Código 1600
GDCHO 01-06-26-0338

Señores.
INFORTEC.
Nit: 900991717-8
Correo electronico: gerentedecuenta2@infortec.co
Ciudad.

ASUNTO: Solicitud de cotización para licenciamiento Microsoft 365, servicios de migración y soporte

Cordial saludo,

La Gobernación del Chocó, en el marco de su estrategia de fortalecimiento institucional y transformación digital, se encuentra adelantando acciones orientadas al robustecimiento de su plataforma tecnológica y de su esquema de seguridad informática institucional.

En ese sentido, la Entidad requiere contratar un proveedor especializado que "*suministre los servicios de renovación de licencias de antivirus ESET Endpoint Security y del firewall Palo Alto Networks PA-440, incluyendo los servicios asociados de actualización, soporte técnico especializado y asistencia técnica*", con el propósito de garantizar la continuidad operativa, la protección de los activos de información y el fortalecimiento de los controles de seguridad y privacidad de la información institucional.

Lo anterior, en cumplimiento de los lineamientos, planes, políticas y metas establecidas dentro del proceso de Gestión TIC de la Gobernación del Chocó, así como de las directrices relacionadas con seguridad digital, continuidad operativa y protección de la infraestructura tecnológica institucional por el termino de doce (12) meses.

En ese sentido, se invita a presentar una propuesta técnica y económica conforme a los requerimientos descritos a continuación:

<table>
<tr><th>ÍTEM</th><th>ESPECIFICACIONES TÉCNICAS</th><th>CANTIDAD</th><th>V/R UNITARIO</th><th>VALOR TOTAL</th></tr>
<tr><td>1</td><td><u>LICENCIA PARA FIREWALL PALO ALTO NETWORKS PA 440.</u>
<table>
<tr><td>Especificación técnica</td><td>Características Mínimas</td></tr>
<tr><td>Tipo de Dispositivo</td><td>NGFW – Next Generation Firewall</td></tr>
<tr><td>Rendimiento de transacciones</td><td>3,0/2,4 Gb/s</td></tr>
<tr><td>Rendimiento en prevención de</td><td>0,9/1 Gb/s</td></tr>
</table></td><td>1</td><td></td><td></td></tr>
</table>

	amenazas			
	Rendimiento en transacciones IPsec – VPN	1,6 Gb/s		
	Número de sesiones	200.000		
	Capacidad de Almacenamiento	128 GB		
	Puertos 10/100/1000 RJ-45	8		
	Puertos de Gestión E/S	(1) puerto de gestión fuera de banda 10/100/1000, (1) puerto de consola RJ-45, (1) puerto USB, (1) puerto de consola micro-USB		
	Con soporte, actualización y asistencia técnica por 1 año.			
2	**LICENCIA ANTIVIRUS ESET ENDPOINT SECURITY.** La solución deberá ser compatible 100% con la solución PALO ALTO NETWORKS PA 440 y deberá integrarse de forma nativa con la misma. Permitir la gestión del cliente de seguridad de endpoint desde una consola central del fabricante. Compatible con los siguientes sistemas operativos: Microsoft Windows: 7 (32 y 64 bits), 8 (32 y 64 bits), 8.1 (32 y 64 bits), 10 (32 y 64 bits), 11 (64 bits); Microsoft Windows Server: 2012 o superior; Mac OS X: v10.8, v10.9, v10.10, v10.11; Linux: Ubuntu 16.04 o superior, CentOS 7.4 o superior. Garantizar el cumplimiento de las demás especificaciones técnicas requeridas. Con soporte, actualización y asistencia técnica por 1 año	120		
3	**LICENCIA ANTIVIRUS ESET ENDPOINT SECURITY PARA SERVIDORES.** La solución deberá ser compatible 100% con la solución PALO ALTO NETWORKS PA 440 y deberá integrarse de forma nativa con la misma. Permitir la gestión del cliente de seguridad de endpoint desde una consola central del fabricante. Compatible con los siguientes sistemas operativos:	3		

	Microsoft Windows: 7 (32 y 64 bits), 8 (32 y 64 bits), 8.1 (32 y 64 bits), 10 (32 y 64 bits), 11 (64 bits); Microsoft Windows Server: 2012 o superior; Mac OS X: v10.8, v10.9, v10.10, v10.11; Linux: Ubuntu 16.04 o superior, CentOS 7.4 o superior. Garantizar el cumplimiento de las demás especificaciones técnicas requeridas. Con soporte, actualización y asistencia técnica por 1 año			
			SUBTOTAL	
			IVA	
			TOTAL	

Nota: Los costos asociados a los servicios contemplados y cotizados, deberán tener presente los impuestos departamentales y demás deducciones de ley.

Atentamente,

HARLIN ANDRÉS CÓRDOBA CUESTA
Secretario de Planeación y Desarrollo Étnico Territorial
Gobernación del Chocó

Elaboró: Niber Antonio Mosquera – Abogado - Contratista	**Aprobó:** Harlin Andrés Córdoba Cuesta Secretario de Planeación y Desarrollo Étnico Territorial

Outlook

Solicitud cotizacion INFORTEC

Desde Secretaría de Planeación <infoplaneacion@choco.gov.co>
Fecha Lun 2026-06-01 11:36
Para Johana Lopez Baena <gerentedecuenta2@infortec.co>
CC HARLIN ANDRES CORDOBA CUESTA <HACORDOBA@choco.gov.co>; Jannie Yaneth Brand Ortiz <jybrand@choco.gov.co>; JOSE EICNNER BUENAÑOS MOSQUERA <JEBUENANOS@choco.gov.co>
CCO katy jhojana mena mosquera <msskaty2@hotmail.com>

1 archivo adjunto (340 KB)
Solicitud cotizaciòn Nro. INFORTEC.pdf;

Buen día

Por medio del presente envió solicitud cotización de servicios para lo pertinente.

Atentamente,

Secretaría de Planeación y Desarrollo Étnico Territorial
Gobernación del Chocó
Calle 31 con Carrera 1a Esquina - Edificio La Confianza Segundo Piso

Gobernación del **Chocó** | **Secretaría** de Planeación y Desarrollo Étnico Territorial

---

infortec
Especialistas en Ciberseguridad

OFERTA DE SOLUCIONES

¡ENFÓCATE EN TU NEGOCIO , DE LA PROTECCIÓN DE TU INFORMACIÓN DIGITAL NOS ENCARGAMOS NOSOTROS!

Nuestro Propósito

Ayudamos a los profesionales de TI a identificar y resolver sus problemas en materia de ciberseguridad.

Compartir conocimientos y conectar talentos hace parte de nuestra entrega de valor. Por que cada uno de nosotros tiene algo que aportar, promovemos la interacción y colaboración entre profesionales de TI.

GOBERNACIÓN DE CHOCÓ

icontec ISO 9001 SC-CER651123

IQNET CERTIFIED MANAGEMENT SYSTEM

RN Nro. 360-06-06

Pereira, 19 de junio de 2026

Señores:

GOBERNACIÓN DE CHOCÓ
Atte. Secretaría de Planeación y Desarrollo Étnico Territorial
La Ciudad

Cordial Saludo:

Es muy grato para nosotros, poner a su entera disposición nuestra organización.

INFORTEC es una compañía especializada en brindar soluciones de ciberseguridad para la protección de la información y la optimización de los recursos informáticos.

Más de 24 años de experiencia y un equipo humano especializado, nos permiten aportar a la construcción de las mejores alternativas para la protección de la información en los puntos críticos donde es accedida, mitigando el riesgo de que ésta sea vulnerada.

Las soluciones de INFORTEC están pensadas en una estrategia de seguridad completa y continua, ajustada a las necesidades de cada cliente, a la manera como fluye la información en el desarrollo de sus actividades y que sea fácilmente adaptable a las nuevas tendencias y riesgos que continuamente aparecen ya sea por la identificación de nuevas amenazas o por la implementación de nuevos servicios propios de la dinámica del negocio.

Agradecemos la oportunidad brindada permitiéndonos aportar, con nuestra experiencia, a la estrategia de su organización.

Atentamente,

Johana López Baena

Johana López Baena
Gerente de Cuenta Senior
Email: gerentedecuenta2@infortec.co
Cel. 318 8216640

infortec
Especialistas en Ciberseguridad

Propuesta Económica de Renovación Endpoint y Perímetro

<table>
<tr><th>DESCRIPCION</th><th>CANTIDAD</th><th>V/UNIDAD</th><th>V/TOTAL</th></tr>
<tr><td>LICENCIA PARA FIREWALL PALO ALTO NETWORKS PA 440
Licenciamiento y Servicios IVA Incluido

<table>
<tr><th>ESPECIFICACIÓN TÉCNICA</th><th>CARACTERÍSTICAS MÍNIMAS</th></tr>
<tr><td>Tipo de Dispositivo</td><td>NGFW – Next Generation Firewall</td></tr>
<tr><td>Rendimiento de transacciones</td><td>3,0/2,4 Gb/s</td></tr>
<tr><td>Rendimiento en prevención de amenazas</td><td>0,9/1 Gb/s</td></tr>
<tr><td>Rendimiento en transacciones IPsec – VPN</td><td>1,6 Gb/s</td></tr>
<tr><td>Número de sesiones</td><td>200.000</td></tr>
<tr><td>Capacidad de Almacenamiento</td><td>128 GB</td></tr>
<tr><td>Puertos 10/100/1000 RJ-45</td><td>8</td></tr>
<tr><td>Puertos de Gestión E/S</td><td>(1) puerto de gestión fuera de banda 10/100/1000, (1) puerto de consola RJ-45, (1) puerto USB, (1) puerto de consola micro-USB</td></tr>
</table>
Con soporte, actualización y asistencia técnica por 1 año.</td><td>1</td><td>$ 38.582.180</td><td>$ 38.582.180</td></tr>
<tr><td>LICENCIA ANTIVIRUS ESET ENDPOINT SECURITY
Licenciamiento exento de IVA
La solución deberá ser compatible 100% con la solución PALO ALTO NETWORKS PA 440 y deberá integrarse de forma nativa con la misma.
Permitir la gestión del cliente de seguridad de endpoint desde una consola central del fabricante.
Compatible con los siguientes sistemas operativos: Microsoft Windows: 7 (32 y 64 bits), 8 (32 y 64 bits), 8.1 (32 y 64 bits), 10 (32 y 64 bits), 11 (64 bits); Microsoft Windows Server: 2012 o superior; Mac OS X: v10.8, v10.9, v10.10, v10.11; Linux: Ubuntu 16.04 o superior, CentOS 7.4 o superior. Garantizar el cumplimiento de las demás especificaciones técnicas requeridas.
Con soporte, actualización y asistencia técnica por 1 año.</td><td>120</td><td>$ 182.800</td><td>$ 21.936.000</td></tr>
<tr><td>LICENCIA ANTIVIRUS ESET ENDPOINT SECURITY PARA SERVIDORES.
Licenciamiento exento de IVA
La solución deberá ser compatible 100% con la solución PALO ALTO NETWORKS PA 440 y deberá integrarse de forma nativa con la misma.
Permitir la gestión del cliente de seguridad de endpoint desde una consola central del fabricante.
Compatible con los siguientes sistemas operativos: Microsoft Windows: 7 (32 y 64 bits), 8 (32 y 64 bits), 8.1 (32 y 64 bits), 10 (32 y 64 bits), 11 (64 bits); Microsoft Windows Server: 2012 o superior; Mac OS X: v10.8, v10.9, v10.10, v10.11; Linux: Ubuntu 16.04 o superior, CentOS 7.4 o superior. Garantizar el cumplimiento de las demás especificaciones técnicas requeridas.
Con soporte, actualización y asistencia técnica por 1 año.</td><td>3</td><td>$ 182.800</td><td>$ 548.400</td></tr>
<tr><td colspan="3">VALOR TOTAL DE LA RENOVACION IVA E IMPUESTOS INCLUIDOS</td><td>$ 61.066.580</td></tr>
</table>

CONDICIONES TECNICAS

CONDICIONES TECNICAS PERIMETRO

Los componentes de los Módulos de Protección para el Dispositivo de Seguridad Perimetral NGFW (Next Generation Firewall / Cortafuegos de Nueva Generación) y funciones ATM (Advanced Threat Management/Gestión Avanzada de Amenazas), con el que cuenta la entidad debe incluir las siguientes funcionalidades:

- Incorporación de tecnología Machine Learning (ML) y automatización de las políticas.
- Identificación y categorización de aplicaciones en todos los puertos, en las 7 capas del modelo OSI.
- Control de aplicaciones.
- Detección y prevención avanzada de amenazas con servicios de seguridad actualizables en la nube. Esto incluye filtrado avanzado de URLs (Web) para asegurar un entorno seguro a los usuarios, sistema de prevención de intrusiones en el tráfico de red, detección y prevención de malware con análisis e inteligencia permanentemente actualizados basados en la nube, seguridad DNS en tiempo real basado en tecnología ML y funcionalidad SD-WAN.
- Reportes.
- Consola Central.
- Control de aplicaciones que permita priorizar el tráfico de red importante, como VoIP, a la vez que limitar o bloquear el tráfico no deseado como el streaming de medios. Incluso si no impone ninguna política de control de aplicaciones, debe saber qué aplicaciones están poniendo a su red y a su empresa en riesgo.
- Gestión, configuración y monitoreo centralizado a través de software en una interfaz de usuario unificada, que permita conocer detalles sobre el tráfico de red, amenazas, políticas, reportes generales y detallados de la actividad monitoreada, reportes basados en usuarios y grupos y no sólo basados en direcciones IP.
- Detección y prevención avanzada de amenazas con servicios de seguridad actualizables en la nube. Esto incluye filtrado avanzado de URLs (Web) para asegurar un entorno seguro a los usuarios, sistema de prevención de intrusiones en el tráfico de red, detección y prevención de malware con análisis e inteligencia permanentemente actualizados basados en la nube, seguridad DNS en tiempo real basado en tecnología ML y funcionalidad SD-WAN.
- Plataforma optimizada para análisis de contenido de aplicaciones en capa 7.
- Procesamiento e inspección de aplicaciones que utilicen HTTP/2.
- Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.
- Posibilidad de aumentar la visibilidad y la seguridad de todos los dispositivos, incluidos los dispositivos de IoT no gestionados, sin la necesidad de implementar sensores adicionales.
- Posibilidad de descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos
- Posibilidad de descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.
- Inclusión de un módulo de optimización de políticas, que identifique las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Este módulo deberá facilitar la migración de la política de Capa 4 a una política de Capa 7 a través de un wizard.
- Incorporación de tecnología Machine Learning (ML) en el núcleo del cortafuego, para proveer identificación y prevención de ataques desconocidos o nunca antes vistos. Uso de análisis de comportamiento para detectar dispositivos IoT para realizar nuevas políticas y recomendaciones. Automatización de las políticas y recomendaciones para ahorrar tiempo y reducir la posibilidad de errores humanos.
- Identificación y categorización de aplicaciones en todos los puertos, en las 7 capas del modelo OSI. Uso de las aplicaciones como base para establecer decisiones y políticas de control y bloquear archivos maliciosos o intentos de intrusión. Creación de reportes de uso de las aplicaciones para proveer mayor conocimiento sobre el tráfico de la red.

CONDICIONES TECNICAS

CONDICIONES TECNICAS ENDPOINT

LICENCIA ANTIVIRUS PARA ENDPOINT Y SERVIDORES
La solución deberá ser compatible 100% con la plataforma NGFW ofertada en el presente proceso y deberá integrarse de forma nativa con la misma.
Permitir la gestión del cliente de seguridad de endpoint desde una consola central del fabricante.
Compatible con los siguientes sistemas operativos:
Microsoft Windows: 8 (32 y 64 bits), 8.1 (32 y 64 bits), 10 (32 y 64 bits); Microsoft Windows Server: 2012 o superior; Mac OS X: v10.8, v10.9, v10.10, v10.11; Linux: Ubuntu 16.04 o superior, CentOS 7.4 o superior.

ESET PROTECT ADVANCED

características técnicas:
1. Consola de Administración
Administración centralizada desde consola web local o en la nube.
Gestión unificada de políticas de seguridad.
Monitoreo en tiempo real del estado de los equipos protegidos.
Generación de reportes ejecutivos y técnicos.
Despliegue remoto de agentes y soluciones de seguridad.
2. Protección de Endpoints
Protección antivirus y antimalware de última generación.
Detección proactiva mediante tecnologías de aprendizaje automático (Machine Learning).
Protección contra ransomware.
Control de dispositivos extraíbles (USB, discos externos, etc.).
Firewall personal.
Sistema de prevención de intrusiones basado en host (HIPS).
Protección contra ataques de red y explotación de vulnerabilidades.
3. Protección Avanzada Contra Amenazas
Servicio de sandboxing en la nube para análisis de archivos sospechosos.
Detección de amenazas de día cero (Zero-Day).
Análisis dinámico y reputacional de archivos.
4. Cifrado de Información
Cifrado completo de disco (Full Disk Encryption).
Administración centralizada de políticas de cifrado.
Compatibilidad con equipos Windows y macOS.
5. Protección de Servidores
Protección para servidores Windows y Linux.
Protección en tiempo real de archivos y procesos.
Exclusiones configurables para aplicaciones empresariales.
6. Protección de Dispositivos Móviles
Compatibilidad con dispositivos Android e iOS.
Administración centralizada de dispositivos móviles.
Aplicación de políticas de seguridad corporativa.
7. Compatibilidad
La solución deberá ser compatible, como mínimo, con:
Windows 10 y Windows 11.
Windows Server 2016, 2019, 2022 y superiores.macOS.
Linux (Ubuntu, Debian, Red Hat y derivados).
Entornos virtualizados y plataformas cloud públicas.
8. Requisitos de Infraestructura
Implementación en modalidad Cloud o On-Premise.
Acceso a Internet para actualizaciones y servicios de reputación.
Capacidad de escalamiento para crecimiento futuro de la infraestructura protegida.
9. Licenciamiento
Licenciamiento corporativo administrado desde una consola central.
Actualizaciones de firmas, motores de detección y funcionalidades incluidas durante toda la vigencia del contrato.
Soporte técnico del fabricante y/o partner autorizado.

Condiciones Comerciales

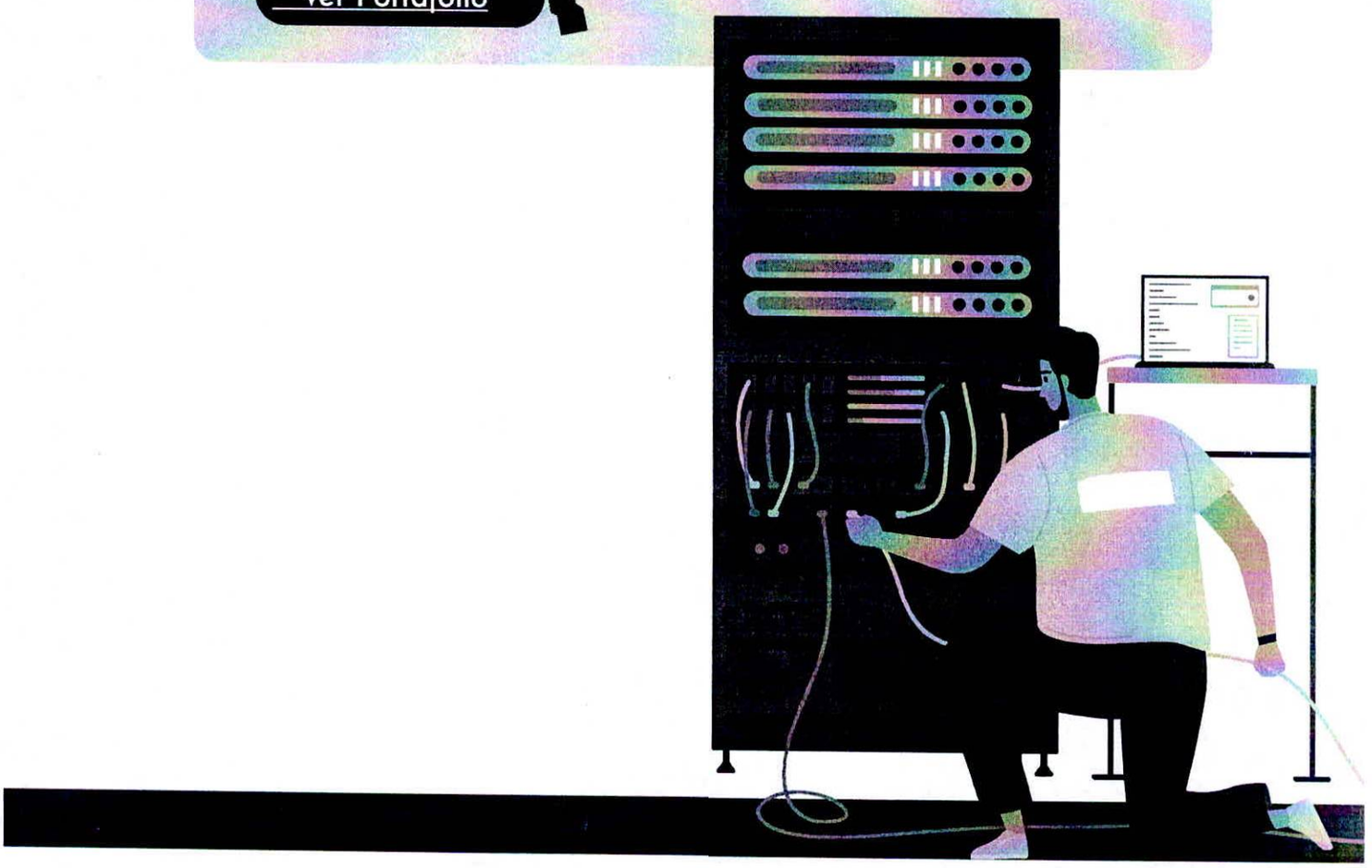
- Valores en pesos, IVA e impuestos incluidos.
- Forma de pago, contra entrega a satisfacción
- Tiempo de entrega, 15 días a partir de la aprobación.
- Vigencia de la propuesta: 30 días calendario.

Para nosotros es importante entregarle servicios de calidad, consulte aquí nuestro Acuerdo de Nivel de **Servicios - ANS**

¡Conoce todo en lo que podemos ayudarte!

Conocimiento, talento, experiencia y pasión nos caracterizan. Tenemos mucho para aportarte; hecha un vistazo a nuestro portafolio de soluciones:

Ver Portafolio



Contacto

Johana López Baena

Gerente de Cuenta

(+57) 318 8216640

gerentedecuenta2@infortec.co

Más Información

www.infortec.co

Cra 7 # 18-21, Of. 310 , Ed. Antonio Correa, Pereira, Colombia

@infortec_latam @infortec_latam @infortec_latam