Oferta No. 2185
UPME

Contacto Comercial
Laura Alejandra Álvarez Marín I
Sales Consulting
Cel: +57 3173779590 I Email: Laura.Alvarezl@ngeek.co
Bogotá, 14 de Marzo de 2025

NGEEK

Cra 16a # 79 – 05 Of 607
Bogotá, Colombia
www.ngeek.co
+57 3143554583
+57 3186113985

OFERTA TÉCNICA

Antecedentes:

El cliente UPME se encuentra en proceso de desplegar nuevos servicios en la nube, además de gestionar el balanceo de carga en su infraestructura de centros de datos on-premises (DC). Como parte de sus planes de optimización de la infraestructura, se propone asegurar la conectividad con el servicio Distributed Cloud XC de F5, ya sea los nuevos servicios en nube o en sus instalaciones locales.

Alcance:

Conectividad con Customer Edge en XC de F5: Despliegue de dos (2) Customer Edge (CE) en la infraestructura on-premise o en nube, los cuales contaran con conectividad a los POPs de XC (Nube) de F5 para garantizar su administración y visualización de reporte central, de forma que el tráfico se pueda balancear entre su infraestructura local o sus servicios en la nube. Esto es esencial para garantizar que el tráfico se gestione de forma eficiente, tanto en su centro de datos on-premises o en la nube.

Balanceo de máximo 5 aplicaciones a través del Customer Edge.

Protección de aplicaciones en la Nube de F5 (Regional Edge) con WAAP: En la nube de F5 (Regional Edge), se realizará el despliegue de máximo 5 Load Balancers, los cual proporcionará protección y seguridad para las aplicaciones desplegadas (WAAP). Estos load balancers asegurarán que el tráfico pase por la nube de F5, lo cual proporcionará un entorno más controlado y seguro para sus aplicaciones.

Aseguramiento por medio del módulo de WAAP en la nube de F5 de máximo 10 aplicaciones.

Propuesta Técnica

F5 Distributed Cloud ***Web Application and API Protection (WAAP)*** ofrece una mayor seguridad para las aplicaciones y las API en una solución basada en SaaS fácil de implementar, pero poderosa.

Las aplicaciones son el elemento vital de las empresas en la actualidad, lo que impulsa un aumento en el gasto mundial en software empresarial que se espera que supere los US $ 600 mil millones para 2021, según Statista.com. Pero con la implementación y el uso cada vez mayores de aplicaciones en todo el mundo, surgen requisitos para una seguridad de aplicaciones poderosa.

La necesidad de una mayor protección aumenta porque las organizaciones implementan cada vez más aplicaciones en un modelo distribuido entre proveedores de nube, ubicaciones de borde y entornos públicos y privados. Esto es particularmente cierto para aquellos que usan aplicaciones modernas creadas con microservicios y múltiples clústeres distribuidos.

Al mismo tiempo, los ciberdelincuentes han encontrado más formas que nunca de exponer, alterar, deshabilitar, robar u obtener acceso no autorizado a las aplicaciones y la infraestructura de TI, en parte debido a la creciente complejidad general de los entornos de las aplicaciones. Los ataques provienen de vectores en todos los puntos de interacción de la superficie de la aplicación, lo que

requiere una defensa sofisticada y de amplia base. Los malos actores continúan siendo oportunistas para encontrar formas de explotar vulnerabilidades (Log4j es un ejemplo reciente).

En el panorama de seguridad actual, "***toda organización debe esperar ataques frecuentes de algún tipo, pero ni las organizaciones ni los atacantes son grupos uniformes***", afirma el Informe de protección de aplicaciones de F5 Labs para 2022. "*Las organizaciones ejecutan diferentes aplicaciones en diferentes redes, almacenan diferentes tipos de datos, tienen diferentes clientes, diferentes controles, diferentes regímenes regulatorios y diferentes apetitos por el riesgo. Las arquitecturas de aplicaciones están cada vez más distribuidas y descentralizadas para el rendimiento y la resiliencia, lo que a su vez introduce múltiples responsabilidades que se cruzan con respecto a la protección de datos*".

A medida que los entornos de aplicaciones evolucionan y se expanden, ilustra aún más la importancia de una estrategia de seguridad de aplicaciones global, una que implemente un enfoque de varias capas y un esfuerzo de seguridad más coordinado en todos los equipos que participan en el ciclo de vida de la aplicación.

Dado lo anterior se diseña la siguiente arquitectura de alto nivel (HLD) que cubre las diferentes aristas de seguridad en entornos Multi-Cloud.

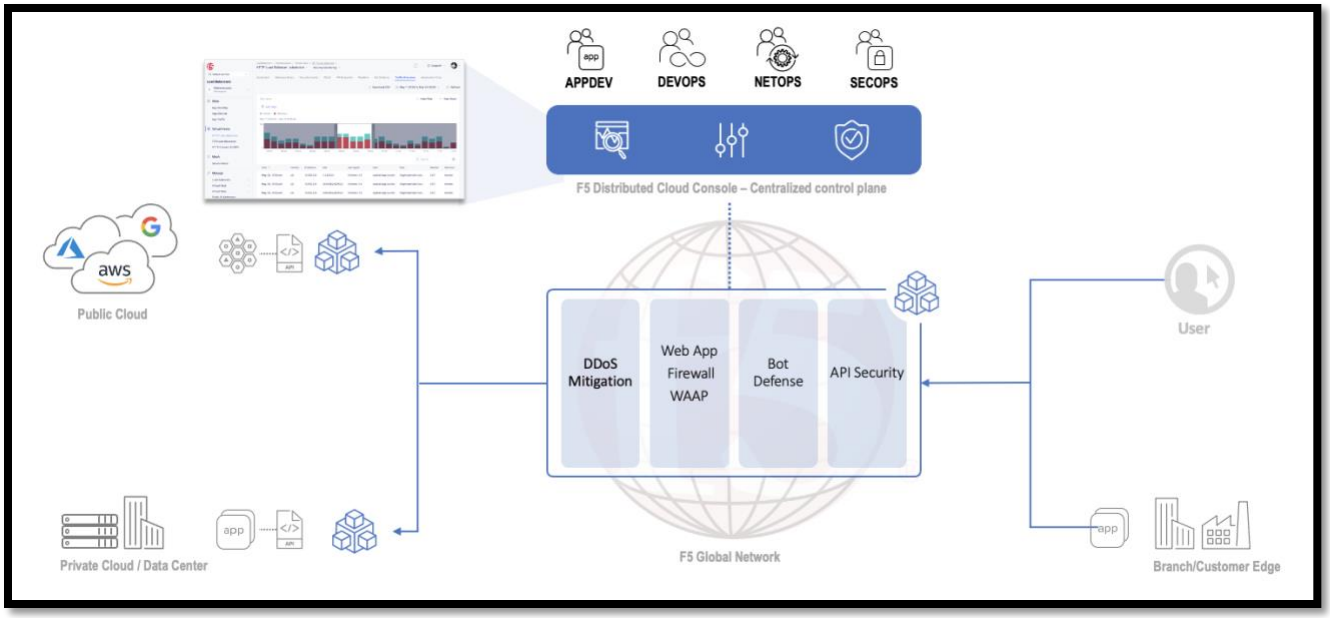


Figura 2. Arquitectura de Alto Nivel (HLD) UPME

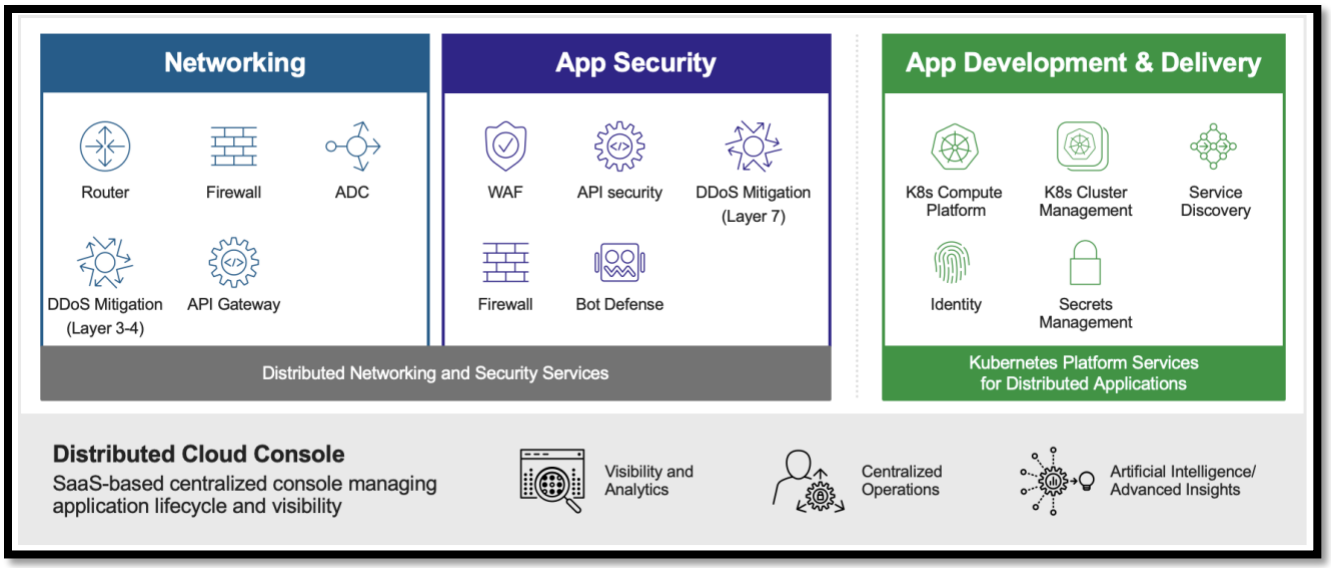
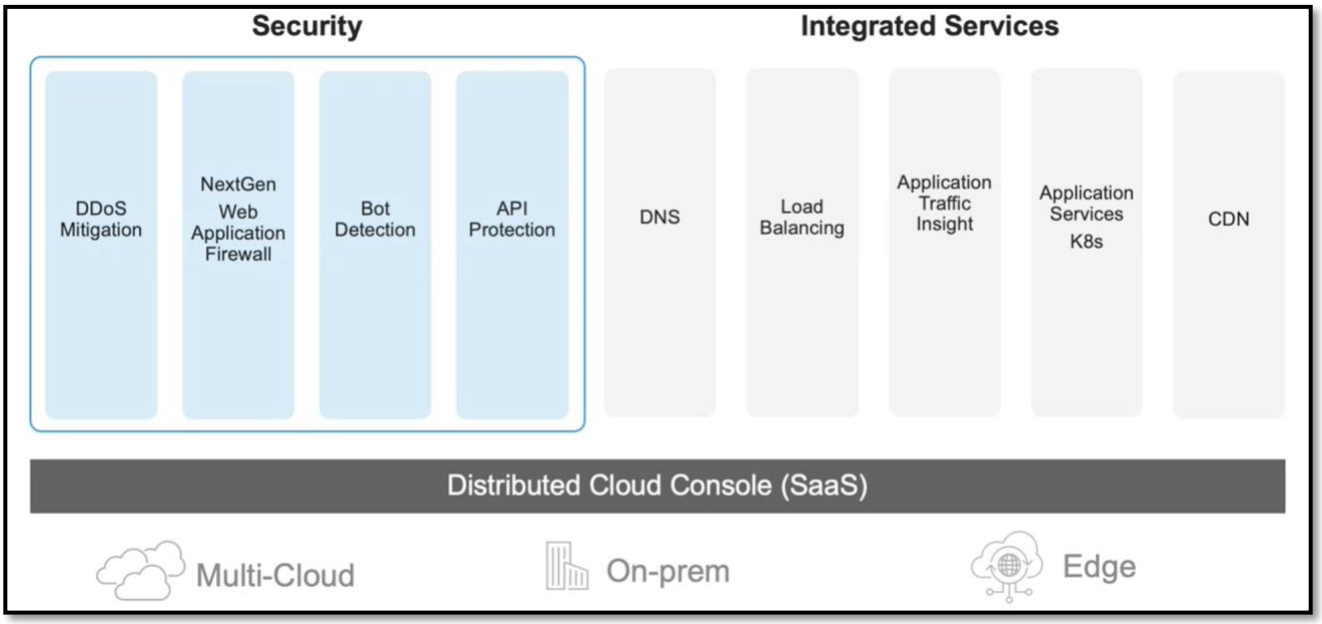


Figura 1. Componentes de F5 Distributed Cloud (XC)

Descripción del servicio



Como se puede observar en el anterior gráfico, F5 divide las soluciones en dos (2) grandes grupos, el primero es de **Security** compuesto por: DDOs Mitigation, NextGen web Applivcation Firewall, Bot Detection y API Protection; el segundo es de **Integrated Services** compuesto por: DNS, Load Balancing, Application Trafico Insight, Application Services K8s y CDN.

Con el fin de proporcionar una defensa en profundidad y una arquitectura de seguridad coordinada para las aplicaciones web y las API de una organización, F5 presenta F5 Distributed Cloud **Web Application and API Protection (WAAP).** Servicio basado en SaaS el cual protege las aplicaciones web y las API implementadas en entornos distribuidos y de varias nubes, lo que simplifica la seguridad de las aplicaciones y aumenta la eficacia general. Reúne cuatro componentes clave críticos para asegurar la experiencia digital para las empresas modernas de hoy:

- **Mitigación de DDoS:** con F5 Distributed Cloud DDoS Mitigation, las organizaciones obtienen protección multicapa contra ataques en las capas 3 a 7, incluido el blindaje a nivel de red de denegación de servicio distribuida volumétrica (DDoS), firmas de DoS, políticas de servicio que incluyen limitación de velocidad, Reputación de IP y depuración avanzada con inspección profunda de paquetes. Esto ofrece protección contra el tráfico falsificado y mal formado, las inundaciones de solicitudes y otras formas de abuso que intentan sobrecargar las propiedades web y las aplicaciones.

- **Firewall de aplicaciones web (WAF):** F5 Distributed Cloud WAF aprovecha la poderosa tecnología Advanced WAF, combinando protección basada en firmas y comportamiento para aplicaciones web. Actúa como un proxy intermedio para inspeccionar solicitudes y respuestas de aplicaciones para bloquear y mitigar un amplio espectro de riesgos derivados del OWASP Top 10, campañas de amenazas, usuarios maliciosos y más.

- **Bot Defense:** F5 Distributed Cloud Bot Defense administra y desvía la automatización maliciosa para evitar ataques sofisticados que emulan humanos. Reúne telemetría unificada, inteligencia de red e IA/ML con análisis humano para identificar y defenderse de amenazas automatizadas como el relleno de credenciales y la apropiación de cuentas, el raspado, el descifrado de tarjetas y más.

- **Seguridad API:** F5 Distributed Cloud API Security protege las interfaces de programación de aplicaciones (API) de los actores de amenazas que intentan explotarlas para facilitar una violación o una interrupción de los servicios. Con el descubrimiento automático de API que puede identificar y asignar puntos finales de API a cualquier aplicación, además de brindar soporte para un modelo de seguridad positivo a través de la importación de swagger de API, las organizaciones pueden observar, refinar y aplicar fácilmente el comportamiento adecuado de la API.

Del grupo de Integrated Services se tienen las siguientes funciones:

- **DNS:** F5 Distributed Cloud DNS es un servicio de DNS autorizado primario y secundario basado en SaaS ofrece distribución global, protección DDoS, ***DNSSEC*** y la flexibilidad para escalar automáticamente para satisfacer las crecientes demandas de las aplicaciones. Permite utilizar DNS inteligentes para distribuir tráfico entrante del servicio entre múltiples clouds y/o enlaces.

- **Load balancing:** El balanceo de carga de F5® Distributed Cloud Mesh es un balanceador de carga distribuido globalmente administrado centralmente y proxy con descubrimiento de servicios, verificación de estado, microsegmentación de aplicaciones y política de aplicaciones que proporciona la implementación más avanzada de balanceador de carga perimetral con capacidad de entrada/salida para cualquier servicio. El descubrimiento de servicios se integra con múltiples registros como Kubernetes o DNS junto con soporte de verificación de estado para http/https, tcp, personalizado, etc. El estado del punto final se distribuye a todos los sitios donde el servicio virtual está expuesto usando extensiones para el BGP y esto nos proporciona información valiosa sobre cómo distribuir globalmente la función de balanceo de carga. La compatibilidad con TLS y TLS mutuo para la autenticación con autorización basada en políticas en el proxy brinda la capacidad de hacer cumplir la seguridad de extremo a extremo del tráfico de aplicaciones.

- **F5 Application Traffic Insight (ATI):** es una herramienta de prueba de valor (PoV) que proporciona información sobre las conexiones, los dispositivos y el comportamiento de los usuarios no deseados en su aplicación web. Con ATI, puede analizar fácilmente las anomalías del flujo de tráfico, determinando actores humanos y no humanos (bots/automatización) tanto maliciosos como legítimos. ATI también le presenta opciones de actualización para las soluciones completas de detección de fraude y anti-bot que ofrece F5.
- **Application Services K8s:** F5 Distributed Cloud Application services K8s, servicio saas que proporcionan una instalación, orquestación y funcionamiento sencillos de los clústeres de kubernetes. es el camino más rápido y sencillo a kubernetes.

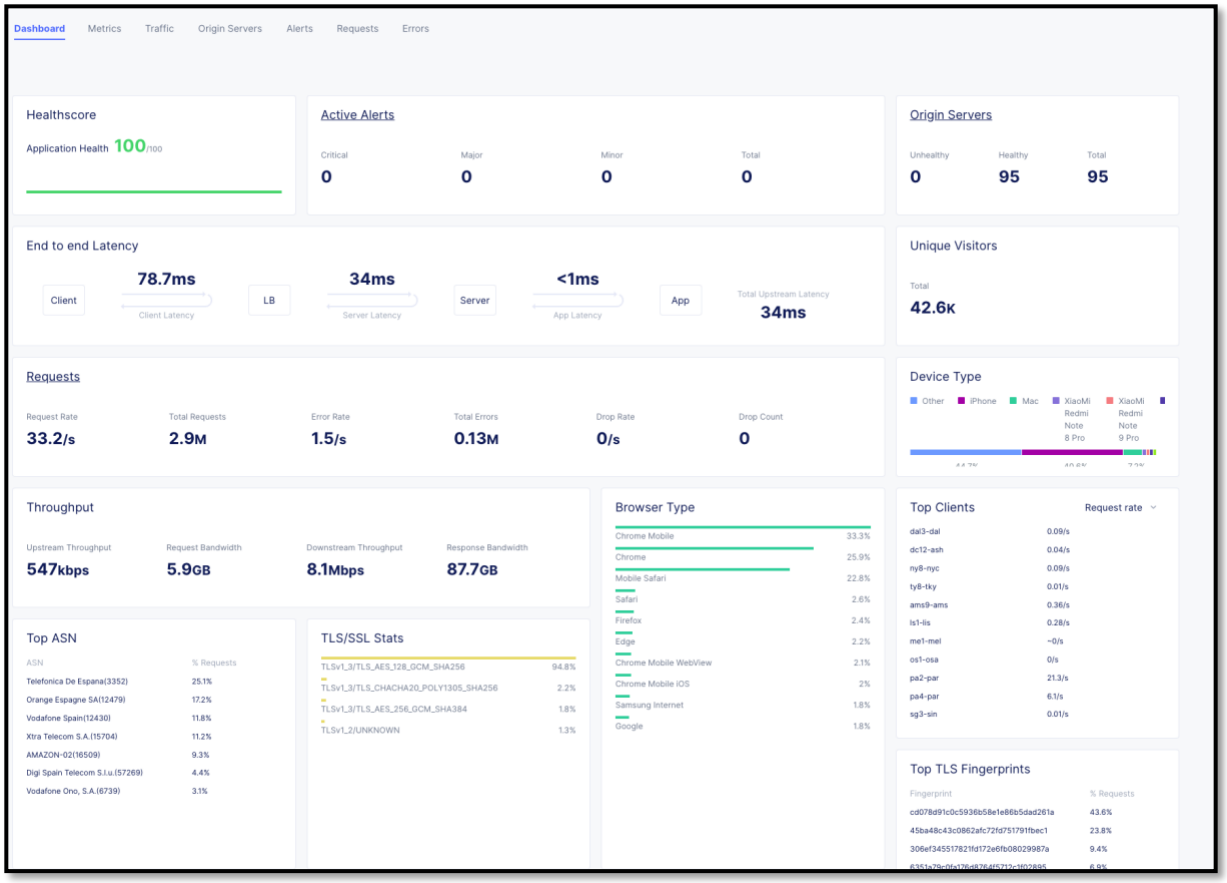
- **Content Delivery Network (CDN):** Una red de entrega de contenido (CDN) es una infraestructura que ayuda a las organizaciones a entregar contenido web estático, medios digitales enriquecidos y todo lo demás a empleados, proveedores, socios y clientes de todo el mundo, en el menor tiempo posible y al menor costo posible.

Visibilidad y Servicios Mejorados:

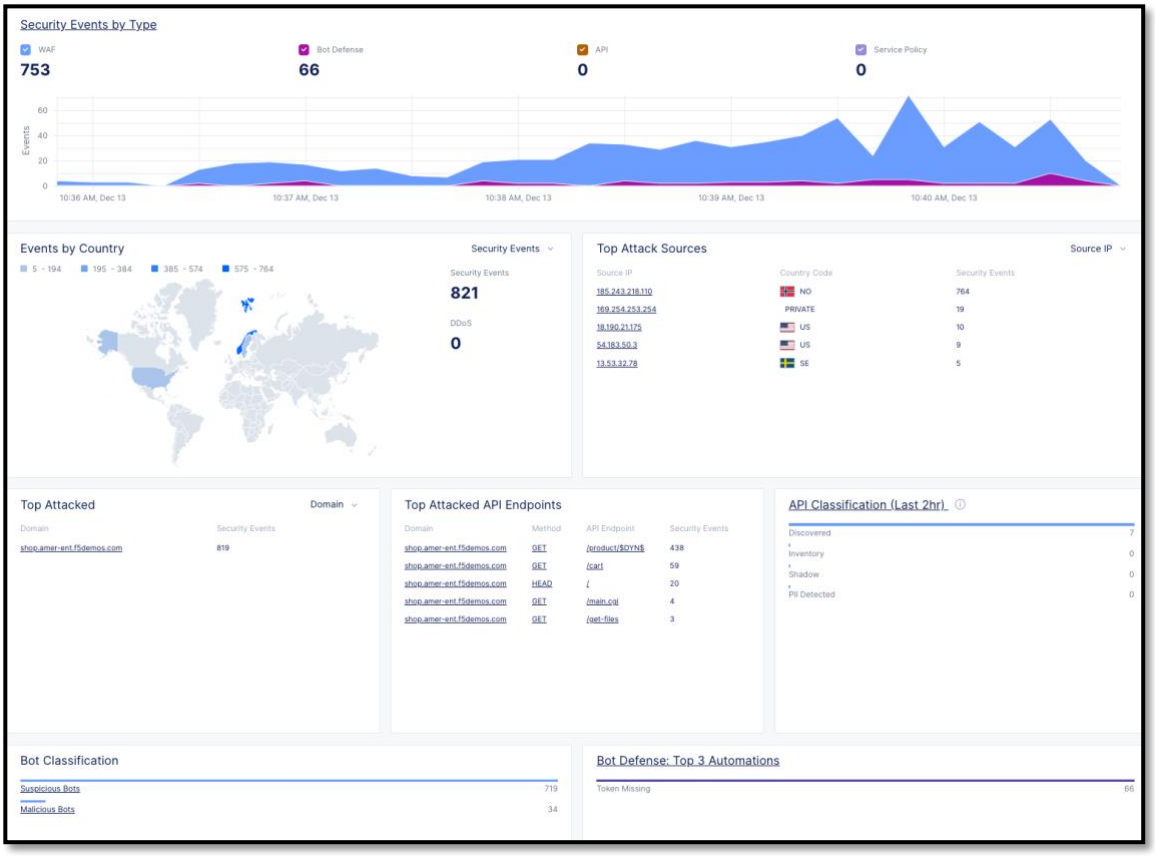
La consola de Distributed cloud Services cuenta con dashboards detallados para conocer datos en tiempo real e históricos sobre el consumo de las aplicaciones, estos nos permiten entender la forma en que han sido utilizadas las apps y filtrar eventos de manera que sea más sencillo conocer el performance y la seguridad de los servicios.

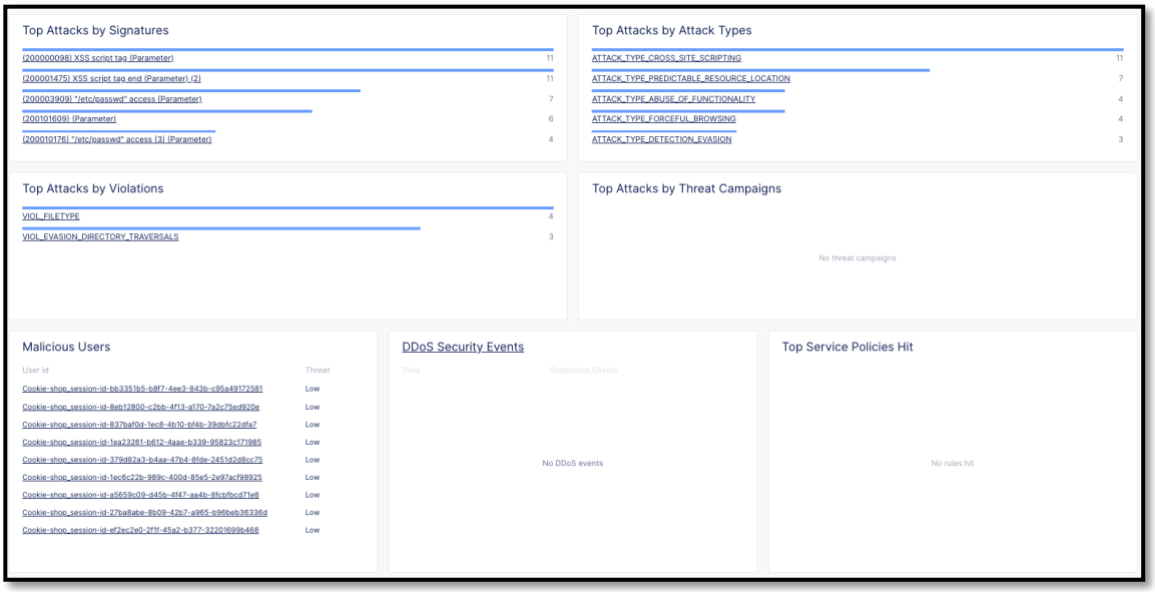
Dashboard de Performance, dentro del dashboard de performance podremos ver información sobre la salud de las aplicaciones, en sus orígenes y como promedio, conocer la latencia de consumo, cantidad de request, tipos de dispositivo, tipo de browser, ASN utilizando protocolo TLS, TLS fingerprint, entre otros datos. Estos pueden ser visualizados de manera general o por request.

Dashboard de Performance:



Dashboard de Seguridad, Nos permite conocer datos directamente relacionados con eventos de seguridad, categorizándolos por WAF, Bot Defense, APISec y Service Policy, entrando con detalles de locación del cliente, top attack sources, endpoints más atacados, clasificación de bots, ataques de WAF y firmas.





Identificación de usuarios maliciosos:

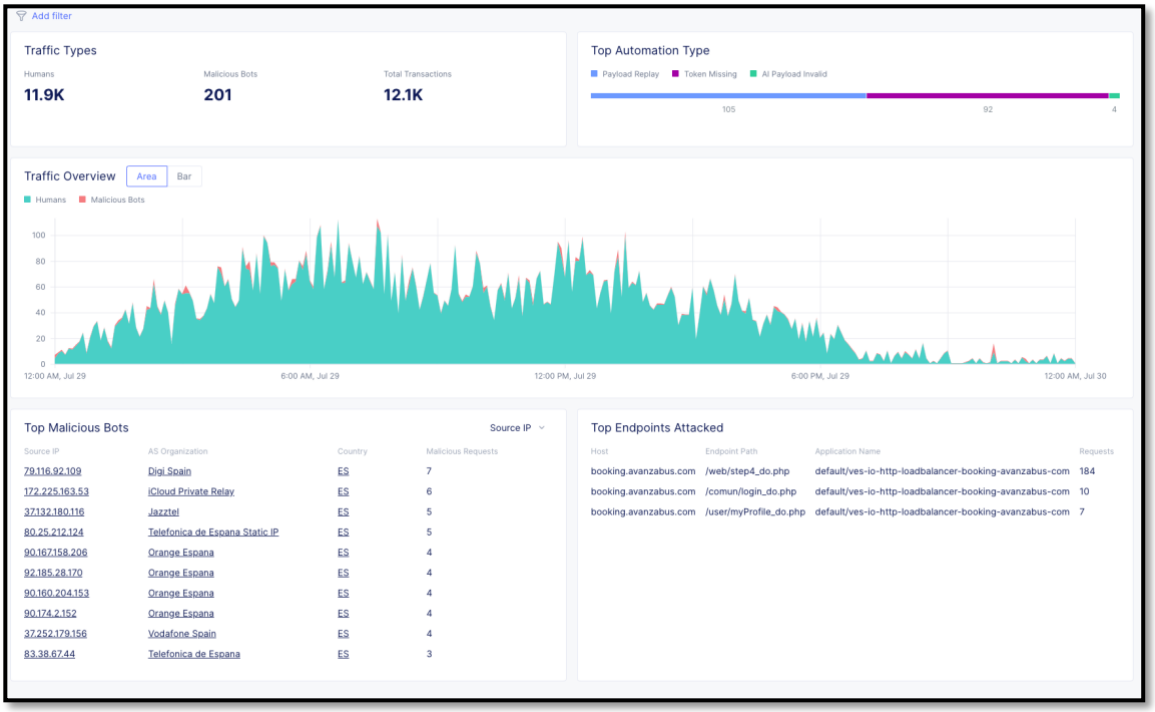
Permite la identificación de usuarios y su mapeo de acuerdo con el comportamiento presentado en la aplicación utilizando los diferentes engines de seguridad integrados como un solo servicio.



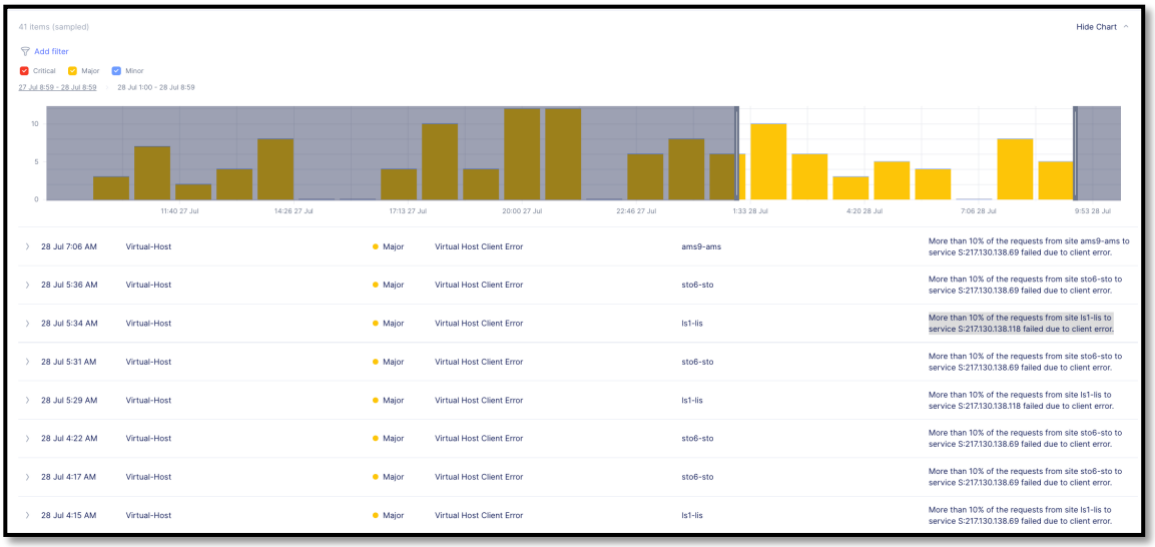
Detalle sobre eventos de Seguridad:



Detección de Automatización:



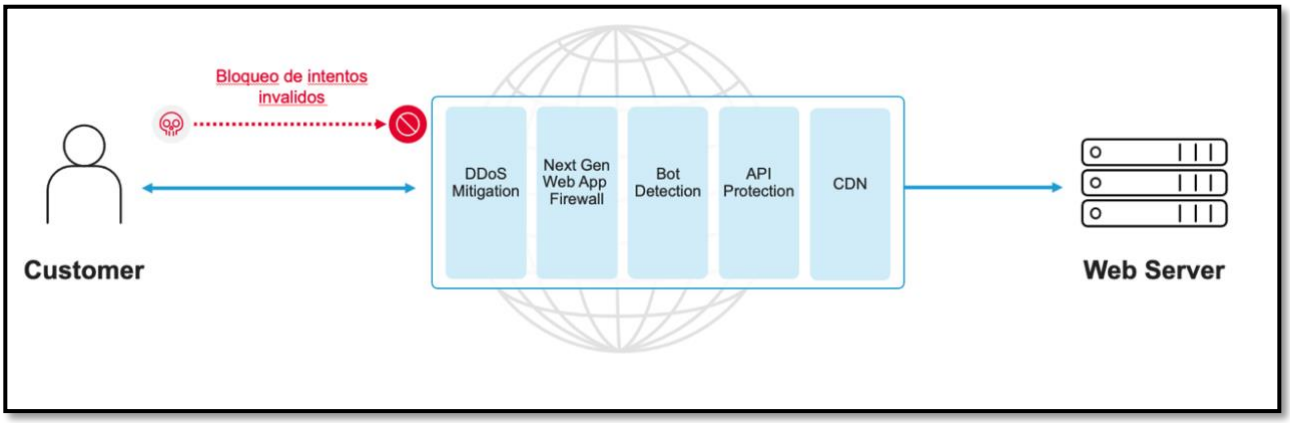
Eventos de performance:



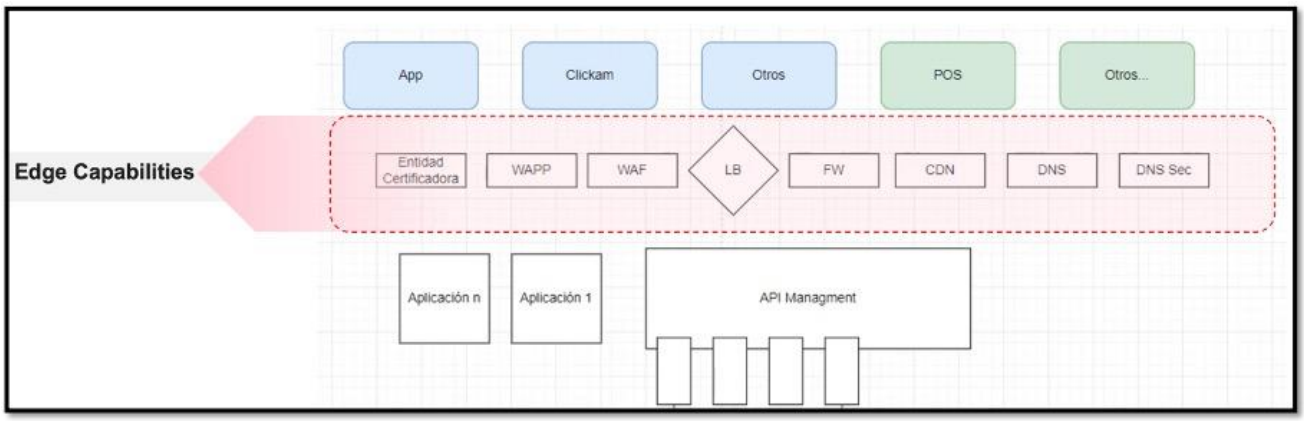
Arquitectura de alto nivel

La solución propuesta es una “Software as a Service” con arquitectura de proxy utilizando diversos puntos de presencia con entrega del servicio a través de anycast o redirigiendo el tráfico a través de

DNS para que las peticiones pasan por F5 Distributed Cloud antes de llegar al servidor de la aplicación.



Arquitectura Referencial



Servicios Propuestos

Los servicios de Distributed Cloud se han diseñado utilizando un paquete base con la capacidad de ampliar con opciones y servicios adicionales.
El paquete base, brinda a los clientes una cantidad significativa de capacidades, que incluyen:

Global Application Delivery Network

- Load Balancing
- Secure Networking
- Application Security
- Basic API Security
- DNS Primary/Secondary up to 250 Zones
- DNS Load Balancing para 50 FQDNs

Load Balancing

- Globally Distributed Public Load Balancer
- Unlimited number of Endpoints (Origin Servers)
- Unlimited number of Endpoint Locations for Health-checks

Security Capabilities

- One Global Anycast VIP, Included
- Two DNS Domain Delegation
- Layer 3 DDoS Protection
    - Fast ACLs: 500 Rules included
    - Policing included
- Web Application Firewall included in Regional Edges
- Layer 7 DDoS Protection
    - HTTPS SSL Termination included
    - Layer 7 (HTTP) Policies (e.g., JS Challenge, Whitelisted IP Lists, Customer L7 Policies)
    - 200 Service Policy Rules included

Administration

- Unlimited number of Users
- Single Sign On capabilities included
- RBAC capabilities included

Observability

- Metrics, Request Logs, and Audit Logs
- Log Export capabilities included
- Alerts/Notifications based on Policy Rules included

Additional capabilities:

- API Protection basada en millones de peticiones API al mes.
- Load Balancers adicionales.

- F5 Advanced Bot Technology for BOT/Automation Proteccion basada en incrementos de 20Millones de transacciones al mes.
- Rate Limiting basada en Millones de reques al mes.
- CDN basada en request al mes y cantidad de datos transferidos

SLA:

Distributed Cloud: Authentication Intelligence, Aggregator Management, Client-Side Defense, Account Protection, Bot Defense (Managed Service), and Bot Defense (Self Service)	
Porcentaje de tiempo de disponibilidad mensual o estándar de rendimiento	**Descripción**
99.99% Uptime	Sujeto a las condiciones especiales a continuación, haremos todos los esfuerzos comercialmente razonables para que la Oferta de SaaS en la nube distribuida aplicable esté disponible para usted al menos en el Porcentaje de tiempo de actividad mensual en el período aplicable.
Tiempo de Respuesta: 30 minutes	Proporcionaremos una respuesta inicial a las solicitudes de sus contactos aprobados dentro de los 30 minutos posteriores a la recepción de la comunicación por teléfono o correo electrónico.
***Root Cause Analysis for Sev1 or Sev2 Incident: 24 hours (draft); 7 days (final)**	Proporcionaremos un informe que describa el evento, las causas técnicas, la acción correctiva y los planes a largo plazo para la prevención.

Crecimiento

El servicio permite realizar crecimientos por cada tipo de protección, antibot, APIsec, Ratelimit, LB (WAF). Cada uno de los siguientes elementos puede crecer de manera individual y se aplican a nivel de tenant, por lo que se pueden compartir entre las diversas aplicaciones, de la manera que se detalla en la siguiente tabla:

Index	Producto	Descripción
4	Antibot Avanzado	Crecimiento por **cada 500 Mil peticiones diarias,** aplica solo para los endpoints pprotegidos por antibot avanzado, como, Login, creacion de cuentas, reset pasword.
8	Load Balancer en Nube	Crecimiento **por cada LB** en nube, permitiendo tener dashboards dedicados a este servicio. En un LB pueden haber más de una aplicación/FQDN

5	Seguridad avanzada de API	Prteccion de API avanzada, con Machine Learning, incluye la protección de **1 Millon de API calls al mes.**
6	L7 DDoS Rate Limiting	Proteccion de L7 Rate limiting, se calcula **por cada Millón de peticiones al mes**
2	Customer Edge	Máquinas Virtuales de F5 XCS con capacidades de seguridad locales, permiten el enforcement de seguridad con las mismas políticas que existen en nube, el crecimiento es por nodo o por cluster de 3 los cuales trabajan en activo activo, incluyen Ratelimit. Posibles addons WAF, APISec.
7	Customer Edge WAF Addon	Permite la utilización de políticas de WAF de manera local en los Customer Edge.
3	Trafico Generado desde Ces a la nube de F5 XCS	El crecimiento es en el orden de TB de subida al mes.

Condiciones Generales de Implementaciones NGEEK

NGEEK acepta que por ningún motivo podrá divulgar, comercializar o dar a conocer los trabajos realizados como parte de este servicio por tratarse de productos y/o sistemas que son propiedad industrial del cliente, por lo que acepta firmar una carta de confidencialidad, en caso de que así se requiera.

Es responsabilidad del administrador del área sistemas del cliente y/o gerente del pro, informar a sus usuarios sobre el mantenimiento o instalación que se realice sobre su infraestructura y el tiempo en el que los servicios no se encontrarán disponibles. Así mismo, deberá, en caso de ser necesario respaldar o realizar una copia de seguridad de la información relevante para él o para la organización que representa.

Cualquier requerimiento adicional que surja durante o posterior a la realización del proyecto y que no esté cotizado y/o documentado como parte del alcance, objetivos y actividades a realizar en el presente dimensionamiento base, será motivo de una nueva propuesta técnica y económica.

NGEEK no se hace responsable por el corte del servicio debido a fallos en la red, así como cortes en la energía eléctrica u otros factores ajenos al funcionamiento, configuración e instalación de la solución propuesta en la presente oferta.

Es responsabilidad del líder del proyecto (PM) por parte del cliente informar los diferentes cambios en la infraestructura que se generen durante el proyecto, así como a los usuarios al momento de tenerse previsto una indisponibilidad en algún servicio.

De requerirse cualquier otro servicio complementario, tendrá que ser cotizado por separado.

El cliente se compromete a recolectar y entregar NGEEK la información técnica pertinente para llevar a cabo de forma satisfactoria la ejecución del proyecto. En caso de no suministra dicha información antes de iniciarse el inicio de la instalación, esto eximirá a NGEEK de cualquier problema que se pueda

presentar en la misma y podrá ocasionar costos adicionales para el cliente referentes a procesos de reinstalación.

El horario para la implementación será horario de oficina de lunes a viernes de 8:00 a.m. a 6: 00 p.m., en las instalaciones del cliente o de forma remota según se haya acordado.

Los trabajos aquí descritos, su alcance y actividades están contemplados para iniciar inmediatamente a más tardar en un plazo 30 días. Si por alguna excepción, los prerrequisitos, los Insumos, facilidades o Infraestructura requerida y de la cual NGEEK no es responsable no estuviese adecuada o disponible, NGEEK colocara en Espera "Standby" el Proyecto por un plazo Máximo de dos (2) meses (60 Días) y procederá a facturar la instalación como si está ya se hubiera realizado.

Finalizado este tiempo, NGEEK no se hace Responsable de mantener el Recurso de Ingeniería asignado, y de finalizar actividades contempladas en el SoW, salvando toda responsabilidad por daños y perjuicios a que haya lugar.

Requerimientos, Supuestos y Exclusiones

Requerimientos Generales

- ✓ Asegurar la conectividad remota a la interfaz de administración de los equipos, para poder realizar las actividades que hacen parte del presente alcance.
- ✓ Asegurar la disponibilidad del personal apropiado de la red, especialmente switch, router, firewall, DNS, etc.
- ✓ Los retrasos debidos a la falta de información requerida, la falta de acceso físico o falta de disponibilidad podrá dar lugar a la reprogramación de las actividades que se están realizando.
- ✓ Antes de comenzar con cualquier actividad es necesario la firma de Statement Of Work (SoW).
- ✓ Los equipos (BIG-IP o F5 VE) involucrados en el proyecto deben contar con soporte del fabricante antes de realizarse cualquier actividad que involucre actualización o parchado del S.O.
- ✓ El cliente se compromete a recolectar y entregar la información técnica pertinente a NGEEK para llevar a cabo la configuración de los equipos de comunicaciones y de seguridad integrantes de la solución.

Supuestos

Con el fin de establecer con claridad del alcance del servicio que presta NGEEK, a continuación, se mencionan los supuestos que se dan por cumplidos, los cuales hacen parte de la correcta prestación de servicio:

- ✓ El cliente realizará una inducción al personal de NGEEK, acerca de los procesos, normas, reglamentos de seguridad y de convivencia a cumplir durante la permanencia en las instalaciones (si aplica).

- ✓ El cliente suministrará los dispositivos de identificación y autorización de ingreso a las áreas adecuadas para las personas de nuestra organización que participaran en las actividades de ejecución durante el proyecto y la operación del servicio, para los casos en que este último haya sido considerado (si aplica).

- ✓ El cliente asignará un coordinador, líder, jefe o gerente de proyecto que en conjunto con el coordinador, líder, jefe o gerente de proyecto de NGEEK realizará y establecerá la definición y presentación del proyecto, planificación de las actividades durante todas y cada una sus fases, además de establecer los objetivos generales y particulares del proyecto, supervisar tareas de ejecución, gestionar recursos asignado a su respectivo rol y entre otras tantas.

- ✓ El cliente recolectará y entregará la información técnica pertinente a NGEEK para llevar a cabo la configuración de la solución que hace parte del presente alcance.

- ✓ El cliente gestionará todas las comunicaciones y configuraciones que sean requeridas para la implementación de la solución y será el facilitador de información para el recurso asignado.

- ✓ El cliente dará cumplimiento a todos los requerimientos necesarios para la correcta ejecución del proyecto. El Anexo de Requerimientos, estará expuesto en el Statement Of Work (SoW) que será acordado y revisado por las partes, antes de iniciar la ejecución de las actividades del proyecto.

Exclusiones

No se incluye en el alcance del presente proyecto:

- ✓ La ejecución de instalación física de ningún componente que haga parte de la solución, entendiéndose por componente, cualquier elemento como appliances, cableado, conectores, etc.

- ✓ La administración, seguimiento y control del recurso humano del cliente, asignado para el desarrollo del proyecto.

- ✓ Configuraciones sobre los PCs del usuario final, y con esto, la instalación, reparación y actualización del Sistema Operativo de las estaciones de trabajo del cliente.

- ✓ Elaboración de guías pasó a paso para uso y administración de las soluciones.

- ✓ Implementación de cambios de red (equipos Switching y/o Routing), y/o de seguridad Perimetral (Firewall, IDS, WAF) de propiedad de cliente final y/o de terceros.

- ✓ Implementación y desarrollo de funcionalidades adicionales que no estén expresamente descritas o provistas por el producto y/o servicio a ser implementado.

- ✓ Adiciones o modificaciones de recursos físicos, lógicos, operativos y/o logísticos a los dispuestos en el presente alcance.

- ✓ Otros elementos que no estén expresamente mencionados en esta propuesta.

** En caso alguna actividad requerida no se encuentre explícitamente mencionada en el presente Alcance, NGEEK está en total disposición y disponibilidad para realizarlas según lo demande el cliente final, previa ejecución del proceso de control de cambios, donde se realizará evaluación presupuestal y disponibilidad de recursos.*

Soporte Premium F5



En un mundo donde el cambio es la única constante, usted confía en su tecnología F5® para lograrlo, no importa el tipo de negocio. A medida que surgen desafíos, encontrar rápidamente la mejor solución para su negocio puede significar la diferencia entre la crisis de TI y la agilidad de TI.

El soporte como el Premium (24x7) incluyen asistencia remota tanto en línea y por teléfono, soporte proactivo para el mantenimiento planificado, devolución anticipada.

Reemplazo de autorización de materiales (RMA), actualizaciones de software y ayuda con F5 iRules.

Puede actualizar el soporte Premium con Servicios de RMA acelerados y paquetes complementarios de mantenimiento. Además, F5 proporciona muchos recursos gratuitos de autoservicio para ayudarlo a aprovechar al máximo su inversión en F5.

Beneficios

- Reciba ayuda rápida e informada con sus preguntas o problemas relacionados con su tecnología F5, por lo que puede seguir prestando los servicios en los que su el negocio depende.
- Soporte de vía rápida para mantenimiento programado para minimizar el tiempo dedicado a abrir un nuevo caso.
- Aproveche al máximo la flexibilidad que ofrece Scripts de iRules para personalizar sus dispositivos F5.
- Con Premium, expertos en F5 proporcionan asistencia de iRules en la resolución de problemas, comprobando la sintaxis y validando la lógica.

- Obtenga más valor de su inversión al utilizando los recursos en F5.com para buscar el base de conocimientos, amplíe su conjunto de habilidades y interactuar con la comunidad de desarrolladores de F5.
- Asistencia experta cuando la necesite
- Las nuevas versiones de software están disponibles sin cargo para las unidades de soporte.
- Para aprovechar al máximo su inversión en la solución F5, explore los recursos proporcionados por la base de conocimientos AskF5 ™ y la comunidad en línea de F5 DevCentral
- RMA para casos de fallos y eventualidades con el equipamiento.

Cuente con F5 Support para brindarle la ayuda que necesita, cuando la necesita. F5 en todo el mundo la organización de atención al cliente ha implementado una Calidad que cumple con ISO 9001: 2015 Sistema de gestión que garantiza que F5 se adhiera a los procesos y procedimientos documentados y continúa mejorando la prestación de asistencia al cliente. Con el cumplimiento de ISO, puede confiado en que recibirá un servicio excelente de manera constante.

Alcance Premium Support de F5

Los servicios de soporte de F5 están diseñados para ayudarle de forma remota con problemas específicos de reparación de averías relacionados con el mantenimiento continuo de sus productos de F5. El soporte técnico se limita a los productos de F5 con contratos de soporte activo. Dentro del alcance se encuentra:

- Disponibilidad del soporte de F5 en horario 24/7
- Acceso ilimitado a la base de conocimientos de "AskF5"
- Acceso al portal del soporte web
- Respuesta a llamadas de sitio inactivo dentro de los 30 minutos (solo por teléfono)
- Reemplazo de RMA

Portal de soporte web

El portal de soporte web de F5 les brinda más flexibilidad y acceso rápido a los centros de soporte de red de F5, en cualquier momento. Cree rápidamente nuevos casos de soporte, reciba un número de caso automatizado, lea detalles y actualizaciones de casos, cargue archivos adjuntos de solución de problemas y más. La ayuda en línea está siempre disponible.

Base de conocimientos "AskF5"

Considere AskF5 como su primera fuente de respuestas. Visite el sitio web de AskF5 para descargar software, herramientas de licencia, guías de productos, notas de la versión, soluciones a problemas conocidos e información práctica. También puede registrarse para recibir alertas de seguridad por correo electrónico y fuentes RSS específicas del producto.

Horario de soporte

Contamos con personal ingeniero de soporte de red de F5 continuamente, las 24 horas del día, los 7 días de la semana, los 365 días del año. Independientemente de dónde se encuentren sus oficinas, el soporte técnico de F5 está disponible durante su día laboral.

Tiempos de respuesta

F5 busca proporcionar tiempos de respuesta rápidos para todos los casos entrantes. Si un técnico no está disponible inmediatamente para ayudarle, un representante de atención al cliente registrará su llamada en nuestro sistema de respuesta de casos y le dará un número de caso.

Todos los Centros de soporte de la red F5 mantienen las siguientes definiciones de gravedad de casos y tiempos de respuesta objetivo para garantizar que se utilicen los recursos apropiados para resolver todos los problemas técnicos de la manera más eficiente posible.

F5 se esforzará por responder a los problemas de gravedad 1 en treinta minutos. Entendiendo que los eventos imprevistos podrían retrasar los intentos, F5 espera que la mayoría de los problemas de Gravedad 1 se respondan dentro de este nivel de servicio.

La respuesta inicial se define como el tiempo desde que se creó el caso F5 hasta que un ingeniero de soporte de red intenta contactarlo por primera vez para solucionar el problema y luego actualiza el registro del caso para reflejar esta acción.

Oferta Económica

Descripción	Precios COP
F5 XC Distributed Cloud	$ 182.045.531
Valor Total	$ 182.045.531

Servicios Profesionales	Precios COP
Servicios profesionales	$ 14.946.750
Valor Total	$ 14.946.750
IVA	$ 2.839.883
Total	$ 17.786.633

Condiciones Comerciales

- Los precios de la renovación están dados en pesos colombianos.
- Los precios se presentan antes de Impuestos. El valor neto de la factura se emitirá después de retenciones, impuestos, tasas o gravamen a que haya lugar.
- Para los servicios profesionales se incluye el IVA
- Validez de la oferta por 30 días según la fecha en la portada de esta oferta. Al terminar la vigencia de la presente oferta Ngeek se guarda el derecho de cambiar cualquier afirmación de la presente oferta incluyendo descuentos y precios ofrecidos.

Condiciones Facturación

- Se entregará facturación electrónica de acuerdo a la legislación Colombiana.
- Se facturara un único pago contra entrega del licenciamiento.

Condiciones Recaudo

- El pago será el valor neto de la factura después de retenciones, impuestos, tasas o gravamen a que haya lugar.
- El pago de la factura se efectuará a los 30 días de la radicación de la factura.
- El no pago oportuna de las facturas emitidas generará interés de mora la tasa máxima legal vigente.
- Serán pagados mediante transferencia electrónica en pesos colombianos hacia la cuenta de Ahorros No 69800001613 Banco Bancolombia, titular Ngeek S.A.S Nit 900697738-2

Entiéndase por “Documento Confidencial” toda aquella información, ya sea técnica, financiera, comercial o de cualquier otro carácter, que sea suministrada y/o comunicada por NGEEK SAS en relación con el PROYECTO, mediante palabra, por escrito o por cualquier otro medio o soporte, tangible o intangible, actualmente conocido o que posibilite el estado de la técnica en el futuro.

En el supuesto de que, previamente a la celebración de este acuerdo, su empresa hubiera tenido acceso a información de NGEEK SAS aquélla será considerada, a todos los efectos previstos en el presente documento, como Información Confidencial, salvo aquella que expresamente sea clasificada por NGEEK SAS como información de libre uso y/o divulgación.

Bogotá
viernes, 14 de marzo de 2025

Señores
UPME
Atn. Gustavo Baquero
Bogotá D.C.

Asunto: Propuesta solución F5 distributed Cloud

Estimado Gusatvo reciba un cordial saludo,

Agradecemos la confianza depositada en GAMMA INGENIEROS S.A.S. para nosotros es un placer poner nuestras soluciones a su servicio. A continuación, se describen los objetivos, el alcance de la propuesta y el valor de la solución, junto a las condiciones comerciales necesarias para la negociación.

Quedamos a su entera disposición para aclarar cualquier inquietud referente a nuestra propuesta, no dude en comunicarse con nosotros para atenderlo inmediatamente.

Atentamente,

Karol Lopez

Directora Comercial

Karol.lopez@gammaingenieros.com

Cláusula de confidencialidad

Toda la información contenida en este documento es proporcionada con confidencialidad con el único propósito de presentar una propuesta comercial con la entidad receptora prohibiendo expresamente su publicación, divulgación o utilización del contenido para fines propios o de terceros no autorizados sin consentimiento previo expreso y por escrito de Gamma Ingenieros S.A.S.

Acerca de Gamma Ingenieros S.A.S.

Gamma Ingenieros, creada en febrero de 1983, es una empresa colombiana dedicada a satisfacer las necesidades de sus clientes con Soluciones y Servicios en Tecnologías de la Información, generando confianza y mejorando la experiencia de los clientes.

Nuestros pilares tecnológicos

Ciberseguridad

Brindamos a nuestros clientes productos y servicios de alta calidad, que les permitan asegurar sus servicios digitales críticos logrando que su negocio siempre esté disponible y seguro.

Conocer soluciones

Infraestructura

Optimizamos, agilizamos y escalamos de manera rápida y simple los servicios digitales de nuestros clientes a través de productos y servicios enfocados en conectividad, almacenamiento e hiperconvergencia.

Conocer soluciones

Cloud

Proporcionamos a nuestros clientes la capacidad de adoptar de manera correcta y segura el viaje hacia entornos cloud o híbridos, que les permita transformación digital de su negocio.

Conocer soluciones



OT/SCADA

Aseguramos entornos de alta criticidad e impacto en la industria con nuestros servicios y productos especializados y enfocados a proteger e interconectar los entornos de OT.

Conocer soluciones



Cibersecurity Operation Center

A través de un amplio abanico de servicios especializados brindamos asesoría a nuestros clientes que les permita tener capacidad de abordar en distintas capaz una protección holística de sus servicios digitales por medio de la identificación, protección, detección, respuesta y recuperación ante alguna eventualidad que impacte su negocio.

Conocer soluciones

Propuesta económica

Se propone la solución de F5 distributed Cloud para fortalecer la infraestructura de seguridad, con capacidades avanzadas que incluyen balanceo de servicios con DRP, firewall de aplicaciones avanzado, protección antibot, y mecanismos efectivos contra diversos vectores de ataque como inyecciones SQL, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Botnet y ataques DDoS, entre otras características.

Alcance:

- Solución XC F5
- Servicios profesionales

OFERTA COMERCIAL

Producto		Precios COP
A	Distributed Cloud F5	$ 254.087.975
Valor Total		$ 254.087.975

Servicios Profesionales		Precios COP
A	Instalador y Configurador	$ 19.495.046
Valor Total		$ 19.495.046
IVA		$ 3.704.059
Total		$ 23.199.105

Forma de Pago

Por favor tenga en cuenta las siguientes indicaciones:

- Precios en Pesos colombianos
- Los anteriores valores incluyen IVA.
- Se factura el 100% de los equipos/licencias con el acta de entrega.
- Se factura el 100% de los servicios con acta de recibo a satisfacción del cliente final.
- El pago de las facturas es 50% de anticipo y 50% a la recepción de bienes o servicios.
- El pago de la/s factura/s se realizará a los 30 Días de plazo
- Para la entrega de los servicios o soluciones ofertados se requiere de un contrato u orden de compra formal por parte del cliente

Tiempo de Ejecución y Entrega

El tiempo de entrega de Equipos/licencias es de 30 días y los servicios se coordinarán de acuerdo con la disponibilidad de los líderes de Proyecto de UPME

Validez de la Oferta

30 días a partir de la fecha de emisión de la presente propuesta.

Responsabilidades de Gamma Ingenieros S.A.S.

Sumado a las obligaciones que se generan comercialmente, GAMMA INGENIEROS S.A.S. también será el responsable de la ejecución de los alcances de la propuesta, en coordinación y con la participación del personal de UPME; así como del servicio postventa relacionado con los paquetes de servicio adquiridos a través de organización propia o de terceros.

Responsabilidades de UPME

Sumado a las obligaciones que se generan comercialmente, UPME será responsable por la disposición de los recursos técnicos necesarios, de la entrega de la Información técnica solicitada, de la disposición de tiempo, espacio y lugar para el desarrollo del proyecto. De este modo, una vez cumplidos todos los requerimientos previamente solicitados junto con la realización de la prueba a la solución ofertada, con un resultado de: "EN CONDICIONES NORMALES DE OPERACIÓN", UPME será responsable de la firma de las actas de recepción definitiva del proyecto.

Garantías de la solución ofertada

Las garantías de las soluciones ofertadas son de 1 año.

Portafolio de producto

Portafolio de soluciones IT



- Centro de entrenamiento especializado.
- Gamma CyberAcademy - Programa de sensibilización en ciberseguridad



- Centro de entrenamiento especializado. EDR - Respuesta y detección sobre endpoint.
- UEM - Gestión unificada de endpoint.
- Antimalware de nueva generación.



- SD-WAN.
- ZTNA.
- Switching y Wireless.
- NAC - Control de Acceso
- NGFW - Next Generation Firewall.
- Balanceo de datacenter.
- Cableado y adecuación de datacenter.



- SEG - Seguridad en e-mail.
- ADC - Balanceo de aplicaciones.
- WAF - Seguridad de aplicaciones web.
- Anti DDoS.
- Doble factor de autenticación.
- CIAM - Autenticación sin contraseña.
- CASB - Seguridad para acceso cloud.
- SASE - Secure Access Service Edge.
- HCI - Hiperconvergencia.
- PAM - Administración de accesos privilegiados.
- Backup seguro (inmutable) y recuperación.



- Monitoreo de red con inteligencia artificial.
- SOAR - Respuesta y automatización y orquestación de seguridad.
- SIEM - correlacionador de eventos de seguridad.
- Pentesting automatizado.
- Deception - Tecnología de engaño y señuelos.
- Sandbox.
- XDR - Detección y respuesta extendida.
- Gestión de vulnerabilidades.



- Servicios profesionales.
- Servicios especializados
- GRC - Gobierno, riesgo y cumplimiento.

Portafolio de Infraestructura IT

USUARIO | INFRAESTRUCTURA TRADICIONAL | INFRAESTRUCTURA DE NUEVA GEN. | NUBE | DRP

- Centro de entrenamiento especializado.
- Gamma CyberAcademy - Programa de sensibilización en ciberseguridad.





USUARIO | INFRAESTRUCTURA TRADICIONAL | INFRAESTRUCTURA DE NUEVA GEN. | NUBE | DRP

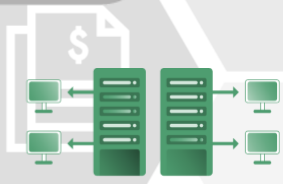
- Servidores.
- SAN / NAS.



USUARIO | INFRAESTRUCTURA TRADICIONAL | INFRAESTRUCTURA DE NUEVA GEN. | NUBE | DRP

- Hiperconvergencia.
- Backup.







- Nube pública.
- Nube híbrida.
- Almacenamiento en la nube.





- Consultoría.
- Replicación.



Portafolio de soluciones Cloud

USUARIO | IAAS | SAAS/PAAS | SERVICIOS PROFESIONALES

- Centro de entrenamiento especializado.
- Gamma CyberAcademy - Programa de sensibilización en ciberseguridad

USUARIO | IAAS | SAAS/PAAS | SERVICIOS PROFESIONALES

- EDR - Respuesta y detección sobre endpoint (Instancias).
- Antimalware de nueva generación (Instancias).
- CNP- Protección nativa de nube
- Backups y protección (kubernetes y dockers)
- Analítica y optimización de recursos Multi-Cloud.
- NGFW- Next Generation Firewall.
- ADC - Balanceo de aplicaciones.
- SEG - Seguridad en e-mail.
- WAF - Seguridad de aplicaciones web.
- Anti DDoS.
- SIEM - Correlacionador de eventos de seguridad.
- Sandbox.
- PAM - Administración de accesos privilegiado



- CASB - Seguridad para acceso CLOUD.
- SASE (Secure Access Service Edge).
- SEG - Seguridad en e-mail.
- WAF - Seguridad de aplicaciones web.
- Backups.
- Anti DDoS.
- GSLB- Balanceo de carga global y datacenter.
- Doble Factor de Autenticación.
- SSPM – Postura seguridad aplicaciones SaaS.



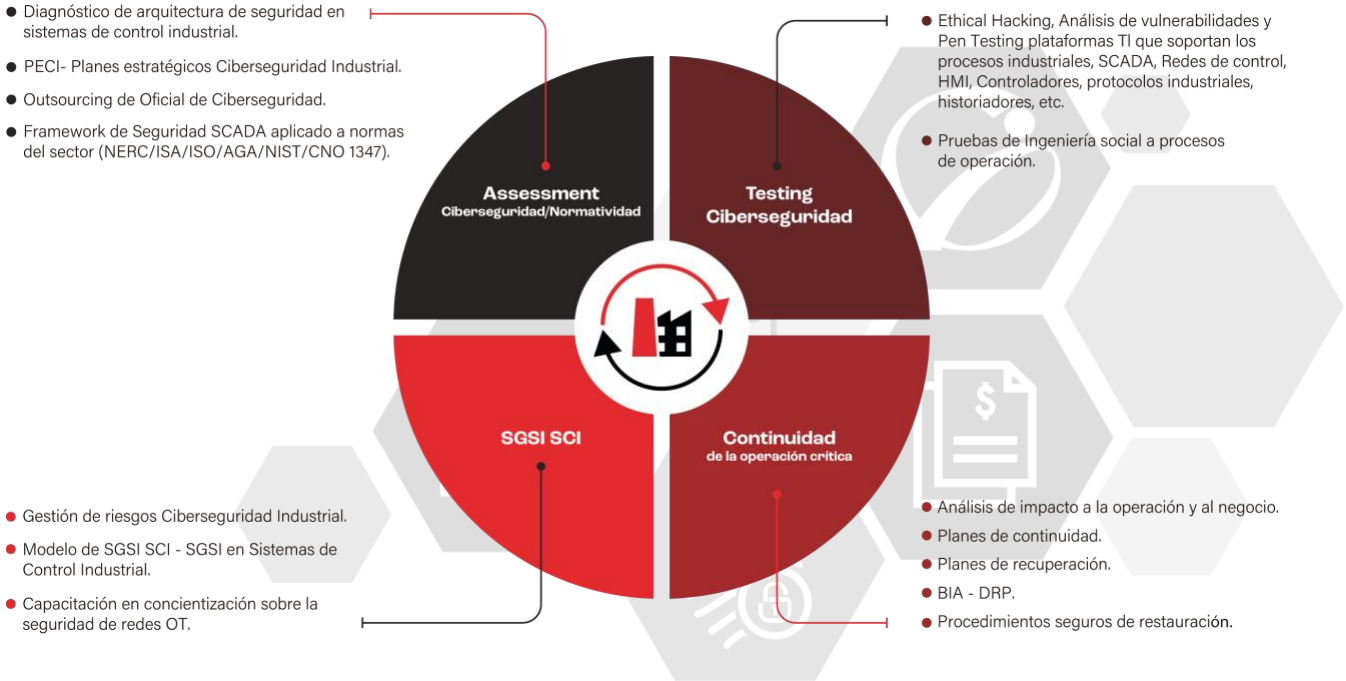
- Servicios profesionales.
- Servicios especializados

Portafolio de soluciones OT

NIVEL 0	Ambiente fisico	
NIVEL 1	Zona de control	• SW/WIFI OT.
NIVEL 2	Zona de monitorización	• EPP/EDR especializado OT. • SW/WIFI OT.
NIVEL 3	Zona de manufactura	• W/WIFI OT. • Sistemas de Hiperconvergencia.
NIVEL 3.5	DMZ Industrial	• SW/WIFI OT. • SIEM OT. • APT/IA OT. • Gestión centralizada para NGFW OT. • Centralización de acción de logs para NGFW OT. • NAC. • Tecnologías de engaño para redes OT
NIVEL 4	Lan Corporativa	• Endpoint EPP/EDR.

NIVEL 5	Internet DMZ corporativa	• NGFW - Next Generation Firewall. • WAF - Seguridad de apl icaciones web. • SEG - Seguridad en e-mail.
RED EXTERNA	Internet	• SD-WAN. • MFA2 - Usuarios remotos. • ZTNA - Acceso Zero Trust a la red. • VPNs OT.

Servicios profesionales OT



Cybersecurity Operation Center



IDENTIFICACIÓN

- Análisis y gestión de riesgos (ISO 31000, 27005).
- Consultoría en ciberseguridad (ISO 27000, ISA 62443, CNO 1241, NIST, PCI, otras).
- CISO como servicio.
- Análisis de código fuente.
- Ingeniería social.
- Ethical Hacking.
- Pentesting.
- Gestión de vulnerabilidades.

PROTECCIÓN

- Gamma BlueTeam.
- Seguridad gestionada MSSP,
- Boletines periódicos de ciberseguridad.
- Servicios de capacitación CyberAcademy

DETECCIÓN

- Servicios de XDR (Respuesta y Detección extendida de amenazas)
  - Monitoreo y alertamientos de anomalías por comportamiento de usuario (UEBA).
  - Correlación de eventos SIEM.
  - Inteligencia Artificial y caza de amenazas persistentes avanzadas.
  - Análisis de eventos e incidentes de Ciberseguridad.
- Gamma RedTeam.
- Protección digital de marca.
- Deception Service.

RESPUESTA

- Gestión a incidentes de ciberseguridad.
  - SOAR — Respuesta automática de incidentes de ciberseguridad.

RECUPERACIÓN

- Apoyo de investigación forense.

Sobre nuestro CSOC

Gamma Ingenieros cuenta con un CSOC (Cyber Security Operations Center) ubicado en la ciudad de Bogotá, certificado en ISO 27001 donde realizamos todo el monitoreo de nuestros clientes brindando soporte permanente, minimizando los riesgos de nuestros clientes en cuanto disponibilidad, confidencialidad e integridad de la información.

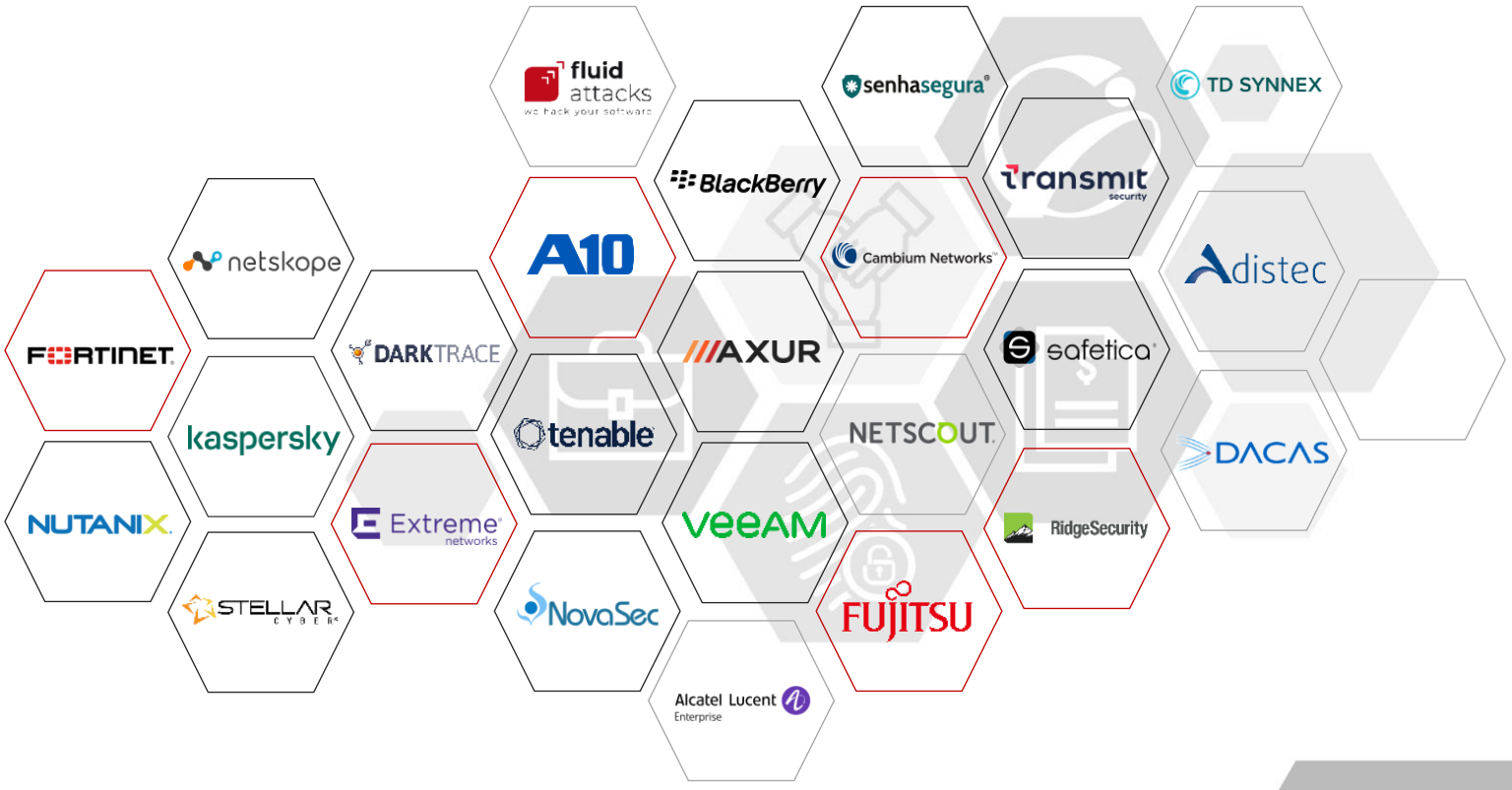
El CSOC cuenta con alianzas con los fabricantes más importantes de la industria y entidades de certificación en normas internacionales como PCI DSS, ISO 27001, SOX entre otras. Contamos con acuerdos de valor que benefician a nuestros clientes.



- Detectar, reportar y evaluar incidentes de seguridad de la información.
- Responder a incidentes de seguridad de la información, incluida la activación de controles adecuados para la prevención y la reducción de impactos, y la recuperación de ellos (por ejemplo, en el soporte para las áreas de gestión de crisis).
- Reportar las vulnerabilidades de seguridad de la información que aún no han sido aprovechadas para causar eventos de seguridad de la información y posiblemente incidentes de seguridad de la información, evaluarlas y tratarlas adecuadamente.
- Aprender de los incidentes y vulnerabilidades de seguridad de la información, implementar controles preventivos y hacer mejoras al enfoque global para la gestión de incidentes de seguridad de la información.

Nuestros aliados comerciales

Tenemos más de 10 años de relacionamiento con los siguientes fabricantes, la mayoría de ellos, líderes en Partner e IDC. Además, contamos con escalamiento a nivel de fábrica.



Nuestras certificaciones son nuestra carta de presentación

Gamma Ingenieros cuenta con certificaciones internacionales que son garantía de nuestra calidad del servicio y el manejo de la información que nos suministran nuestros clientes, somos certificados ISO 27001, la cual se ha convertido en la principal norma a nivel mundial para la seguridad de la información.

Gamma

ISO 14001 | ISO 9001 | ISO 18001 | ISO 27001 | lacnic csirt | FIRST

Equipo de trabajo

PMP | CYBERSECURITY FOUNDATION | ISO 31000 | ISO 27032 | NETSKOPE | KASPERSKY | NUTANIX

SCR | ITIL | ISO 22301 | ISO 27001 | ISO 27001 | Ethical Hacking | FORTINET NETWORK

Aliados

ENGAGE FORTINET EXPERT PARTNER Integrator, MSSP | kaspersky Platinum Partner | Alcatel-Lucent Enterprise Accredited | NUTANIX RESELLER PROFESSIONAL | netskope prime | aws | DARKTRACE SILVER PARTNER | safetica Certified Associate

OFERTA TÉCNICA

Alcance:

F5 Distributed Cloud se presenta como la solución para fortalecer la seguridad de la infraestructura, ofreciendo balanceo de servicios con DRP, firewall de aplicaciones avanzado, protección antibot y mitigación de ataques como SQLi, XSS, CSRF, botnets y DDoS.

- Solución Distributed Cloud F5
- Servicios profesionales

Oferta Económica

Producto	Precios COP
Distributed Cloud F5	$ 262.547.787
Valor Total	$ 262.547.787

Descripción	Precios COP
Servicios Profesionales	$ 20.060.033
Valor Total	$ 20.060.033
IVA	$ 3.811.406
Total	$ 23.871.439

CONDICIONES COMERCIALES

- Los precios están dados en pesos colombianos
- El plazo de validez de este documento caduca en 30 días a partir de la fecha de presentación de esta oferta. Después de este tiempo no estarán vigente los precios y las condiciones presentadas, por lo cual tendrá que ser actualizada.

Condiciones Facturación

- Se entregará facturación electrónica de acuerdo con la legislación colombiana.

Condiciones Recaudo

- El pago deberá ser anual anticipado

Coridialmente,

