Servicios Administrados de Seguridad de la Información y Comunicaciones (SASIC)

La provisión de estos servicios estará circunscrita a empresas que cuenten con la capacidad, conocimiento y experiencia demostrable para ofrecer servicios relacionados con la implementación de infraestructura virtual de comunicaciones, gestión de infraestructura de comunicaciones on premise; protección a puestos de servicio, servidores y aplicaciones; seguridad de la información tales como el control, aseguramiento, diagnóstico, análisis de vulnerabilidades, metodologías, auditorías, investigación forense y personal especializado en materia de seguridad y tecnologías de la información; ciberseguridad y criptografía.

De manera enunciativa más no limitativa, los proveedores interesados en obtención de este Titulo de Autorización, deberán ser capaces de demostrar experiencia en al menos cuatro de los servicios siguientes:

1. Productos y servicios relacionados con implementación de infraestructura virtual de comunicaciones (nube pública, privada y/o híbrida). – Servicios que incluyan el aprovisionamiento, instalación, migración, habilitación, puesta a punto, gestión, monitoreo, soporte y mantenimiento de los componentes tecnológicos de seguridad y comunicaciones que permiten cumplir los requerimientos de conectividad, comunicación y protección de la red, en al menos los siguientes componentes: Firewalls, Concentradores de VPN, Prevención de intrusos de red IPS, Balanceador de cargas y cifrado SSL, XML y API Gateway, Protección de aplicaciones, Monitoreo de red, Resolución de nombres de dominio, Firewalls para red fuera de banda, Protección contra ataques de denegación, Orquestador de red y Orquestador de multisitios.

2. Servicios de gestión de infraestructura de comunicaciones. - Servicios que incluyan la gestión, monitoreo, soporte, mantenimiento, migración, habilitación y puesta a punto de infraestructura de redes y seguridad incluyendo el licenciamiento, para su óptima operación instalada en los centros de datos on premise, en al menos los siguientes componentes: Switches de core, Switches de distribución, Switches de agregación de baja densidad, Switches de acceso para almacenamiento IP, Switches de agregación de servicios, Routers, Firewalls, Concentradores de VPN, Prevención de intrusos de red, Filtrado de contenido web, Balanceador de cargas y cifrado SSL, XML, Gateway, Protección de aplicaciones, Monitoreo de red, Solución AAA, Resolución de nombres de dominio, Sincronización con NTP, Switches de acceso para red fuera de banda, Switches de core para red fuera de banda, Firewalls para red fuera de banda, Control de acceso a red, Conectividad SFP, Conectividad 10Gbe e Infraestructura de seguridad y comunicaciones legada.

3. Productos o servicios relacionados con protección de información. – Servicios que incluyan la instalación, habilitación, configuración, puesta a punto, gestión, monitoreo, soporte, mantenimiento y licenciamientos de soluciones para puestos de servicio, servidores, aplicaciones y bases de datos que brinden la protección ante las principales vulnerabilidades y amenazas que puedan poner en riesgo y/o comprometer los servicios e información, tales como: Antivirus, Host IPS, Control

de aplicaciones, Prevención de fuga de información, Borrado seguro, Cifrado de disco duro, Antivirus y filtrado de contenido, Antivirus para navegación e internet, Respaldo de correo, Consolas de gestión, Detección y protección contra amenazas avanzadas y Protección de bases de datos.

4. Productos o servicios relacionados con seguridad de la información. - Servicios que incluyan la implementación, gestión, operación, mantenimiento y respuesta a incidentes de los conceptos que complementan el esquema de seguridad institucional de forma consistente y robusta, tales como: Control de accesos y resguardo de contraseñas, Correlación de eventos y pistas de auditoria, Pruebas y Verificación de vulnerabilidades en aplicaciones on premise y en la nube, Pruebas y Verificación de vulnerabilidades en aplicaciones móviles, Pruebas de penetración en ciberseguridad, Prevención de phishing, Escaneo de vulnerabilidades, Análisis forense digital (Adquisición e Investigación), Sistema de gestión de seguridad de la información, Gestión de riesgos, Concientización de seguridad, Evaluaciones de cumplimiento a terceros autorizados.

5. Productos o servicios relacionados con ciberseguridad. – Servicios que incluyan la implementación, gestión, operación y mantenimiento de los conceptos enfocados en la protección de la infraestructura y la información contenida en ella, tales como: Inteligencia de ciberseguridad con Telemetría, Machine learning y Big data, Monitoreo de ciberinteligencia, Inteligencia de amenazas, Tecnología Honey pots, API Gateway, Detección de anomalías en entornos híbridos y Respuesta de incidentes de ciberseguridad.

6. Productos o servicios relacionados con criptografía. – Servicios que incluyan la instalación, configuración pruebas y/o puesta a punto de soluciones de manejo de llaves públicas y certificados digitales implementadas en centros de datos, y/o en la nube (pública, privada e híbrida), Diseño de estrategias y arquitecturas para la recuperación ante desastres, incluyendo los procesos, procedimientos y/o pruebas de validación, Firmado de imágenes y plantillas de máquinas virtuales, Gestión de ciclo de vida de certificados digitales y Solución de sellos digitales de tiempo conforme al estándar RFC 3161.