para diez (10) funcionarios, diez (10) horas. Modalidad Virtual.

*****Se entregará acta de asistencia, diapositivas y evaluación de la capacitación.

Nota: LA SECRETARÍA DE INNOVACIÓN DIGITAL proporcionará los recursos de Hardware y software base necesarios para la implementación de las soluciones ofertadas en el presente componente. En la primera fase del proyecto se entregará el documento de requerimientos técnicos requeridos por cada solución: Características de hardware, S.0, permisos, puertos, protocolos, etc.

Solución de seguridad para bases de datos Database Activity Monitoring (DAM) (Componente 4)

A través de entrevistas y revisión de la documentación existente se identificarán las necesidades de la Entidad, en detalle se ejecutarán las siguientes actividades:

- Entendimiento de requisitos de la entidad frente a la protección de bases de datos.
    - Entrevistas con personal de la entidad responsable de los procesos y controles de seguridad informática asociados.
- Entendimiento de las bases de datos más Críticas para la Entidad.
- Estrategia de despliegue de la solución de seguridad para bases de datos Database Activity Monitoring (DAM)

Específicamente se desarrollará:

- **<u>Suministro de la solución Database Activity Monitoring (DAM) por 24 meses Imperva-DAM para la Entidad, a continuación, se detalle los componentes a entregar:</u>**

    - Imperva - *SF-SUB-DBF-X452-GWCL-GWCL-TBL
      *Suscripción de software X4520 para Firewall de base de datos (cantidad 3).
    - Imperva - *SS-REPUESTO-X452-H1 *X4520 Gateway Appliance (cantidad 3)
    - Imperva - *SS-REPUESTO-X452-SL3 *X4520, repuesto in situ para Gateway Appliance. (cantidad 3)
    - Imperva - *SF-SUB-M17-TBL *Suscripción de software M170 para el software Management Server, suscripción mejorada. (cantidad 1)
    - Imperva - *SS-REPUESTO-M17-H1 *Servidor de gestión M170, Appliance. (cantidad 1)
    - Imperva - *SS-REPUESTO-M17-SL3 *M170 Management Server, repuesto in situ para Appliance. (cantidad 1)
    - Imperva - *U-DBURM-SUB-100-R-TBL *Actualización: licencia de administración de derechos de usuario para 100DBis, suscripción mejorada. (cantidad 1)

        - Implementación de Imperva-DAM en la Entidad con sus módulos base. Para un máximo de 10 bases de datos. Transferencia de conocimiento.
            - Transferencia de conocimiento
                - Documento de configuración
                - Documento de operación.
                - Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual

- Capacitación: Seguridad en base de datos y aplicaciones.
  - Grupo máximo: Diez (10) funcionarios
  - Diez (10) horas
  - Modalidad: Virtual.

Entregables:

- Documento de implementación de herramienta y Arquitectura:
  - Imperva Database Activity Monitoring (DAM)
- Documento de configuración:
  - Imperva Database Activity Monitoring (DAM)
- Documento de operación.
  - Imperva Database Activity Monitoring (DAM)
- Acta de Capacitación Administración de Imperva Database Activity Monitoring **(DAM)** para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual.
- Acta de Capacitación Seguridad en base de datos y aplicaciones para diez (10) funcionarios, diez (10) horas. Modalidad Virtual.

***Se entregará acta de asistencia, diapositivas y evaluación de la capacitación.

Nota: LA SECRETARÍA DE INNOVACIÓN DIGITAL proporcionará los recursos de Hardware y software base necesarios para la implementación de las soluciones ofertadas en el presente componente. En la primera fase del proyecto se entregará el documento de requerimientos técnicos requeridos por cada solución: Características de hardware, S.0, permisos, puertos, protocolos, etc.

Solución de Control de Acceso a la red (Next Generation NAC) (Componente 5)

FASE III – Cierre del Proyecto

Una vez finalizado el proyecto, se realizará una presentación con sus resultados. De manera adicional, se realiza una entrega formal de toda la documentación del proyecto que se encuentre dentro de su alcance.

Esta presentación va acompañada de la carta de aceptación de implementación de la solución y visto bueno de parte del cliente.

Entregables

- Medio Magnético con Documentación definitiva
- Presentación de cierre
- Acta de Finalización del Proyecto

EQUIPO DE TRABAJO

El equipo de trabajo propuesto para el desarrollo del proyecto es el siguiente:

2 REQUERIMIENTOS

Para cada una de las etapas de ejecución, **LA SECRETARÍA DE INNOVACIÓN DIGITAL** deberá garantizar los siguientes requerimientos de proyecto, humanos, documentales o logísticos.

Generales y Administrativos

- Acceso a las herramientas de conexión virtual que defina **LA SECRETARÍA DE INNOVACIÓN DIGITAL** para los consultores que ejecutarán el servicio**.** (Teams, Log mein, TeamViewer, etc)
- Suministro de plataforma virtual y capacidades tecnológicas para la instalación de las herramientas establecidas en la presente propuesta. (donde aplique)
- Conectividad directa a la Plataforma donde se va a realizar el aprovisionamiento de los componentes técnicos del servicio. (VPNs)
- Un líder de proyecto que se encargue de cualquier requerimiento técnico o logístico que surja a partir de la ejecución de las tareas especificadas.
- Acompañamiento por parte de un funcionario de **LA SECRETARÍA DE INNOVACIÓN DIGITAL** en el proyecto para la gestión de las solicitudes que requiera el equipo de consultores que ejecutará el servicio**.**

En la ejecución del Proyecto

- No modificación de los compromisos, fechas y plan de trabajo.
- Entrega oportuna de la información requerida para el desarrollo de cada una de las fases del proyecto
- Revisión y aprobación oportuna de los componentes, de acuerdo con el plan de trabajo definido.

Lugar de Desarrollo de los Trabajos

Teniendo en cuenta la situación actual relacionada con el COVID-19 y con el propósito de tomar todas las medidas de bioseguridad necesarias para proteger a nuestros clientes y

nuestros colaboradores, las actividades se ejecutarán de manera remota**.** Igualmente, se programara sesiones en sitio cuando se estime pertinente.

3 MODELO METODOLÓGICO PROPUESTO

Para todo el servicio, ***adicional a las metodologías y estrategias definidas específicamente para la ejecución del proyecto***, detalladas en la descripción de los servicios ofrecidos; el marco metodológico está basado en cuatro etapas estructuradas con el modelo de madurez internacional propuesto por PMI. Estas cuatro etapas permiten de una manera simple y coordinada llevar a cabo la gestión del proyecto.

Inicio – Planeación

Durante esta etapa se determinan todos los aspectos necesarios para afinar el requerimiento y entender las expectativas del cliente. Esta etapa va desde la presentación de la oferta hasta el perfeccionamiento del contrato, siendo este último el documento de "kick-off" del proyecto, produciendo un documento inicial que detalla, de manera coordinada con el cliente, los objetivos, alcances y metas que persigue el proyecto, así como los recursos que estarán involucrados, su disponibilidad de participación y el tiempo de duración.

NOTA: Es imprescindible para la realización del proyecto que la dirección haya informado a todos los responsables involucrados en el proyecto y dichos responsables acepten su participación en el mismo. Este acuerdo busca evitar situaciones de no disponibilidad del personal.

Los documentos asociados a esta etapa son:

- Contrato
- Informe de Definición del Proyecto.

Construcción Plan Gestión Proyecto

En esta etapa se define con exactitud el alcance del proyecto, se ajusta el cronograma de trabajo y responsables como también la definición y firma del plan de calidad del proyecto que se convierte en la carta de navegación de este.

Adicionalmente, se realiza la recopilación de toda la información necesaria para la ejecución del proyecto. Entre otras se buscará la recopilación de:

- Pliegos, ofertas y demás documentos de definición y formalización del proyecto
- Requerimientos y necesidades iniciales, vs implementación actual
- Metodologías utilizadas
- Nivel de apoyo de la alta dirección
- Cultura de la Organización
- Metodología existente para gestión de activos de TI
- Responsables y demás involucrados (Stakeholders)
- Terceros involucrados

- Contratos
- Clientes de la solución
- Requerimientos normativos, legales que aplican al objeto del Proyecto
- Identificación y formalización de expectativas del cliente.

Entregables

- ✓ Alcance y Objetivos del Proyecto (Según contrato y lo acordado con las partes)
- ✓ Acuerdo de criterios de aceptación y niveles de servicio acordados
- ✓ Plan de Gestión del Proyecto y entregables asociados (PMI) como:
    - Plan de Riesgos del Proyecto
    - Plan de Calidad del Proyecto
    - Plan de Comunicaciones del Proyecto
- ✓ Cronograma detallado de actividades actualizado del proyecto y línea base de definitivos.

Ejecución, Control y Monitoreo

Durante esta etapa, se tomarán los objetivos, alcances y metas definidos en la etapa de iniciación (expresados en el informe de Definición del Proyecto y se desarrolla un plan de proyecto que contempla los siguientes aspectos:

- Cronograma de Proyecto (Diagrama de Gantt) identificando etapas, tareas e hitos (objetivos medibles de cumplimiento).
- Requerimientos de Calidad del Proyecto por cada hito, concertando con El Cliente la manera como se aceptarán los Entregables relacionados y estableciendo la métrica de calidad de los mismos.
- Identificación de Riesgos de Proyecto, presentando todos los riesgos visualizados y un plan para mitigarlos

Con estos tres ítems se crea el documento de Plan de Trabajo, el cual será de referencia para las partes en materia de cumplimiento y control de ejecución del proyecto.

Adicionalmente, se define de manera conjunta el seguimiento a las actividades, en materia de periodicidad de reuniones de control y evaluación. Los avances quedarán documentados en forma de actas que serán tenidas en cuenta como informes de avance entre las partes. Particularmente, en esta etapa deberá llevarse a cabo una reunión de inicio en donde se haga la entrega formal del plan de trabajo y se definan aspectos adicionales, y posteriormente, de acuerdo con la periodicidad acordada, se harán reuniones de seguimiento para mantener el control y observar los avances; todo con su correspondiente documentación en forma de actas.
Los documentos especificados en esta etapa serán:

- Plan de Trabajo
- Acta de Inicio
- Actas de seguimiento

Cierre de Proyecto

Como última etapa, el cierre de proyecto se centrará en la elaboración de un acta final en donde quede constancia de ciertos aspectos clave del desarrollo del proyecto, así como la formalidad de aceptación del mismo por parte del cliente incluyendo al menos los siguientes ítems:

- Nombre del Proyecto
- Texto de cierre y recibido a satisfacción por parte del cliente
- Comentarios adicionales al cierre del proyecto

Adicional al acta de cierre, se realizará una reunión final con el objetivo de establecer la experiencia del cliente durante el proyecto e identificar aquellas situaciones susceptibles de mejora y en general lecciones aprendidas del proyecto que sean aplicables para todos en el futuro. Esto quedará consignado en un documento que será llamado “Lecciones Aprendidas”

Los documentos especificados en esta etapa serán:

- Acta de Cierre del Proyecto
- Documento de Lecciones Aprendidas.

4 ÍTEMS FUERA DEL ALCANCE

La presente propuesta contempla exclusivamente los servicios especificados en el texto del documento. Se encuentra fuera del alcance particularmente:

- Implementación de controles no definidos en la propuesta
- Implementación de recomendaciones
- Migración de plataforma tecnológica
- Modificación de las configuraciones
- Modificación de códigos fuente, arquitectura o en general cualquier modificación relacionada directamente con la ejecución de los servicios.
- Adquisición, configuración o puesta en operación de cualquier elemento de hardware y/o software que surja como requerimiento de seguridad.
- Suministro de los recursos de Hardware y software base necesarios para la implementación de las soluciones ofertadas en la presente propuesta.
- Cualquier otro servicio que no se encuentre explícito en la presente propuesta

5 DURACIÓN DEL PROYECTO

Para la ejecución de los servicios contemplados en la presente propuesta, se ha definido como plazo de ejecución cinco (5) meses.

Fases	Duración	Mes 1				Mes 2				Mes 3				Mes 4				Mes 5			
		S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18	S19	S20
➢ **FASE I** – Inicio del Proyecto - Entendimiento Situación – Construcción Plan Gestión Proyecto																					
➢ **FASE II** –Diagnóstico y Valoración de la Seguridad Informática																					
C1-Fortalecimiento en la Operación																					
C2- Gestión continua de Vulnerabilidades																					
C3- Solución de Gestión de Accesos Privilegiados-PAM																					
C4- Solución de seguridad para bases de datos Database Activity Monitoring (DAM)																					
C5- Solución de Control de Acceso a la red (Next Generation NAC)																					
➢ **FASE III** – Cierre del Proyecto																					

Nota: Para el cumplimiento del cronograma propuesto es necesario la disponibilidad del personal de la entidad y la entrega oportuna de la documentación y requerimientos técnicos solicitados.

- ✓ El cronograma de ejecución de actividades definitivo del proyecto será ajustado con el cliente una vez inicie el proyecto.
- ✓ Para los componentes opcionales se deberá ajustar el cronograma considerando la capacidad del recurso humano y tecnológico de la Entidad para no afectar los tiempos de ejecución de los componentes base.

DESCRIPCIÓN	Valor (COP)	IVA	Valor Total (COP) con IVA
Fortalecimiento de la Seguridad Informática para la **ESU-SECRETARIA DE INNOVACION DIGITAL DE MEDELLIN.** **Componente 1: Fortalecimiento en la Operación.** ▪ Revisión Centro de Operaciones de Seguridad SOC o Revisión del SOC para dar cumplimiento a lo dispuesto en el artículo 17 de la resolución 0500 de 2021 capacidades y servicios de SOC institucionales • Propuesta de estructura, proceso, procedimiento, formatos, manuales, perfiles, recomendación de herramientas. • Propuesta de especificaciones técnicas para la tercerización del servicio de acuerdo con la oferta disponible en el mercado actual. o Fortalecimiento de seguridad FIRST ▪ Plan de acción. ▪ Revisión de solución SIEM o Evaluación de fuentes y Eventos de Seguridad ▪ Revisión de documentación asociada a políticas, procedimientos, manuales, instructivos o prácticas asociadas a gestión de usuarios, gestión de logs, gestión de eventos, gestión de accesos, gestión de la actualización de las plataformas tecnológicas, ▪ Generación de Catálogo descriptivo para el fortalecimiento de actividades de detección y caracterización de eventos de seguridad. ▪ Ciberinteligencia y apoyo. o Implementación de SIEM.			

○ Suministro de la solución Splunk Enterprise Security suscripción por 2 años, capacidad de ingesta 50GB/d con almacenamiento en la nube 3 meses. Enterprise Support. (1 contact) ▪ Implementación de cinco (5) conectores ▪ Documento de configuración e implementación ▪ Documento de operación. ▪ Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual. ○ Integración Splunk con MISP ▪ Documento de configuración e implementación. ▪ Documento de operación. ▪ Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual. ○ Parametrizaciones Splunk ▪ Configuración de alertas base y creación de 1 acción para la notificación de incidentes. ▪ Configuración de 5 Dashboards & reports ▪ Documento de configuración ▪ Documento de operación. ▪ Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual. Recomendaciones de seguridad basadas en hallazgos encontrados durante la prestación del servicio.			
Fortalecimiento de la Seguridad Informática para la **ESU-SECRETARIA DE INNOVACION DIGITAL DE MEDELLIN.** . **Componente 2**: Gestión continua de Vulnerabilidades ▪ Revisión del proceso de gestión de vulnerabilidades de la entidad. ▪ Revisión de Procesos, procedimientos, formatos, instructivos, documentos que soportan el proceso de gestión de vulnerabilidades. ▪ Revisión de capacidades asociadas al proceso. (Personas, herramientas) ▪ Revisión de la estructura actual para la gestión continua de vulnerabilidades. ▪ Pruebas de Seguridad: ○ Pruebas de vulnerabilidad para cien (100) direcciones internas. ○ Informe ejecutivo, informe técnico. ▪ Suministro de licenciamiento SaaS: ○ Suministro de una suscripción de Tenable por 24 meses. a continuación, se detalle los componentes a entregar: *Tenable.sc Suscripción, IP Bands: 1650 *Tenable.io Web Application Scannings, Web Apps: 30 Transferencia de conocimiento ✓ Documento de configuración ✓ Documento de operación. ✓ Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual Capacitación: 10 horas Pruebas de seguridad en plataformas críticas.			

Grupo máximo: 10 personas Modalidad: Virtual.			
Fortalecimiento de la Seguridad Informática para la **ESU-SECRETARIA DE INNOVACION DIGITAL DE MEDELLIN.** **<u>Componente 3: Solución de Gestión de Accesos Privilegiados-PAM</u>** Suministro de la solución de Gestión de Accesos Privilegiados-PAM CyberArk para la Entidad. **Para 30 usuarios privilegiados.** a continuación, se detalle los componentes a entregar: •Credential Protection, Session Isolation, Recording, Detection,Remote Access, and Strong Authentication. Price per user permonth Cantidad: 30 Las cuentas privilegiadas representan la mayor vulnerabilidad de seguridad a la que se enfrentan las organizaciones en la actualidad. Estas cuentas privilegiadas se utilizan en casi todos los ataques cibernéticos y cualquier persona que tenga acceso a las mismas puede controlar los recursos de la organización, desactivar los sistemas de seguridad y acceder a grandes cantidades de datos sensibles. Para proteger estas cuentas y los recursos críticos a los que se puede acceder con dichas cuentas, las organizaciones necesitan controles exhaustivos para proteger, controlar, detectar y responder a todas las actividades realizadas desde cuentas con privilegios. CyberArk es el experto de confianza en la seguridad de cuentas privilegiadas. Diseñada desde cero enfocada en la seguridad, CyberArk Privileged Account Security Solution proporciona la solución más completa para la seguridad de las cuentas privilegiadas de sistemas on-premise, en la nube y en infraestructura crítica. Para implementar la solución PAM en la Entidad con sus módulos base, se ofrecen los servicios profesionales de diseño, implementación, configuración de la solución con el siguiente alcance: • Integración con el dominio • Parametrización de los módulos PSM, CPM y PVWA • Configuración de 16 accesos a servidores Transferencia de conocimiento ✓ Documento de configuración ✓ Documento de operación. ✓ Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual Capacitación: 10 horas Privileged Access Management Grupo máximo: 10 personas Modalidad: Virtual.			
Fortalecimiento de la Seguridad Informática para la **ESU-SECRETARIA DE INNOVACION DIGITAL DE MEDELLIN.** . **<u>Componente 4: Solución de seguridad para bases de datos Database Activity Monitoring (DAM)</u>** Suministro de la solución Database Activity Monitoring (DAM) por **24 meses Imperva-DAM** para la Entidad, a continuación, se detalle los componentes a entregar:			

•Imperva - *SF-SUB-DBF-X452-GWCL-GWCL TBL*Suscripción de software X4520 para Firewall de base de datos (cantidad 3). •Imperva -*SS-REPUESTO-X452-H1 *X4520 Gateway Appliance (cantidad 3) •Imperva - *SS-REPUESTO-X452-SL3 *X4520, repuesto in situ para Gateway Appliance.(cantidad 3) •Imperva - *SF-SUB-M17-TBL *Suscripción de software M170 para el software Management Server, suscripción mejorada. (cantidad 1) •Imperva *SS-REPUESTO-M17-H1 *Servidor de gestión M170, Appliance. (cantidad 1) •Imperva *SS-REPUESTO-M17-SL3 *M170 Management Server, repuesto in situ para Appliance. (cantidad 1) •Imperva - SKU: *U-DBURM-SUB-100-R-TBL *Actualización: licencia de administración de derechos de usuario para 100DBis, suscripción mejorada. (cantidad 1) Database Activity Monitoring suministra a la Entidad el monitoreo, la auditoría y la generación de informes de manera automatizada y escalable para entornos heterogéneos de base de datos. Ayuda a la Entidad a demostrar su conformidad con las normas legales a través de procesos, análisis y generación de informes automáticos. Esta solución hace más ágil la respuesta ante incidentes, mediante la administración centralizada y herramientas Implementación de Imperva-DAM en la Entidad con sus módulos base. Para un máximo de 10 bases de datos. Transferencia de conocimiento. Transferencia de conocimiento ✓ Documento de configuración ✓ Documento de operación. ✓ Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual Capacitación: 10 horas Seguridad en base de datos y aplicaciones. Grupo máximo: 10 personas Modalidad: Virtual.			
Fortalecimiento de la Seguridad Informatica para la **ESU-SECRETARIA DE INNOVACION DIGITAL DE MEDELLIN.** **<u>Componente 5: Solución de Control de Acceso a la red (Next Generation NAC)</u>** Suministro de la solución CISCO ISE 24 meses así: •Cisco ISE Virtual Machine Common PID Cantidad 3. •SOLN SUPP SWSS Cisco ISE Virtual Machine Common PID Cantidad 3. •Cisco Identity Service Engine Essentials Subscription Cantidad: 5100 •Cisco Identity Service Engine Premier Subscription Cantidad: 7400 •Cisco ISE Device Admin Node License Cantidad: 3 •Cisco AnyConnect Apex License, Users: Cantidad: 400			

A través de CISCO ISE – la Entidad puede emplear la información de toda su pila para hacer cumplir las políticas, administrar los puntos finales y brindar un acceso confiable. En la arquitectura de confianza cero, el motor de servicios de identidad (ISE) es el punto de decisión de la política. Recopila información de la pila para autenticar a los usuarios y puntos finales, y contiene automáticamente las amenazas. Implementación de CISCO-ISE en la Entidad con sus módulos base. Para un máximo de 50 dispositivos . Transferencia de conocimiento. Transferencia de conocimiento ✓ Documento de configuración ✓ Documento de operación. ✓ Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual Capacitación: 10 horas- Seguridad en redes bajo la filosofía Zero Trust. Control de Acceso a la red. Grupo máximo: 10 personas Modalidad: Virtual.			

RESUMEN

Servicio	Detalle	Precio	IVA	Costo final pesos (COP)
Fortalecimiento en la Operación	Revisión SOC			
	Revisión SIEM+ Ciberinteligencia			
	Licencia			
Gestión continua de Vulnerabilidades	Servicios			
	Licencia			
CyberArk (PAM)	Servicios			
	Licencia			
Firewall Base de Datos	Servicios			
	Licencia			
Solución CISCO NAC	Servicios			
	Licencia			
TOTAL				