



Tecnia
Security

CONTRATACION
M. LA OSPINA
C.C. 813.005.265-7

FECHA 02/01/2025
HORA 2:05 pm
IDENTIFICACION nm

Tecnia Security SAS

- Barranquilla, Colombia
- info@tecnica.com.co
- 316 523 8982

ACERCA DE NOSOTROS

Tecnia Security S.A.S. es una compañía que trabaja como una familia para ofrecer soluciones de hardware y software que permitan a nuestros clientes alcanzar sus objetivos.

Enfocamos nuestros esfuerzos en apoyar a nuestros clientes en sus necesidades de seguridad informática y administración IT.

Nuestro personal se encuentra en constante capacitación para brindar la asesoría adecuada y apoyar el desarrollo de sus colaboradores, logrando el cumplimiento de los objetivos de trabajo.

Ofrecemos soluciones para:

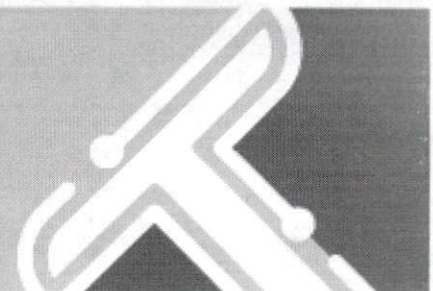
❖ Protección antivirus	❖ Cifrado de email, USB.
❖ Seguridad Perimetral	❖ Colaboración y correo electrónico.
❖ Prevención de fuga de datos	❖ Virtualización
❖ Backups de información	❖ Mesa de ayuda.
❖ Inventario de Hardware y software.	❖ Firewall de aplicaciones
❖ Servidores Rack, Blade	❖ Seguridad electrónica y CCTV

Somos Partner Autorizado de las soluciones que ofrecemos, tenemos presencia en las ciudades de Barranquilla y Medellín. Contamos con más de 150 clientes en todo el país.

La tranquilidad que te brinda la tecnología.

- Tecnia Security te brinda la tranquilidad de estar preparado para enfrentar un ataque informático y resolverlo con éxito.

Te brindamos
la **tranquilidad**
que necesita tu
empresa.



CONDICIONES COMERCIALES

Tiempo de entrega: 30 días hábiles después de recibido el respectivo anticipo y orden de compra.
O anticipo sujeto a disponibilidad.

Bancolombia cuenta ahorros N. 769-175225-26

Si no es cliente de la empresa por favor realizar el registro a la importación de equipos comenzará a partir de la fecha de consignación del anticipo, la importación de los equipos se estima en 30 días calendario, aunque este tiempo podría reducirse aproximadamente en 20 días calendario.

La instalación del equipo tiene una duración aproximada de 15 a 30 días hábiles debido a afinación de políticas.

Capacitaciones adicionales al incluido en la oferta tendrán costo adicional.

Todo servicio técnico será prestado siempre y cuando el cliente reporte el mismo a través de nuestra mesa de servicio en nuestra página web (<https://www.tecniasecurity.com>) dando click en la pestaña soporte.

El tiempo de atención será en las siguientes 4 horas después de asignado el ticket teniendo en cuenta las horas hábiles de atención de lunes a viernes de 8:00 am a 12:00pm y de 2:00pm a 6:00 pm y los sábados de 9:am a 1:00pm. El soporte remoto se puede llegar a prestar incluso de forma inmediata siempre y cuando se haya creado el ticket y contemos con disponibilidad inmediata de nuestro personal técnico. Para la atención presencial en el área metropolitana de Barranquilla se realizará 4 horas después de ser realizado el soporte remoto o telefónico de primer nivel. Otras ciudades aplican tiempos diferentes de acuerdo con su ubicación.

Servicios con costo: Nuevas configuraciones o cambios en las establecidas en la configuración inicial del equipo, actualizaciones de Firmware, Capacitaciones adicionales a las realizadas con la entrega del equipo, Reinicio de equipo, cambio de ubicaciones, servicios técnicos de red o conectividad que no sean ocasionados por Sophos. EL CONTRATISTA puede realizar estos servicios bajo un contrato de administración adicional.



PROPUESTA ECONOMICA SOPHOS CENTRAL

DETALLE	CANTIDAD	V/UNIDAD	V/ FINAL
<i>Sophos Central Intercept X Advanced antivirus estaciones de trabajo + 12 servidores</i>	512	\$140.000	\$71.680.000
TOTAL, EXENTO DE IVA			\$71.680.000

IMPLEMENTACIÓN

DETALLE	CANTIDAD	V/UNIDAD	V/ FINAL
<i>Bolsa de soporte técnico en horario 5*8.</i>			
<i>Instalación, configuración y puesta en marcha de la solución de forma remota.</i>	50	\$120.000	\$ 6.000.000
TOTAL, EXENTO DE IVA			\$6.000.000

Notas: Observaciones Generales de la Oferta

Validez: 30 días fecha factura.

Valores en pesos.

Forma de pago, Contado.

Tiempo de entrega, 15 días hábiles.

Te brindamos
la **tranquilidad**
que necesita tu
empresa.



TIEMPO DE EJECUCION

Se realiza la apertura oficial del proceso de implementación del Servicio o producto con la aceptación formal del CLIENTE, mediante orden de compra o firma de contrato entre las dos partes. El CONTRATISTA acepta como válida, por solicitud expresa del CLIENTE, una comunicación formal de aceptación de la Oferta Comercial, donde se debe especificar fecha de la Oferta, valor y tiempo de entrega. Este documento también debe tener validez para realizar el proceso de facturación. Aceptación de la Oferta Comercial a través de correo electrónico solo aplica para servicios profesionales.

A partir de la aprobación formal de esta Oferta, EL CONTRATISTA requerirá de 5 días hábiles para el inicio de las actividades a través de una reunión o teleconferencia para formalizar el inicio de la implementación, tiempo durante el cual se asignará el equipo de trabajo y se realizarán las actividades de planificación necesarias para la adecuada gestión. Teniendo en cuenta nuestra experiencia y lecciones aprendidas producto de nuestras anteriores implementaciones, ofrecemos flexibilidad en el tiempo de entrega puesto que este será acorde a las necesidades del cliente en el tiempo y según la disponibilidad de sus recursos.

Te brindamos
la **tranquilidad**
que necesita tu
empresa.



EXCLUSIONES Y GARANTIA

Garantías y recursos.

- (i) Software. Sophos garantiza que cada versión del Software funcionará de una manera sustancialmente conforme con lo descrito en la correspondiente documentación del Producto durante un año a partir de la fecha en que el Cliente obtenga la primera licencia para dicha versión. Si no funciona así y el Cliente lo notifica a Sophos dentro del período de garantía, entonces Sophos deberá a su criterio elegir entre (1) devolver el precio que haya pagado el Cliente por la licencia del Software o (2) reparar o sustituir el Software.
- (ii) Servicios Online. Sophos garantiza que cada Servicio Online funcionará de acuerdo con el SLA aplicable durante el uso que haga el Cliente. Los recursos del Cliente en caso de incumplimiento de esta garantía se especifican en el SLA.

Los únicos recursos de que dispone el Cliente ante un incumplimiento de las garantías son los indicados anteriormente en esta sección. El Cliente renuncia a cualquier reclamación por incumplimiento de garantías que no se realice durante el período de garantía.

Exclusiones. Las garantías otorgadas en la presente Propuesta no se aplican a los problemas causados por accidente, abuso o uso de un modo incompatible con esta Propuesta, incluido el incumplimiento de los requisitos mínimos de sistema. Estas garantías no se aplican a productos gratuitos, de prueba, preliminares o beta, ni a los componentes de los Productos que el Cliente tenga permiso para redistribuir. c. Exclusión de Responsabilidad. Excepto por las garantías limitadas anteriores, el Fabricante no ofrece ninguna otra garantía o condición y excluye cualquier otra garantía explícita, implícita o legal, incluidas las garantías de calidad, titularidad, ausencia de infracción de derechos, comerciabilidad e idoneidad para un fin particular.

Te brindamos
la **tranquilidad**
que necesita tu
empresa.



METODOLOGIA E IMPLEMENTACION

EL CONTRATISTA Propone una metodología de implementación progresiva que se llevara a cabo de la siguiente forma:

Preparación

- Reunión de Inicio con Cliente
- Documentos, Plan de trabajo.
- Conocimiento de necesidades

Parametrización

- Reunión de conocimiento del sistema
- Definición de reglas, configuraciones Posibles de la herramienta

Implementación

- Capacitación e implementación
- Asistencia y acompañamiento continuo

Cierre

- Capacitación técnica
- Entrega de servicios o productos.

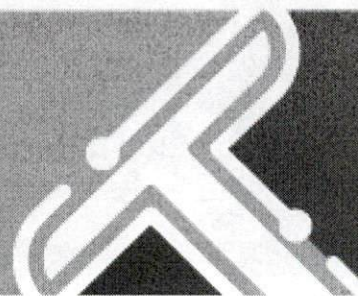
Te brindamos
la **tranquilidad**
que necesita tu
empresa.



Este servicio maneja 3 niveles diferentes:

	Sophos Threat Advisor	Sophos MDR	Sophos MDR Complete
Supervisión y respuesta a amenazas 24/7 a cargo de expertos	✓	✓	✓
Compatible con productos de seguridad de otros proveedores	✓	✓	✓
Informes semanales y mensuales	✓	✓	✓
Sesión informativa mensual: "Sophos MDR ThreatCast"	✓	✓	✓
Función Comprobar la cuenta de Sophos		✓	✓
Búsqueda de amenazas a cargo de expertos		✓	✓
Contención de amenazas: se interrumpen los ataques y se impide su propagación <small>Utiliza el agente Sophos XDR completo (protección, detección y respuesta) o Sophos XDR Sensor (detección y respuesta)</small>		✓	✓
Soporte telefónico directo durante incidentes activos		✓	✓
Respuesta a incidentes integral: se eliminan las amenazas por completo <small>Requiere el agente Sophos XDR completo (protección, detección y respuesta)</small>			✓
Análisis de causa raíz			✓
Responsable de respuesta a incidentes dedicado			✓
Breach Protection Warranty <small>Cubre hasta 1 millón USD en gastos de respuesta</small>			✓

Te brindamos
la **tranquilidad**
que necesita tu
empresa.



¿Que incluye?

La siguiente tabla contiene un resumen de los beneficios que se obtienen al adquirir XDR:

	Detección y respuesta ampliadas (XDR)
Fuentes de datos entre productos	✓
Detección, investigación y respuesta entre productos	✓
Lista de detecciones priorizada e investigaciones guiadas por IA	✓
Sophos Data Lake	✓
Periodo de retención de Data Lake	30 días
Información del estado en tiempo real	✓
Periodo de retención de datos en disco	Hasta 90 días
Biblioteca de plantillas de operaciones de TI y búsqueda de amenazas	✓
Capacidades de protección en Intercept X	✓

- MDR

Es un servicio 24/7 totalmente gestionado prestado por expertos de Sophos que detectan y responden a ciberataques dirigidos contra sus ordenadores, servidores, redes, cargas de trabajo en la nube, cuentas de correo electrónico y más.

Te brindamos
la **tranquilidad**
que necesita tu
empresa.



La siguiente tabla provee un resumen de la funcionalidad de Sophos Email Security:

Funciones de protección	Email Advanced	Funciones de protección	Email Advanced
Reglas de flujo de correo de Microsoft 365	✓	Análisis del nombre mostrado	✓
Protección posentrega para Microsoft 365	✓	Comprobaciones de dominios de imitación	✓
Escaneado de malware y antispam	✓	Políticas DLP de múltiples reglas	✓
Espacio seguro en la nube	✓	Listas de control del contenido	✓
Detección de URL maliciosas	✓	Cifrado TLS impuesto	✓
Reescritura de direcciones URL en el momento del clic	✓	S/MIME	✓
SPF, DKIM, DMARC	✓	Cifrado basado en imposición	✓
Protección contra phishing de suplantación de identidad	✓	Cifrado basado en extracción	Complemento

Detección y Respuesta Extendida (XDR) y Gestión de Detección y Respuesta (MDR)

Son servicios que permiten recopilar y correlacionar datos de diferentes superficies de ataque, de forma proactiva.

- XDR

Le permite obtener una visión holística del entorno de su organización con conjuntos de datos exhaustivos y un análisis profundo para la detección, investigación y respuesta a las amenazas, tanto para los equipos SOC dedicados como para los administradores de TI.



- Reducción del riesgo de filtraciones de datos con tecnologías de borrado remoto y antirrobo.
- Forzar el cumplimiento de las políticas corporativas: establecer requisitos para las contraseñas, prohibir el jailbreak y muchas más.
- Gestione fácilmente el inventario de dispositivos y las políticas desde la misma consola que utiliza para las estaciones de trabajo.

Control de aplicaciones

Política flexible basada en el usuario para el control de contenido descargable, incluidos tipos de archivos y contenido dinámico a través de FTP, HTTP o HTTPS.

Las plantillas de filtrado de contenido le permiten controlar cientos de diferentes tipos de archivos, ejecutables y contenido dinámico fácilmente como parte de cualquier política de control web de usuarios o de la red.

Cree definiciones de tipos de contenido fácilmente añadiéndolas a categorías de filtrado de contenido existentes o a sus propias categorías personalizadas.

Las opciones de escaneo de contenido le permiten personalizar cuándo y cómo se escanea el contenido con opciones de tamaño y escaneo en tiempo real o en modo de lote.

El almacenamiento web en caché reduce el consumo de ancho de banda almacenando en la caché el contenido web y las descargas admitidas, incluidas las actualizaciones de Sophos Endpoint.

Seguridad de correo electrónico

Con Sophos Email Security integrado a su proveedor de correo, usted puede confiar que la bandeja de entrada de los usuarios y su información crítica esté protegida contra todo tipo de malware.

Con esta herramienta, usted garantiza lo siguiente:

- Integración con proveedores de correo electrónico corporativo: Microsoft 365, Gmail de Google Workspace y otros.
- Seguridad del correo electrónico basada en API para Microsoft 365 con protección post-entrega.
- Detener spam, malware, ransomware y URL maliciosas.
- Bloquear el phishing sin malware y los intentos de suplantación de identidad.
- Proteger los datos confidenciales con el cifrado del correo electrónico y la prevención de pérdida de datos.

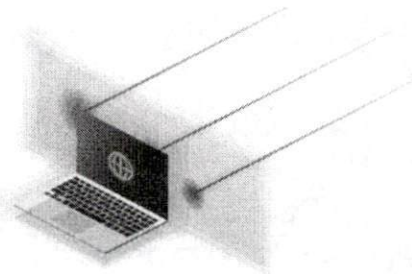
Te brindamos
la **tranquilidad**
que necesita tu
empresa.



Reduzca la exposición con control web y seguridad web

La web es uno de los vectores de infecciones más comunes para los dispositivos de usuario final. Sophos Central protege a sus usuarios con seguridad web integrada. Además, la política de control web facilita la tarea de asegurarse de que se hace un uso seguro y productivo de la web, independientemente de si sus usuarios se encuentran en el trabajo, en casa o mientras viajan.

- Bloquea automáticamente el acceso a sitios web maliciosos.
- Haga cumplir sin esfuerzo la política de Internet en la estación de trabajo: sin necesidad de servidores proxy, VPN o configuración específica de aplicaciones

Protección de servidores de alto rendimiento

Sophos Server Protection protege su entorno de servidor frente al malware, al mismo tiempo que mantiene el rendimiento de sus servidores al máximo. Además, reconoce automáticamente aplicaciones de servidor populares y adapta la configuración automáticamente. Detecta y bloquea virus, troyanos, rootkits y otro malware conocido y de día cero, para que sus servidores y datos permanezcan seguros.

- Se adapta automáticamente a su entorno de servidor.
- Protección diseñada para servidores con exclusiones automáticas.
- Optimizado para la protección y el rendimiento.

Gestión de dispositivos móviles

Sophos Mobile permite gestionar la seguridad de sus dispositivos móviles. Sus teletrabajadores pueden seguir siendo productivos y mantener sus datos corporativos seguros al mismo tiempo, incluso en movimiento.

Te brindamos
la **tranquilidad**
que necesita tu
empresa.



Seguridad integrada para Windows, Mac y móviles



Sophos es la única solución de seguridad integrada que protege a dispositivos Windows, Mac y dispositivos móviles. Una experiencia de usuario sencilla e intuitiva hace que Sophos sea fácil de implementar, administrar y mantener.

No es necesario instalar ningún servidor y la consola de administración está alojada en la nube. Tendrá todo en funcionamiento en tan sólo 60 segundos.

También permite usar directorio activo para un rápido despliegue y gestión continua de usuarios y grupos.

Tecnología de protección probada

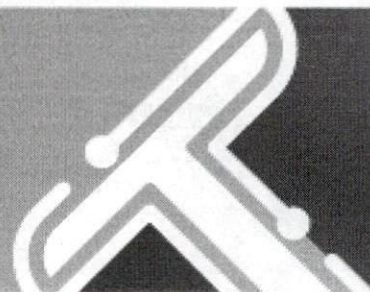
Sophos protege a más de 100 millones de dispositivos en todo el mundo, por medio de su tecnología de inteligencia artificial "Deep learning", la cual verifica el comportamiento en tiempo de ejecución del código malicioso.

Maneja capas de protección para detener los programas maliciosos: detección de vulnerabilidades web, HIPS, protección contra desbordamientos de búfer y más.

Reduce la superficie expuesta a ataques mediante el control o la restricción del acceso a los dispositivos extraíbles.

Mantiene actualizada automática y periódicamente la protección para sus dispositivos, mediante políticas de actualización,

Te brindamos
la **tranquilidad**
que necesita tu
empresa.



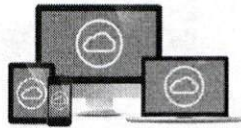
SERVICIOS Y FUNCIONALIDADES



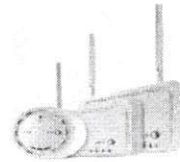
Sophos ofrece un completo portafolio de seguridad que le ayuda en todos los puntos de la red. Las tecnologías de Sophos permiten que su compañía cuente con seguridad sincronizada.



Firewall de nueva generación para la protección Perimetral



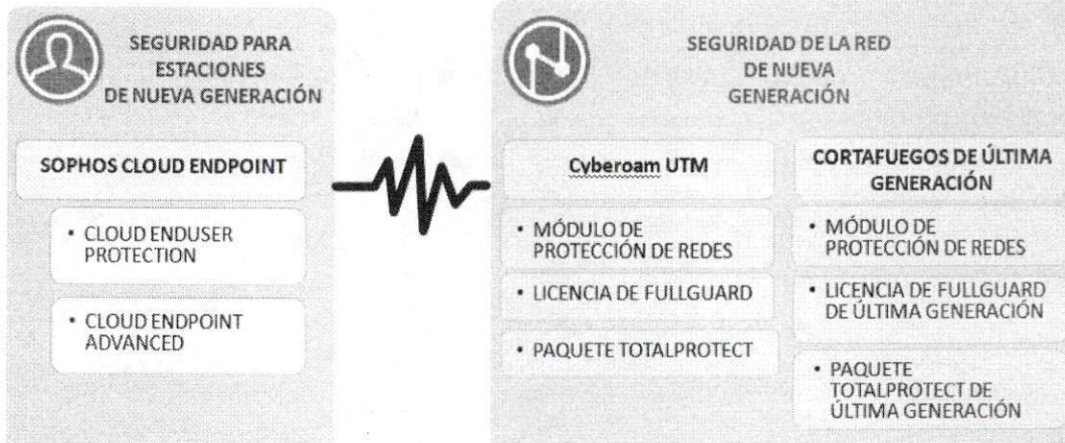
Protección endpoint en la nube



Conexiones WIFI de alto nivel y seguras



Cifrado de los datos



Te brindamos la **tranquilidad** que necesita tu empresa.



Barranquilla, 02 de enero de 2025


Señores
HOSPITAL CARMEN EMILIA HOSPINA
Barranquilla

Referencia: Solución **SOPHOS SEGURIDAD SINCRONIZADA**

TECNIA SECURITY SAS, partner autorizado (en adelante llamado "EL CONTRATISTA"), quiere poner a su disposición la propuesta de servicios, según su requerimiento específico, **SOPHOS CENTRAL**.

Cualquier inquietud no dude en comunicarse.

Cordialmente


Nombre del Ejecutivo
JUAN MIGUEL VIZCAINO
TEL. 3601450 – 3517078

Te brindamos
la **tranquilidad**
que necesita tu
empresa.



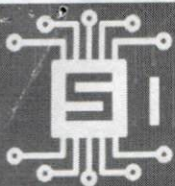
- Imagínate disponer de un equipo con profesionales de gran experiencia, centrados en aplicar la tecnología para mejorar los procesos y la productividad de tu empresa. Imagínate tener tiempo para gestionar tu negocio porque puedes confiar tu seguridad y tecnología a un profesional sólido, innovador y fiable.
- Tecnia Security está permanentemente formándose y actualizándose para ofrecer siempre, la tecnología más actual, confiable, y las soluciones más innovadoras para tu negocio, sin importar el tamaño de este. La calidad de nuestro servicio es nuestra ganancia.

Problemas: El tiempo y el conocimiento.

Gestionar la seguridad informática de su empresa requiere que usted pueda analizar, investigar y resolver las incidencias. Para hacerlo, necesita conocimiento avanzado en seguridad informática. Nuestro equipo técnico le brinda este conocimiento para que usted pueda concentrarse en las actividades más importantes del core de su negocio.

Te brindamos
la **tranquilidad**
que necesita tu
empresa.





SITE SECURITY
Soluciones Inteligentes



Sophos
Gold
Partner

Pereira, Enero 02 de 2025

Señores
ESE CARMEN EMILIA HOSPINA
Atte. Doctor, JULIO CÉSAR QUINTERO VIEDA
La ciudad

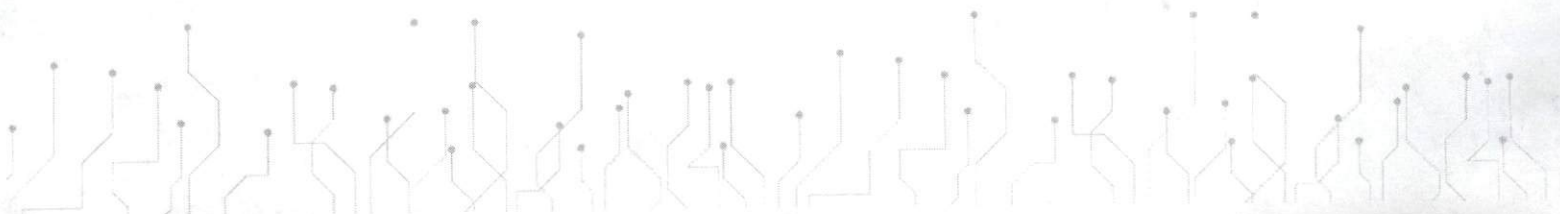
CONTRATACION
CARMEN EMILIA OSPINA
NIT. 813.005.265-7
FECHA 02/01/2025
HORA 11:00 am
INDICACION RVA

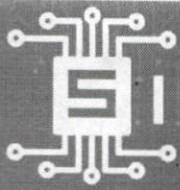
Agradecemos el interés de su distinguida organización en nuestras soluciones de punto final como lo es la solución de Antivirus Corporativo orientado a la protección de punto final y servidores.

En atención a su solicitud, y siguiendo los requerimientos del proceso de adquisición de Solución de Antivirus Corporativa, anexo a la presente la propuesta de diseño e implementación de Sophos Intercept X Advanced with XDR.

Atentamente,

Gerente Comercial
Móvil 318-2453289
Email: nidia.ramos@sitsec.com.co





SITE SECURITY

Soluciones Inteligentes



Sophos
Gold
Partner

SERVICIOS PROFESIONALES

Seguridad Sincronizada Sophos

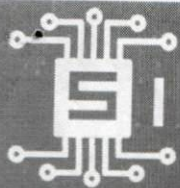
CONFIDENCIALIDAD DE LA PROPUESTA DE SERVICIOS PROFESIONALES

Esta propuesta de Servicios Profesionales es confidencial. Está disponible solo para ESE CARMEN EMILIA HOSPINA OSPINA en el entendimiento de que la información aquí descrita no será divulgada a personas diferentes a las definidas por el cliente para su evaluación, ni será utilizada para propósitos diferentes a los que motivaron su solicitud y preparación, sin consentimiento explícito de SITE SECURITY S.A.S.

Este documento ha sido preparado para ESE CARMEN EMILIA HOSPINA OSPINA y se mantendrá su propiedad hasta el momento en que se perfeccione un contrato formal para desarrollar la prestación del servicio. Por esta razón, el contenido del documento no podrá ser revelado por ESE CARMEN EMILIA HOSPINA OSPINA.

Política de Tratamiento de Datos Personales | Site Security

<https://www.sitsec.com.co/politica-de-tratamiento-de-datos-personales>

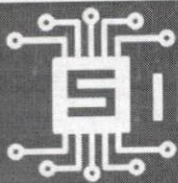


PROPUESTA ECONÓMICA DE RENOVACIÓN SOPHOS CENTRAL

DETALLE	Cantidad	V/ Unidad	Valor total
Central Intercept X Advanced estaciones de trabajo 12 MOS	500	\$102.000	\$51.000.000
Central Intercept X Advanced for Server 12 MOS	12	\$250.000	\$3.000.000
Soporte técnico especializado 5*8 remoto, Instalación, configuración y puesta en marcha de la solución; por un ingeniero certificado Architect de Sophos.	1	0	0
Capacitación: Para máximo 3 personas del área de TI por un ingeniero certificado Architect de Sophos.	1	0	0
Soporte posventa; Bolsa de (100) horas de soporte técnico especializado de forma, remota durante el tiempo de vigencia de la solución en horario 5*8.	100	0	0
Bolsa de (10) horas soporte técnico especializado en horario 7*24 para incidentes de alto impacto.	10	0	0
Dos (2) Voucher para certificación Sophos Central Engineer	2	0	0
Entrega de informe mensualizado del monitoreo y estado de la consola.	12	0	0
VALOR TOTAL, EXENTO DE IVA			\$54.000.000

CONDICIONES COMERCIALES

- Valores en pesos exento de IVA.
- Tiempo de entrega, 8 días hábiles.
- Vigencia de la propuesta, 15 días.
- **Forma de pago, Contado.**



SOPORTE Y ATENCIÓN AL CLIENTE

El soporte y atención será dividida en tres (3) niveles, a saber:

- **Primer nivel:** será responsabilidad del administrador (cliente).
- **Segundo Nivel:** estará a cargo de SITE SECURITY, Includido: instalación configuración transferencia de conocimiento atención inicial de forma remota 5*8.
- **Capacitación:** Para máximo 3 personas del área de TI por un ingeniero certificado Architect de Sophos.
- Soporte posventa; Bolsa de (10) horas de soporte técnico horario 7*24 para incidentes de alto impacto.
- Soporte posventa; Bolsa de (100) horas de soporte técnico especializado de forma, remota durante el tiempo de vigencia de la solución en horario 5*8.
- **Tercer Nivel:** será responsabilidad de SITE SECURITY, establecer el canal remoto necesario con el fabricante.
- Entrega de informe mensualizado del monitoreo y estado de la consola.

MESA DE AYUDA

Las solicitudes de soporte técnico deben ser solicitadas a través de la plataforma Helpdesk, con el fin de realizar un seguimiento de las tareas de los agentes de TI, verificar el estado de los proyectos y tener una visión general de la actividad del soporte; para solicitar el acceso a la plataforma se debe escribir al correo electrónico ingenieria@sitsec.com.co; después de solicitar el acceso se le enviará usuario y contraseña para acceder a la plataforma.

REGISTRACION CORRESPONDENCIA
Estado de Risaralda
Carmen Emilia Ospina
C.I. 813.005.265-7
CONTRATACION
FECHA 02/01/2025
HORA 11:54 am
INFORMACION _____
RECIBO WJA



PROPUESTA DE IMPLEMENTACIÓN SOPHOS CENTRAL

ESE CARMEN EMILIA OSPINA





AVISO 4
TODOS LOS DIAS
INBIT
Technology S.A.S

Pereira, 02 de enero de 2025

Señores
HOSPITAL ESE CARMEN EMILIA OSPINA
Neiva Huila

COTIZACIÓN N°33

Cordial Saludo

Presentamos a usted nuestra propuesta comercial, manifestando nuestro gran interés en ser el socio estratégico en la creación de valor para su empresa, a través del diseño y la implementación de soluciones de comunicación y colaboración, a la medida de sus requerimientos y recursos.

Nuestro factor diferenciador está en la calificación de nuestro personal, en su mayoría certificados por casas fabricantes de Software, Hardware, de la industria y por entidades que garantizan buenas prácticas a nivel de proyectos y servicios para poder así ayudar a nuestros clientes a ser más competitivos alineando sus objetivos tecnológicos con las estrategias organizacionales de sus compañías.

Quedamos muy atentos a sus comentarios.

Cordialmente,

Héctor David Marín Velasco
Gerente General
Cel 3114905705

gerencia@inbit.com.co



+57 3114905705



Pereira, Risaralda





INBIT
Technology S.A.S

¿POR QUÉ SOPHOS?

Con el respaldo de la información sobre amenazas, la IA y el Machine Learning de SophosLabs y SophosAI, Sophos ofrece una amplia cartera de productos y servicios avanzados para proteger a usuarios, redes y endpoints contra el ransomware, malware, exploits, phishing y otros muchos tipos de ciberataques. Sophos proporciona una única consola integrada de administración basada en la nube, Sophos Central, el eje central de un ecosistema de ciberseguridad adaptativa que incluye un Data Lake centralizado que se sirve de un completo conjunto de API abiertas disponibles para clientes, partners, desarrolladores y otros proveedores de soluciones de ciberseguridad. Sophos vende sus productos y servicios a través de partners distribuidores y proveedores de servicios administrados (MSP) de todo el mundo.

Sophos como solución de ciberseguridad protección unificada por medio de:

- Firewall XGS.
- Endpoint Protection.
- Device Encryption.
- Access Point.
- Mobile.
- Email Security.
- Phish Threat.
- Cloud Optix
- Switches.
- ZTNA.

INBIT
Technology

+57 3114905705



gerencia@inbit.com.co

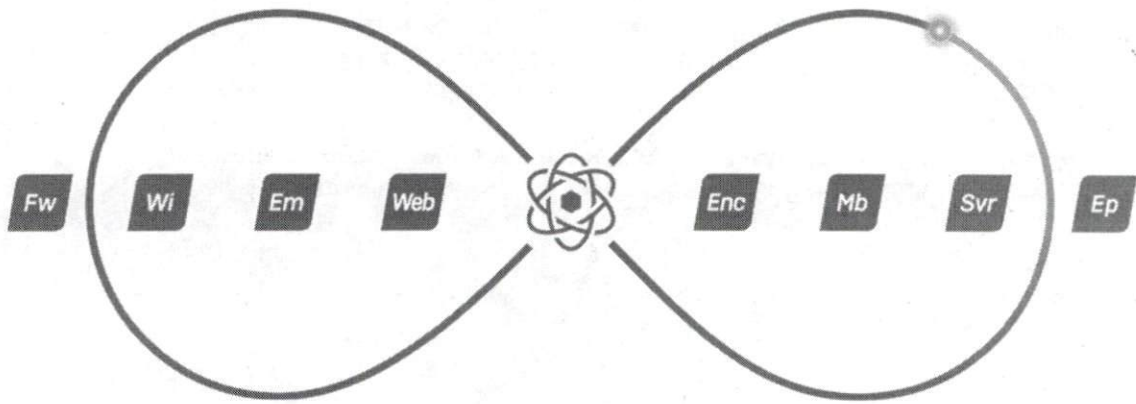


Pereira, Risaralda





INBIT
Technology S.A.S



Seguridad Sincronizada

Las soluciones de Sophos funcionan mejor de forma conjunta. Por ejemplo, Intercept X y Sophos Firewall se coordinan para identificar, aislar y limpiar los dispositivos que se hayan visto comprometidos. Cuando la amenaza queda neutralizada y no hay riesgo de propagación lateral, se restablece la conectividad de red. Todo esto sucede de manera automática sin que sea necesaria la intervención de ningún administrador.

+57 3114905705

gerencia@inbit.com.co

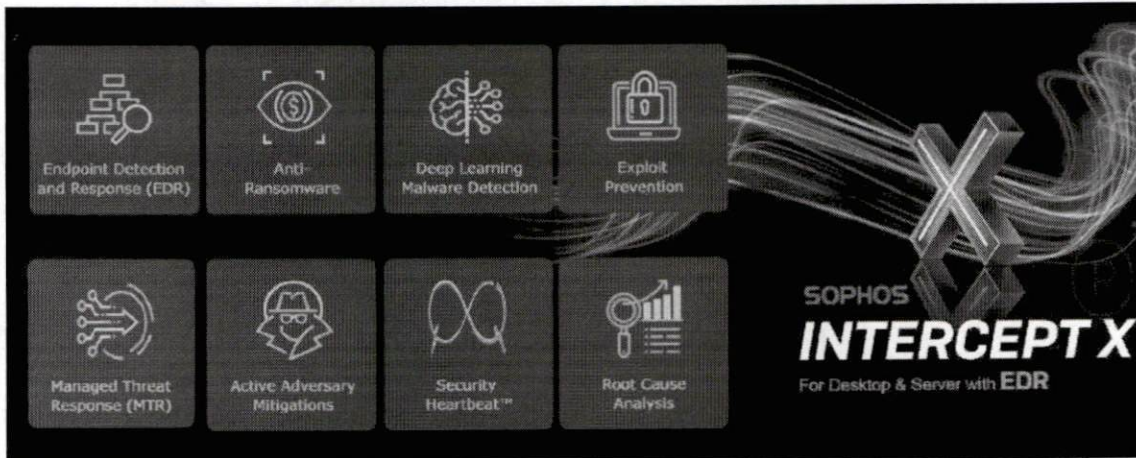


Pereira, Risaralda





INBIT
Technology S.A.S



Implementación de plataforma Cloud de Sophos Central, implementación en estaciones de trabajo.

Se realizará configuración de políticas de seguridad y realizando ajustes de seguridad para brindar la mejor protección

Se iniciará la corrección de errores y advertencias críticas de las estaciones de trabajo, donde se estabilizará el estado de los dispositivos conectados a Sophos Central.

Se realizará ajuste de grupos de usuarios y equipos los cuales me permitan ejecutar perfectamente las políticas de seguridad a los equipos indicados, teniendo la mejor distribución y orden en la plataforma Sophos Central.

Se realizará sincronización con Sophos XGS, realizando pruebas de funcionamiento e implementando la seguridad sincronizada avanzada entre dispositivo de perímetro y agente Endpoint.

Se realizará capacitación virtual de 4 horas por parte de ingeniería certificada en la solución para un grupo máximo de 4 personas técnicas, las cuales obtendrán los conocimientos básicos de la administración, funcionamiento y configuración de la solución.

gerencia@inbit.com.co



+57 3114905705



Pereira, Risaralda





INBIT
Technology S.A.S

COTIZACIÓN SOPHOS ENDPOINT

PRODUCTO	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
Intercept x advanced estaciones de trabajo	500	\$145.000	\$72.500.000
Intercept x advanced Servidores	12	\$290.000	\$3.480.000
VALOR TOTAL, EN PESOS EXENTO DE IVA			\$75.980.000

CONDICIONES COMERCIALES

- Validez de la Cotización veinte (20) días a partir de la presente fecha de emisión.
- Valores en pesos exento de IVA.
- Facturar a la TRM vigente a la entrega de las licencias.
- Tiempo de entrega, 30 días hábiles.
- Forma de pago, Contado.

IMPLEMENTACIÓN, SOPORTE Y ATENCIÓN AL CLIENTE

El soporte y atención será dividida en tres (3) niveles, a saber:
Primer nivel: será responsabilidad del administrador (cliente)
Segundo Nivel: estará a cargo de INBIT Technology.
Tercer Nivel: Fabricante.

