password

*INNOVANDO PARA **ASEGURAR** LAS*
ESTRATEGIAS DIGITALES** DE NUESTROS **CLIENTES



ALCALDIA DE SANTIAGO DE CALI

CONSULTORIA EN GOBIERNO Y SEGURIDAD DIGITAL +
SERVICIO DE CIBERSEGURIDAD- SOC

John Edinson Martinez

OFERTA TÉCNICO -ECONOMICA

Cliente	ALCALDIA DE SANTIAGO DE CALI
Nombre del documento	CONSULTORIA EN GOBIERNO Y SEGURIDAD DIGITAL + SERVICIO DE CIBERSEGURIDAD- SOC
Estado del documento	Liberado
Responsables	John Edinson Martinez Gerente Comercial

Control de versiones del documento

Versión	Creación	Liberación	Descripción Cambio
1.0	30/04/2024	19/09/2024	Liberación Inicial

Tabla de contenido

1. OBJETIVO 9
2. ALCANCE DEL SERVICIO 9
2.1 DESCRIPCION DETALLADO 10
2.1.1 Puesta en Marcha SGSI 10
2.1.1.1 Fase I Diagnóstico, Diseño y Planificación 10
2.1.1.1.1 Actividades a Desarrollar 11
2.1.1.1.2 Entregables Fase I 14
2.1.1.2 Fase-II-Implementación 15
2.1.1.2.1 Actividades a Desarrollar 15
2.1.1.2.2 Entregables Fase II 16
2.1.1.3 Fase-III-Sensibilización y Capacitación 16
2.1.1.3.1 Actividades a Desarrollar 17
2.1.1.3.2 Entregables -Fase III 17
2.1.1.4 Fase-IV-Suministro de herramienta de software para la gestión del SGSI 18
2.1.1.4.1 BENEFICIOS 18
2.1.1.4.2 MODULOS 19
2.1.2 CENTRO DE OPERACIÓN DE SEGURIDAD-CORRELACION DE EVENTOS 23
2.1.2.1 INFRAESTRUCTURA A MONITOREAR 24
2.1.2.2 ALCANCE SOC 25
2.1.2.3 CORRELACION DE EVENTOS 25
2.1.2.4 DESCRIPCION DE LOS SERVICIOS 26
2.1.2.5 NIVELES DE OPERACIÓN 27
2.1.2.6 ARQUITECTURA 28
2.1.2.7 IMPLEMENTACION DEL SERVICIO 29
2.1.2.8 ACUERDOS DE NIVELES DE SERVICIO 30

2.1.2.9 SERVICIOS DE GESTION DE INCIDENTES DE SEGURIDAD. 30

3. Duración del Servicio 31

4. OFERTA TECNICA 31

5. CONDICIONES COMERCIALES. 33

6. ACUERDO DE CONFIDENCIALIDAD 33



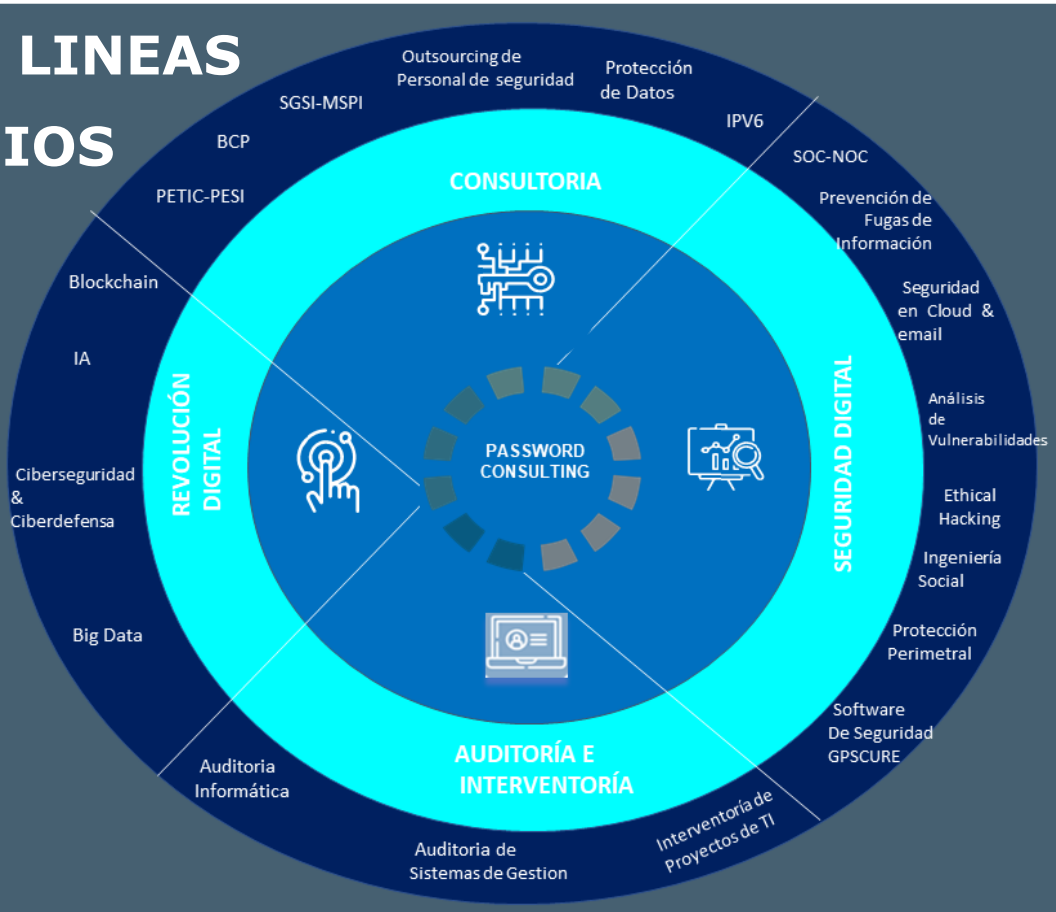
PRESENTACION Y EXPERIENCIA

PASSWORD CONSULTING SERVICES S.A.S., Es una compañía colombiana que cuenta con más de 17 años en el mercado, líderes en seguridad digital, transformación digital, tecnologías de la información y de las comunicaciones. Con nuestra experiencia hemos desarrollado productos innovadores sólidos y confiables. Contamos con un equipo de personas diversas, apasionadas y excepcionales, que se esfuerzan por sobresalir, hacer lo correcto y lograr un cambio positivo en todo lo que hacen.

PASSWORD, aporta al éxito de todos los proyectos por medio de un pensamiento audaz y un deseo de ser los mejores en el trabajo en consultoría, análisis, soluciones de transformación digital y seguridad en industrias, que van desde la defensa hasta el medio ambiente, la educación, la industria y el desarrollo internacional.

Realizamos un acompañamiento continuo e integral a nuestros clientes, convirtiéndonos en parte de la organización para apoyarlos en el camino hacia la revolución digital, agregando valor al negocio y convirtiéndonos en su aliado estratégico.

NUESTRAS LINEAS DE SERVICIOS





Realizamos un acompañamiento continuo e integral a las entidades para que den cumplimiento con la normatividad en materia de tecnología

CERTIFICACIÓNES EMPRESARIALES

CO16/6862

CO19/8986

CERTIFICACIÓNES PROFESIONALES

ALGUNOS DE NUESTROS CLIENTES



EDUCACIÓN

ICESI
USC Universidad Santiago de Cali
Universidad del Quindío
Pontificia Universidad Javeriana
Universidad de San Buenaventura
Universidad Tecnológica de Pereira

ENERGETICO

ecopetrol
EPSA
GdO Gases de Occidente
Efigas
edeq

GOBIERNO

República de Colombia – MinSalud
Contaduría General de la Nación
MinTIC Ministerio de Tecnologías de la Información y las Comunicaciones
Supersalud
DIAN
TRANSMILENIO

SERVICIOS

SuperGIROS
Grupo Coomeva
Giros & Finanzas
Financiera Pagos Internacionales
Comfenalco Valle de la gente
Carvajal Tecnología y Servicios
Siesa

DEFENSA

Policía Nacional

FINANCIERO

Colpatria
Banco W
Banco Agrario de Colombia
Bancoomeva Nos facilita la vida
Finesa

RETAIL Y INDUSTRIA

Incauca S.A.S.
Studio F.
mayagüez & Sancarlos
Cosmoagro
Huevos Santa Rita
Tecnoquímicas

1. OBJETIVO

Prestar el Servicio de Consultoría especializada buscando Mejorar los índices de desempeño institucional de las políticas de gobierno digital y de seguridad de la información dentro del MIPG. Para ALCALDIA DE SANTIAGO DE CALI acorde con las necesidades planteadas, al igual que poder prestar el Servicio especializado de SOC, para cubrir las necesidades actuales en cuanto a CIBERSEGURIDAD

2. ALCANCE DEL SERVICIO

De acuerdo con las necesidades planteadas por **ALCALDIA DE SANTIAGO DE CALI** propuesta cubre el siguiente alcance:

Actualización, Diseño, documentación e implementación y operación de un Modelo de seguridad de la información que promueva de manera consistente y efectiva, mecanismos para la reducción de riesgos de seguridad, de acuerdo con los lineamientos definidos por el Ministerio de Tecnologías de Información y de las Comunicaciones y plasmados en el Decreto 1008 de 2018, el Manual de Gobierno Digital y en la documentación (guías, manual y autodiagnóstico) ofrecida sobre el Modelo de Seguridad y Privacidad de la Información. Y teniendo como marco de referencia la Norma ISO/IEC 27001:2022, esto para para **DOS** procesos de TI de la ALCALDIA. Adicional a estose Proveerá las capacidades de monitoreo centralizado y especializado para identificar, detectar y responder adecuada y oportunamente ante los incidentes de seguridad que puedan afectar la información de una organización.

2.1 DESCRIPCION DETALLADO

Se desarrollará bajo los lineamientos de gestión de proyectos que establezca la Entidad ejecutando las siguientes fases:

- **Puesta en Marcha SGSI**

fase I: Diagnóstico, Diseño y Planificación
fase II : Implementación
fase III: Sensibilización y Capacitación
fase IV: Suministro de herramienta de software para soportar y administrar el SGSI de la entidad.

CENTRO DE OPERACIÓN DE SEGURIDAD-CORRELACION DE EVENTOS

2.1.1 Puesta en Marcha SGSI

2.1.1.1 Fase I Diagnóstico, Diseño y Planificación

Realizar un análisis del estado actual del SGSI, para lo cual se revisa la política y el alcance del SGSI, se establecen los responsables y las responsabilidades en cuanto a seguridad de la información y se realiza el levantamiento y valoración de activos de información, análisis de vulnerabilidades e identificación de riesgos de seguridad de la información. Además de:

- Determinar el nivel de madurez en seguridad de la información con relación a la Norma ISO/IEC 27001:2022
- Identificar el estado actual de la Gestión de Seguridad de la Información de acuerdo a lo contemplado en el Mapa de Procesos que cuenta la entidad.
- Realizar la identificación, valoración y clasificación de los activos de información que posee la entidad.
- Análisis de vulnerabilidades: Identificar las amenazas y vulnerabilidades a las que se encuentra expuesta la Entidad tanto en servidores, equipos de cómputo, activos de red, sistemas de información esto para un máximo de **500 activos.**

- Gestión de Riesgos de Seguridad de la Información para los procesos incluidos. Adoptar y ajustar, la metodología de gestión

del riesgo. Que incluye, análisis, evaluación y mitigación del riesgo, basados en la Norma ISO 27005:2013 o Norma ISO 31000.

2.1.1.1.1 Actividades a Desarrollar

Recolección y análisis de la información: levantamiento de la información para realizar el diagnóstico del SGSI.

El diagnóstico de seguridad incluye:

- ✓ Realizar entrevistas con las diferentes áreas para levantar el inventario de activos de información, entiéndase como activo de información de acuerdo a la definición de la ISO 27000:2022 (En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización).
- ✓ Revisar las Políticas de Tecnología de Información, esquemas de copias de seguridad o respaldo y esquemas de impresión.
- ✓ Identificar la topología física y lógica de la red.
- ✓ Revisar la documentación existente.
- ✓ Evaluar y desarrollar las políticas de seguridad de la información que requiera la entidad.
- ✓ Formular una propuesta que permita dar tratamiento de Políticas de Seguridad en la entidad que contempla:
  - Definición de los procedimientos para el manejo de la documentación.
  - Control de cambios.
  - Definición de roles y responsabilidades del personal involucrado en el mantenimiento de las políticas de seguridad de la información.
  - Gestión de incidentes.

Para la valoración y clasificación de los activos de información identificados se desarrollan las siguientes actividades:

a) Evaluación de los procesos, procedimientos y actos administrativos existentes en la Entidad relacionadas con el tema de seguridad de la información.
b) Evaluación del estado actual de los sistemas de información en cuanto a su seguridad, teniendo en cuenta los siguientes aspectos:

- Procedimientos de control cambios.
- Procedimientos de administración del sistema.
- Esquemas de acceso al sistema de información.
- Niveles de integridad, confidencialidad y disponibilidad en cuanto a acceso permitido.
- Almacenamiento y archivado, disposición y destrucción.
- Administración y controles existentes sobre las bases de datos
- Procedimientos de respaldo de información.

En la identificación de las amenazas y vulnerabilidades a las que se encuentra expuesta la Entidad ejecutan pruebas de vulnerabilidad en un máximo de 500 activos , Las pruebas de vulnerabilidad se planean y coordinan con la entidad para ser ejecutadas.

El análisis de vulnerabilidades implica desarrollar las siguientes actividades:

a) Análisis de vulnerabilidades para determinar las debilidades existentes de los servicios a nivel interno y externo, aplicando las recomendaciones del OSSTMM.
b) Realizar la delimitación del perímetro y verificación de la red de la entidad.
c) Evaluar la configuración de los firewalls, entre otros: lista de acceso, análisis de los puertos, los servicios abiertos, entre otros.
d) Realizar prueba de intrusión en la red de área local (LAN) tanto alámbrica como inalámbrica y con base en esta determinar el estado actual de la infraestructura tecnológica.
e) Realizar prueba de penetración a 10 IPs públicas, con el fin de determinar el estado actual de la infraestructura tecnológica y la seguridad de su interconexión.
a) g) Realizar análisis de vulnerabilidades en los host.

Pruebas de Ingeniería Social

Ejecución de Ingeniería social presenciales (en las instalaciones de la Entidad) y no presenciales.

1. **Pruebas presenciales**

Análisis del nivel de cumplimiento y madurez de los siguientes controles especificados en el dominio N.º 11 de la norma ISO 27001:2022 (seguridad física y ambiental) como son:

a) Áreas de acceso público

b) Seguridad de los equipos
c) Emplazamiento y protección de equipos
d) Instalaciones de suministros
e) Seguridad de los equipos y activos fuera de las instalaciones
f) Revisión del cumplimiento de la política de escritorio limpio y pantalla bloqueada, determinando los horarios habituales en que los colaboradores no se encuentran en su sitio de trabajo y ejecutando revisiones presenciales para constatar el cumplimiento de los aspectos que comprenden el diagnóstico.

2. Pruebas no presenciales

Estarán orientadas a la utilización de medios informáticos como el correo electrónico, redes sociales e internet y se realizarán con recursos propios del contratista, de los mecanismos a utilizar y los tiempos en los que se ejecutarán.

Las pruebas contemplan:

- Recolección de información que vincule a la entidad, en internet y redes sociales.

- Haciendo uso de técnicas como googlehacking, búsqueda de metadatos y cualquier otra que el contratista proponga y sea aprobada previamente por la entidad, se realiza recolección de información que vincule a la entidad, en Internet y redes sociales, realizando búsqueda de archivos, usuarios y claves de correo o de dominio, nombre de impresoras, maquinas, software, sistemas operativos, extensiones telefónicas, datos personales de los funcionarios de la entidad, entre otra información que se considere relevante. Esto, con el propósito de establecer si es posible encontrar información privilegiada de la entidad y/o sus funcionarios publicada en la red, que pueda ser aprovechada por terceros generando exposición a riesgos de seguridad de la información.

Fake Mailing

Envio de correos electrónicos haciendo uso de la técnica mail relay, a través de un servidor de correo que lo permita a cuentas de correo de la entidad, previamente definidos por la entidad, para lograr los siguientes objetivos:

- Intentar obtener información privilegiada

- Intentar obtener nombres de usuarios y/o contraseñas

- Intentar que el usuario responda y/o reenvíe el correo

Suplantación de un servicio web o intento de phishing

Intento o materialización de un ataque de phishing por medio del correo electrónico con el cual se intente que los receptores del mensaje ingresen a un link y accedan a una página web con las mismas características de algún servicio web provisto por la entidad.

Gestión de Riesgos de Seguridad de la Información. Para adoptar y ajustar la metodología de gestión de riesgos de seguridad de la información, basado en la Norma ISO 27005 o Norma ISO 31000 la ISO 27005, ISO 31000 se ejecutan las siguientes actividades:

1. Revisar la metodología de gestión de riesgos y adoptarlo al SGSI para identificar los riesgos de seguridad de la información, de acuerdo a la norma ISO 27001:2022.

2. Si la entidad a la fecha cuenta con matriz de riesgos de los activos de información se revalida y actualiza, de lo contrario se construye con el acompañamiento de los dueños de los procesos, la cual contendrá los requerimientos mínimos de gestión del riesgo de la norma ISO/IEC 27001:2022

2.1.1.1.2 Entregables Fase I

Como resultado de la consultoría realizada se deben entregar los siguientes productos de los DOS procesos del alcance.

- Informe con la identificación del nivel de madurez resultado del análisis GAP.
- Inventario de activos de información de los procesos del alcance
- Documento con la propuesta de instructivo de clasificación y etiquetado de activos de información.
- Documento que contenga la propuesta de política, el alcance y los objetivos del SGSI.
- Documento que contenga la propuesta de los procesos y procedimientos necesarios para el mantenimiento del esquema de políticas de seguridad de la información.

- Informe del análisis de vulnerabilidades.
- Informe de los resultados de pruebas presenciales y no presenciales.
- Gestión de riesgos de seguridad de la información:
  - Documento con la metodología de la gestión de riesgos.
  - Matriz de valoración riesgos de seguridad de la información
  - Documento con el plan de tratamiento de riesgos

2.1.1.2 Fase-II-Implementación

Corresponde a la ejecución de todo lo planeado en la fase de diseño, con el fin de monitorear resultados y efectuar acciones de retroalimentación y así la implementación del plan de tratamiento de riesgos, implementación de controles e implementación del Subsistema de Gestión de Seguridad de la Información (SGSI), definir el plan de continuidad de negocio (BCP) con su respectivo Análisis de impacto al negocio (BIA).

Así mismo, se pretende medir el estado actual frente al cumplimiento de cada requisito de la norma, es decir, se verifica si se ha ejecutado lo planeado. Se incluye la medición del SGSI, requisitos legales, del cliente y de la organización

Además de:

- Implementación del SGSI a los procesos de la entidad de acuerdo al alcance establecido
- Definir Plan de contingencia y de continuidad del negocio (BCP)
- Definir Análisis de impacto al negocio (BIA)
- Implementar los procedimientos del SGSI
- Evaluar el cumplimiento de las políticas/procedimientos implementados

2.1.1.2.1 Actividades a Desarrollar

- Crear, revisar y/o actualizar el Plan de contingencia y de continuidad del negocio (BCP), Análisis de impacto al negocio (BIA) y el Plan de recuperación de Desastres (DRP) con que cuenta la Alcaldía acorde con las necesidades de ALCALDIA DE CALI
- Definir los indicadores adecuados para la medición del SGSI.
- Revisar la eficiencia, efectividad y eficacia del SGSI
- Revisión del tipo de información que genera la entidad y su esquematización frente a la Ley de transparencia. Análisis de los

lineamientos expedido por MinTic para publicación de la información pública.

- Establecimiento de los lineamientos y condiciones sobre medios para recepción de solicitudes de información pública. Análisis de requisitos a formular para la atención ciudadana y condiciones de seguridad de la información.
- Análisis sobre información clasificada y reservada. Índice de información clasificada y reservada. Protocolo de etiquetado y clasificación de información.

2.1.1.2.2 Entregables Fase II

Plan de tratamiento de riesgos

- Informe de la ejecución del plan de tratamiento de riesgos.
- Documento con la declaración de aplicabilidad.
- Evidencias de las actividades de implementación de procedimientos del SGSI

Definición Del Modelo De Seguridad SGSI

Documento con el modelo de seguridad que contiene:

- Política del SGSI
- El alcance del SGSI
- Objetivos del SGSI
- Manual de políticas de seguridad de la información
- Documento con la definición de los roles y responsabilidades en la SGSI
- Documento con el Plan de continuidad del negocio (BCP)
- Documento con el Análisis de impacto al negocio (BIA)

Seguimiento SGSI

- Documento que contenga lo indicadores propuestos para el SGSI
- Valoración de los indicadores del SGSI.

2.1.1.3 Fase-III-Sensibilización y Capacitación

Diseñar una campaña y estrategia de sensibilización y divulgación de políticas y

procedimientos de SGSI. Así como Evaluar el cumplimiento de las políticas/procedimientos implementados.

2.1.1.3.1 Actividades a Desarrollar

Se proponen **5** actividades de sensibilización y divulgación en cultura de seguridad para los funcionarios de la ALCALDIA DE CALI , las cuales se definen de manera independiente; para validación y selección de las que la entidad considere deben ser ejecutadas por parte del contratista en el proyecto.

Las propuestas contemplan las siguientes alternativas:

a) 1 Performance – representación teatral en la Entidad
b) 2 Talleres de sensibilización en temas de seguridad
c) 2 Conferencias con ayudas audiovisuales

- Planeación y coordinación de la logística para la realización de la sensibilización y divulgación de temas de seguridad de acuerdo con las propuestas seleccionadas por la Entidad.
- Elaboración del material para la divulgación y sensibilización a los funcionarios de la Entidad, incluye 2 videos, 2 wallpapers, 1 pendón, souvenirs.
- Ejecución de la sensibilización y divulgación en temas de seguridad de acuerdo con las propuestas aprobadas por la Entidad.

2.1.1.3.2 Entregables -Fase III

- Documento con el plan de sensibilización y divulgación de seguridad.
- Documento que contiene el plan de ejecución de la sensibilización y divulgación de seguridad.
- Documento que contiene el plan de promoción de sensibilización y divulgación de seguridad.
- Material de promoción para realizar la sensibilización y divulgación en temas de seguridad.
- Evidencias de las actividades de sensibilización

2.1.1.4 Fase-IV-Suministro de herramienta de software para la gestión del SGSI

Como apoyo para la prestación del servicio, se debe suministrar un software especializado en la administración y gestión del SGSI **POR 2 AÑOS** el cual es una herramienta que ayuda a las organizaciones en la implementación, gestión y mantenimiento de Sistemas de Gestión

Que cumpla de manera efectiva con la normativa vigente en materia de implementación de SGSI (ISO/ICE 27001:2022). Todos los módulos complementarios e integrados que posee el software ayudan con el cumplimiento legal y regulatorio a toda la organización.

Nuestra herramienta es un software totalmente desarrollado en un ambiente web que facilita la labor entre todos los integrantes y responsables de su SGSI que puede ser utilizado en cualquier dispositivo.

El cumplimiento de la norma requiere la realización de determinadas tareas por parte de los encargados del SGSI al interior de la organización; **El software** cuenta con módulos que automatizan dichas actividades.

2.1.1.4.1 BENEFICIOS

- ✓ **Gestión desde cualquier lugar:** Administre su SGSI con facilidad desde donde sea que se encuentre (con acceso a su red corporativa), ya que la solución presentada proporciona un 100% de administración centralizada basada en web.
- ✓ **Colaboración:** Es una herramienta de colaboración que facilita la labor entre todos los integrantes y responsables de SGSI y los diferentes usuarios del sistema.

- ✓ **Cumplimiento:** Automatiza las actividades que los encargados del SGSI deben realizar para el cumplimiento de la norma.
- ✓ **Accesibilidad:** Al ser una herramienta Web permite su visualización y gestión desde cualquier dispositivo con acceso a la red de su compañía usando un navegador.
- ✓ **Gran cantidad de módulos:** Nuestra herramienta se encuentra implementada a través de módulos, cada uno de ellos cumple funcionalidades específicas que le permitirán gestionar su SGSI de una manera ágil y eficiente.
- ✓ **Soporte de expertos:** Con nuestra solución su compañía tendrá el acompañamiento de un equipo de gran experiencia en la implementación de SGSI.

2.1.1.4.2 MODULOS

Este Software tendra una vigencia de 24 Meses igual que el contrato inicial , si es password el ofertente adjudicado.

HERRAMIENTA MODULAR PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
GENERALIDADES	• Establece controles de ingreso por usuario, con asignación de roles y grupos de usuarios • Facilita el cargue de tablas básicas pre diligenciadas como procesos, activos, riesgos y en general los datos que la entidad requiera para parametrizar adecuadamente la aplicación. • Permite la fácil consulta a través de filtros con combinación de criterios que permitan obtener reportes en los diferentes módulos del sistema de información. • Tiene control y auditoria para identificar la trazabilidad de los registros y acciones de los usuarios tales como accesos, creación de registros, eliminación, modificación. • Se integra al correo electrónico para él envió de notificaciones. • Cuenta con la autenticación de usuarios a través de una integración con el directorio activo.

	• Cuenta con un sistema de verificación Captcha. • Cuenta con certificado SSL. • Accesible a través de diferentes navegadores. • No solicita la instalación de ningún software en los equipos desde los cuales se acceda. • Permite autenticación por medio de cuentas Microsoft o cuentas de Google.
GESTIÓN DOCUMENTAL	• Permite el control de la documentación del SGSI para poder publicar en el mismo las políticas, normas, procedimientos, instructivos, entre otros • Los documentos se catalogan según su clasificación y sobre ellos garantizar permisos de consulta por grupos de usuarios. • Permite crear y visualizar la caracterización del proceso de seguridad de la información de manera simple y dinámica. • Puede publicar un glosario de términos que permita el uso adecuado del lenguaje y terminología propia del Sistema de Gestión de Seguridad de la Información.
GESTIÓN DE RIESGOS	• Está en la capacidad de realizar la gestión de riesgos: identificación, tipificación, análisis, tratamiento entre otros. • En la identificación de Riesgos permite enlazar los activos de información. • Permite la parametrización de probabilidad e impacto, niveles de valoración de riesgos, amenazas, vulnerabilidades por tipos de activos, definición de niveles de riesgo, listado de riesgos, Catálogo de controles y mapa de calor configurables. • Permite la comparación de los mapas antes y después de valoración de riesgos y la calificación. • Establece cuáles recursos del negocio van a ser considerados dentro del cálculo del impacto del riesgo, (Recurso Financiero, operación, imagen, legal, ambiental, Humano) • Cuenta con un catálogo predefinido de amenazas y vulnerabilidades. • Carga y administra las causas, factores y consecuencias de los riesgos. • Define la parametrización para los niveles de riesgo residual. • Permite generar un plan de tratamiento de riesgos. • Permite asociar controles para la gestión de riesgo. • Permite la parametrización de la declaración de aplicabilidad.

GESTIÓN DE EVENTOS E INCIDENTES	• Permite registrar eventos e incidentes de seguridad, asignándole un identificador o ID de manera automática, las actividades realizadas para diagnosticar, analizar, contener el incidente. • Permite asignar responsable(s) del incidente, tipificarlo y establecer su impacto, criticidad y tiempos de respuesta. • Permite escalamiento y notificaciones enlazado con el correo electrónico. • Permite consultar las lecciones aprendidas. • Permite que cualquier usuario pueda reportar un evento de seguridad de la información. • Cuenta con reportes gráficos de Top de riesgos con mayores activos, Top de vulnerabilidades con mayores riesgos, Top de amenazas con mayores riesgos, Top de factores con mayores Riesgos, Top de riesgos por procesos. • Permite la definición de diferentes tipos de incidentes
GESTION DE USUARIOS ROLES Y GRUPOS	• Brinda a las entidades y organizaciones, la posibilidad de gestionar los usuarios, grupos y roles de forma intuitiva y sencilla, posibilitando la auditoria a usuario, informes de permisos asignados, registro de usuarios por medio de CMS, LDAP (directorio activo), Google o Microsoft, entre otras funcionalidades
AUDITORIA Y SEGUIMIENTO	• Permite administrar y gestionar de manera integral todo el proceso de auditorías internas de seguridad de la información. • Permite la creación automática del informe por cada auditoría realizada. • Cuenta con una opción para revisión por la dirección. • Permite registrar las correcciones inmediatas a las no conformidades detectadas y acciones de mejora
INDICADORES	• El sistema permite diseñar y publicar cualquier indicador requerido para el sistema de gestión de seguridad de la información y su respectiva ficha técnica para su respectiva medición, seguimiento y control. • Permite la valoración de indicadores para calificar el cumplimiento de estos con base en variables automáticas que traiga el mismo sistema relacionados como mínimo con la gestión de eventos o incidentes • Genera reportes, gráficos y poseer elementos que permitan hacer un mejor seguimiento, análisis y mejora a la Entidad. • Permite establecer rangos superiores e inferiores y periodicidad de medición.

PLAN DE CONTINUIDAD	• Permite registrar las variables críticas del BIA, RTO, RPO. • Registra los periodos críticos de operación y llevar un registro de interrupciones ocurridas. • Registra las pérdidas que pueden ocurrir en diferentes recursos del negocio, cuando no es posible ejecutar una actividad o proceso de la Entidad/organización.
GESTION DE ACTIVOS	• Tiene ela capacidad de realizar la gestión de activos: identificación, registro, clasificación, criticidad y valoración entre otras • Permite la creación de nuevos campos personalizados para el formulario de creación de activos de información. • Permite el cargue masivo de información previa, mínimo en formato Excel. • Cuenta con un inventario de activos de información que se consulte desde la herramienta y sea exportable. • Genera reportes, gráficos y poseer elementos que permitan llevar control de la gestión de activos de información. • Permite la personalización de campos como responsable de activo y custodio. • Permite la valoración de activos según las propiedades de criticidad, disponibilidad e integridad.
GESTIÓN DE PROCESOS, OBJETIVOS Y REQUISITOS	• Permite el registro de procesos, áreas, cargos y objetivos estratégicos de la entidad u organización, así como la relación de documentos y requisitos legales a los procesos para la gestión de auditorías dentro del módulo de Seguimiento. •
GESTIÓN DE TAREAS	• Cuenta con un tablero de tareas en donde los usuarios identifiquen las actividades pendientes del sistema de gestión de seguridad de la información. • Permite la configuración de tiempos de gestión de dichas tareas. • Permite Administrar la asignación de tareas para gestionar las actividades propias al sistema. • Permite anexar archivos de evidencia
ANÁLISIS DE BRECHAS	- permite adicionar y administrar las normas, estándares o leyes sobre las cuales se quiere medir el cumplimiento normativo de seguridad de la información por ejemplo MSPI e ISO 27001. - Permite Calificar el nivel de cumplimiento de un control o requisito, navegando por objetivo de control o área de cumplimiento y sub-área o domino.

	Permite que los usuarios justifiquen la calificación de cumplimiento con observaciones y recomendaciones
PROTECCIÓN DE DATOS PERSONALES	- Permite el registro y actualización de bases de datos, que se vinculen a encargados, canales, finalidades. - Permite la creación de Encargados para la base de datos. - Permite gestionar los requisitos de la ley de protección de datos -
GESTION DE CAMBIOS	- Permite cualquier usuario registrar solicitudes de cambio con el potencial de causar un impacto mayor en los servicios, infraestructura tecnológica o aspectos relacionados con la seguridad de la información. - Permite parametrizar y administrar la gestión de las solicitudes, debe contar con el sistema de notificación vía correo electrónico a través del cual se informa el estado de la solicitud. -
ENTRGABLES	- Suministro del portal web para uso de la herramienta por parte de la Organización. - Documentación guía y manuales de usuario disponibles en formato electrónico. - Credenciales de acceso para (4) usuarios administradores de la solución. - Creación de 10 usuarios iniciales para el uso de la herramienta. -

2.1.2 CENTRO DE OPERACIÓN DE SEGURIDAD-CORRELACION DE EVENTOS

Nuestro Centro de operaciones de Seguridad (SOC) registra y analiza los logs de eventos de la infraestructura de seguridad de nuestros clientes para determinar si se están presentado eventos que correspondan a

posibles ataques cibernéticos o a incumplimientos de políticas de seguridad que pongan en riesgo las operaciones del negocio.

Nuestro SOC tiene como propósito:

Proveer capacidades de monitoreo centralizado y especializado para identificar, detectar y responder adecuada y oportunamente ante los incidentes de seguridad que puedan afectar la información de una organización.

Detectar en el menor tiempo posible los ataques para limitar el daño. La rentabilidad que da un SOC se refleja en el ahorro de dinero que implica tratar rápidamente los incidentes de seguridad.

Nuestro servicio de SOC está basado en estos lineamientos para que ALCALDIA pueda obtener los beneficios de un servicio de inteligencia, gestionado y controlado y que adicionalmente no tengan que invertir en aspectos o funciones que no son relevantes dentro de las necesidades de apoyo para la gestión de la ciberseguridad.

2.1.2.1 INFRAESTRUCTURA A MONITOREAR

LINEA BASE DEL SERVICIO

NODOS A MONITOREAS	CANTIDAD
Server	200
Workstation	
Network devices	

2.1.2.2 ALCANCE SOC

Las actividades generales a realizar en este servicio en modalidad 7x 24 incluyen:

- Monitoreo en la notificación de los eventos u ofensas de seguridad, información sobre amenazas emergentes.
- Detección temprana de ataques a través de analítica de logs generadas desde diferentes fuentes.
- Identificar y reportar comportamientos anómalos, no autorizados, fraudulentos y/o sospechosos que atenten contra la disponibilidad e integridad de la información y sistemas correlacionados.
- Entrega mensual de un informe durante la vigencia del contrato que incluye: Top de Reportes, eventos, recomendaciones, lecciones aprendidas, informe de vulnerabilidades.
- Alcance en configuración de reglas simples y de correlación
- Configuración de Dashboard Básicos

2.1.2.3 CORRELACION DE EVENTOS

La Gestión de Eventos se puede definir como el proceso que se encarga detectar cambios significativos para tomar las medidas de control necesarias según determinen estos eventos. Esto quiere decir que la Gestión de Eventos es la base para la supervisión y el control de las operaciones de Seguridad y de TI.

Nuestro proceso de gestión de eventos contempla las siguientes actividades:

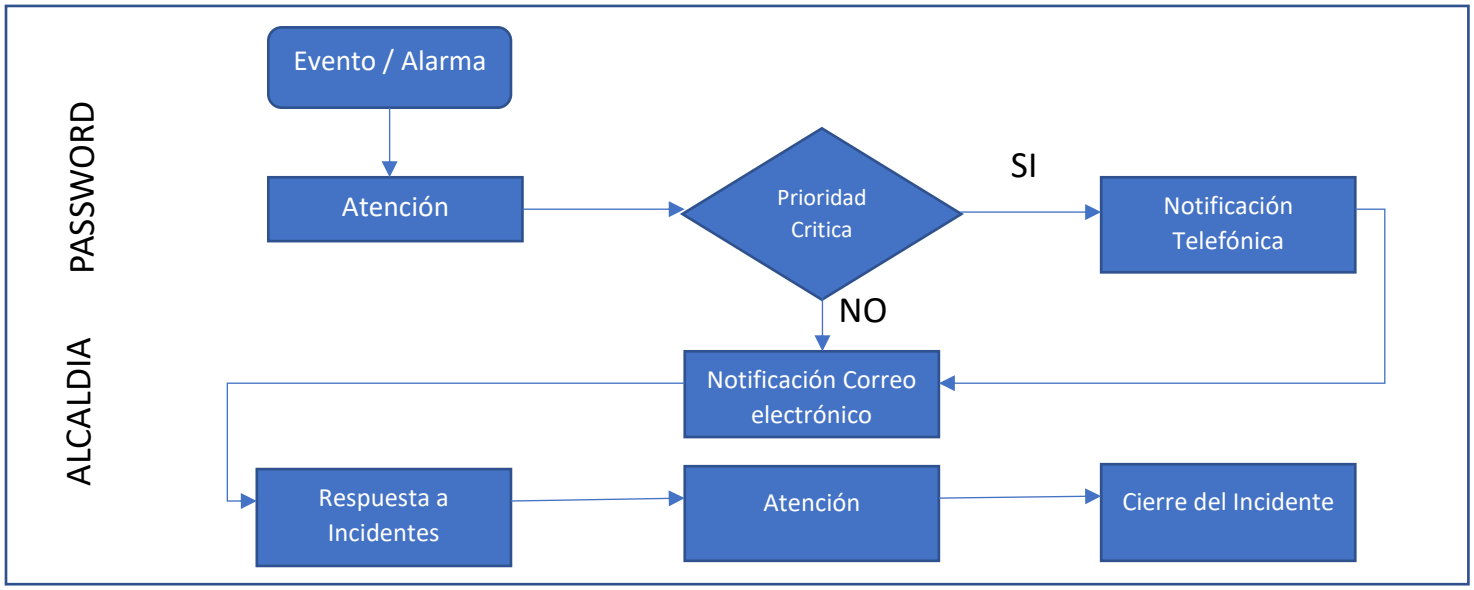
TAREA	DESCRIPCION
Mantenimiento de Mecanismos y Reglas de Monitorización de Eventos	Establecer y mantener los mecanismos para generar reglas efectivas para los procesos de descarte y correlación de Eventos.
Clasificación y Categorización de Eventos	Clasificar aquellos eventos que se pueden obviar, y asignar categorías a los que son significativos.
Correlación de Eventos y Selección de Respuestas	Interpretar el significado de un Evento y elegir una respuesta adecuada.
Revisión y Apoyo Cierre de Eventos	Verificar que los Eventos hayan sido manejados adecuadamente y si se pueden cerrar. Este proceso también sirve para asegurar que los registros de eventos sean analizados de manera que se identifiquen tendencias y patrones que puedan sugerir medidas correctivas necesarias.

Las actividades generales a realizar en este servicio incluyen:

- Gestión y correlación de eventos.
- Monitoreo, gestión en la notificación de los eventos u ofensas de seguridad, información sobre amenazas emergentes.
- Apoyo a la Atención de incidentes y apoyo a la investigación de causa raíz sobre los eventos de seguridad que se materialicen
- Detección temprana de ataques a través de analítica de logs generadas desde diferentes fuentes de ALCALDIA DE CALI.
- Identificar y reportar comportamientos anómalos, no autorizados, fraudulentos y/o sospechosos que atenten contra la disponibilidad e integridad de la información y sistemas correlacionados.
- Entrega mensual de un informe durante la vigencia del contrato, el cual incluya los incidentes detectados así como las acciones de prevención, detección y respuesta frente a eventos de seguridad identificados.

2.1.2.4 DESCRIPCION DE LOS SERVICIOS

El SOC prestara de manera remota la atención de primer nivel de los incidentes detectados, escalando al grupo de seguridad de ALCALDIA , de acuerdo a los SLA definidos en el presente documento. El flujo atención es como se muestra a continuación



* Los eventos de prioridad crítica y alta serán notificados al grupo de seguridad del ALCALDIA a través del contacto telefónico provisto para tal fin. Los eventos de prioridad media, baja e informativos también serán notificados vía correo electrónico.

2.1.2.5 NIVELES DE OPERACIÓN

Nivel 1: Equipo de PASSWORD

- Monitoreo de la plataforma tecnológica de monitoreo.
- Gestión de requerimientos básicos de plataforma bajo los esquemas ya establecidos para estos casos.
- Apoyo especializado a la Gestión con los ingenieros expertos de ALCALDIA en caso de presentarse alguna incidencia que afecte la operación de.
- Gestión de todos los incidentes requerimiento (entre nivel uno)

Nivel 2: Equipo de ALCALDIA encargado de:

- Administración especializada sobre los elementos de la plataforma Tecnológica de seguridad informática.

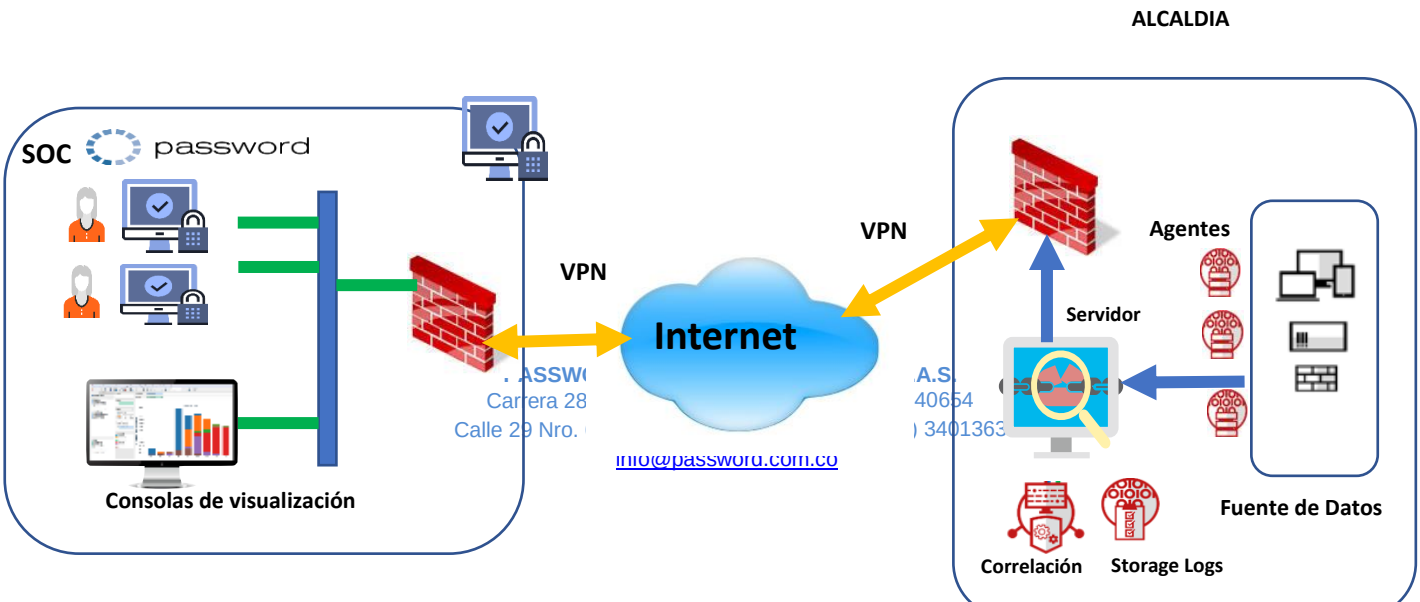
- Gestión de requerimientos, solicitudes e incidentes de la plataforma Tecnológica de seguridad informática.
- Ejecución de cambios básicos de impacto medio y bajo.
- Escalamiento con los fabricantes de las tecnologías incluidas en esta solución.
- Interacción con especialistas de los fabricantes en busca de la solución a un incidente en la plataforma tecnológica de alto impacto

Nivel 3: Equipo de ALCALDIA encargado de:

- Apoyo especializado a los fabricantes en busca de dar solución a incidentes (casos) de la plataforma tecnológica de CLIENTE.
- Tramitar posibles cambios o ajustes en la arquitectura de la plataforma e infraestructura tecnológica de ALCALDIA , obtenida de los procesos y análisis que el oferente nos indique, y si se tiene recomendaciones por parte de los fabricantes se debe cumplir con las recomendaciones mediante plan de trabajo cumpliendo tiempos según la actividad.

2.1.2.6 ARQUITECTURA

La comunicación entre el colector ubicado en la red del cliente y el SOC de Password se realizará a través de internet por medio de túneles de VPN cifrados. Es necesario configurar tanto el firewall del lado del cliente como del lado del SOC de Password para establecer esta comunicación. Se requiere habilitar una conexión VPN Site to Site.



2.1.2.7 IMPLEMENTACION DEL SERVICIO

Para la implementación y puesta en marcha de la operación del servicio nos seguimos bajo el siguiente cronograma:

Instalación	5 días calendario después de la adjudicación
Configuracion	5 días calendario después de la instalación
Puesta en Marcha	5 días calendario después de la configuración

Los pasos para la implementación serán las siguientes:
Reunión inicial – La reunión se realizará a más tardar 10 días calendario después de la adjudicación, ya sea de forma física o a través de medios tecnológicos y se debe establecer lo siguiente:

- Dispositivos/equipos a instalar
- Ubicación física o lógica de la herramienta – En infraestructura del Cliente
- Ubicación de repositorios de los informes- En infraestructura del Cliente
- Ubicación de repositorios de eventos- En infraestructura del Cliente

- Cronograma de implementación
- Equipo humano que va a realizar la implementación

2.1.2.8 ACUERDOS DE NIVELES DE SERVICIO

	NIVEL DE CRITICIDAD		
	Alta	Media	Baja
Gestión de eventos (7x24) *Notificación de Alarma	2 horas	4 a 6 Horas	8 a 24 Horas

* Todas las alertas con criticidad "Baja" serán reportadas en el informe mensual de servicio; si estas son reiterativas durante un periodo de tiempo especificado, serán reportadas al cliente en el tiempo mencionado en el cuadro.

*Se utilizará 30 Minutos para reportar el incidente.

2.1.2.9 SERVICIOS DE GESTION DE INCIDENTES DE SEGURIDAD.

Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.

Ante la detección de eventos de seguridad individuales o simultáneos que constituyan situaciones potenciales de violación a la seguridad de la información, se requiere adelantar actividades de análisis, contención y respuesta para controlar e impedir estos potenciales ataques. Para esto PASSWORD Dispondrá de una Bolsa de 20 HORAS para el apoyo a dichos incidentes.

Las actividades incluidas dentro de la gestión de los incidentes son:

- Definición de criticidad y catalogación de incidentes para que responda adecuadamente a los requerimientos.
- Coordinar las pruebas y ejecución de las acciones de respuesta a incidentes de seguridad, contención y recuperación junto con el equipo de

expertos de ALCALDIA , administradores de plataforma y terceros involucrados en el incidente.

- Al momento de darse un evento o incidente de nivel medio o alto, dentro de las recomendaciones debe presentarse un informe de resolución de fallas (Root cause analysis).

3. Duración del Servicio

Se estima como tiempo para el cumplimiento de las actividades y objetivos de la consultoría**, Maximo (2) meses** calendario

4. OFERTA TECNICA

A continuación, se establece el valor económico para Servicio.

ITEM	DESCRIPCION	VALOR UNITARIO	VALOR IVA	VALOR TOTAL
1	Diagnóstico y Planificación	$ 265.000.000	$ 50.350.000,00	$ 315.350.000,00
1.1	Actividades a Desarrollar			
	* Recolección y análisis de la información: levantamiento de la información para realizar el diagnóstico del SGSI.	$ 30.000.000	$ 5.700.000,00	$ 35.700.000,00
	* valoración y clasificación de los activos de información identificados	$ 30.000.000	$ 5.700.000,00	$ 35.700.000,00
	* En la identificación de las amenazas y vulnerabilidades a las que se encuentra expuesta la Entidad ejecutan pruebas de vulnerabilidad en un máximo de 500 activos	$ 90.000.000	$ 17.100.000,00	$ 107.100.000,00
1.2	Pruebas de Ingeniería Social	$ 85.000.000	$ 16.150.000	$ 101.150.000
	* Pruebas presenciales	$ 40.000.000	$ 7.600.000	$ 47.600.000
	* Pruebas no presenciales	$ 45.000.000	$ 8.550.000	$ 53.550.000
1.3	*---------Fake Mailing	$ 20.000.000	$ 3.800.000	$ 23.800.000
1.4	*--------Suplantación de un servicio web o intento de phishing	$ 25.000.000	$ 4.750.000,00	$ 29.750.000,00
1.5	Gestión de Riesgos de Seguridad de la Información.	$ 30.000.000	$ 5.700.000,00	$ 35.700.000,00
2	Implementación	$ 136.000.000	$ 25.840.000,00	$ 161.840.000,00

	* Crear, revisar y/o actualizar el Plan de contingencia y de continuidad del negocio (BCP), Análisis de impacto al negocio (BIA) y el Plan de recuperación de Desastres (DRP) con que cuenta la Alcaldía acorde con las necesidades de Alcaldía de Santiago de Cali	$ 25.000.000	$ 4.750.000,00	$ 29.750.000,00
	* Definir los indicadores adecuados para la medición del SGSI.	$ 20.000.000	$ 3.800.000,00	$ 23.800.000,00
	* Revisar la eficiencia, efectividad y eficacia del SGSI	$ 20.000.000	$ 3.800.000,00	$ 23.800.000,00
	* Revisión del tipo de información que genera la entidad y su esquematización frente a la Ley de transparencia. Análisis de los lineamientos expedido por MinTic para publicación de la información pública.	$ 25.000.000	$ 4.750.000,00	$ 29.750.000,00
	* Establecimiento de los lineamientos y condiciones sobre medios para recepción de solicitudes de información pública. Análisis de requisitos a formular para la atención ciudadana y condiciones de seguridad de la información.	$ 25.000.000	$ 4.750.000,00	$ 29.750.000,00
	* Análisis sobre información clasificada y reservada. Índice de información clasificada y reservada. Protocolo de etiquetado y clasificación de información.	$ 21.000.000	$ 3.990.000,00	$ 24.990.000,00
			$ -	$ -
3	Sensibilización y Capacitación	$ 60.000.000	$ 11.400.000,00	$ 71.400.000,00
	a) 1 Performance – representación teatral en la Entidad	$ 20.000.000	$ 3.800.000,00	$ 23.800.000,00
	b) 2 Talleres de sensibilización en temas de seguridad	$ 20.000.000	$ 3.800.000,00	$ 23.800.000,00
	c) 2 Conferencias con ayudas audiovisuales	$ 20.000.000	$ 3.800.000,00	$ 23.800.000,00
4	Suministro de herramienta de software para la gestión del SGSI	$ 231.260.000		$ 231.260.000,00
			$ -	$ -
5	CENTRO DE OPERACIÓN DE SEGURIDAD-CORRELACION DE EVENTOS	$ 185.000.000	$ 35.150.000,00	$ 220.150.000,00
	Total			$ 1.000.000.000,00

5. CONDICIONES COMERCIALES.

Alcance

La descripción técnica de la solución propuesta es el alcance de los servicios suministrados por - PASSWORD CONSULTING SERVICES S.A.S, todo aquello que no este escrito no hace parte del alcance de la presente propuesta y se da por entendido que es un nuevo alcance con un costo adicional.

Moneda de la Oferta

Esta propuesta económica se presenta en pesos colombianos (COP).

6. ACUERDO DE CONFIDENCIALIDAD

PASSWORD CONSULTING SERVICES, entrega este documento bajo la condición de confidencialidad mutua, donde las partes deben respetar las la información provista. Por lo tanto, la información aquí contenida no debe ser copiada o entregada a terceras personas.