Descripción:

La provisión de estos servicios estará circunscrita a empresas que cuenten con la capacidad, conocimiento y experiencia demostrable para ofrecer la identificación de los flujos de información críticos del SAT, el diseño arquitectónico, construcción e implementación de una bóveda de datos digital segura, el diseño e implementación de esquemas de seguridad sobre las Bases de Datos e información crítica contenida en ellas, el aseguramiento de los medios de comunicación entre Centros de Datos e implementación de respaldos seguros y restauración de los mismos de manera que el SAT pueda contar con un sitio seguro donde salvaguardar la información crítica de su operación, esquemas de seguridad que permitan el monitoreo y análisis de la información de conductas irregulares, así como, análisis de riesgo a inmuebles y entorno para la protección de infraestructura crítica.

Para lo cual, de manera enunciativa mas no limitativa, los proveedores interesados en la obtención de Título de Autorización, deberán ser capaces de demostrar experiencia en alguno de los siguientes servicios:

1. Diseño, construcción, implementación, puesta en marcha, actualización y mantenimiento de Bóvedas Digitales, así como de cada uno de sus componentes y herramientas, a través de los más altos estándares de calidad y seguridad internacional.

2. Capacitación en el funcionamiento en todos sus vértices de la operación de la Bóveda Digital y cada uno de sus componentes y herramientas.

3. Implementación de servicios de monitoreo y análisis de la información y capacitación.

4. Evaluación, pruebas, análisis y capacitación en relación a amenazas internas y externas sobre el potencial daño de infraestructura, y de la información crítica de organizaciones las cuáles determinen las vulnerabilidades que pueden ser explotadas por terceros, así como implementaciones de modelos de seguridad multicapa para defensa y de reacción de personal.

5. Solución de los diferentes escenarios de riesgos, con la finalidad de llevar a cabo acciones de prevención y toma de decisiones que garanticen la continuidad de la operación.

6. Investigación, estudio y análisis de la información que permita identificar riesgos externos, amenazas y factores de riesgo a que están expuestas las instalaciones.

7. Diagnóstico integral de amenazas y factores de riesgos externos en materia de seguridad basado en la investigación, estudio y análisis de la información.

8. Elaboración de políticas, prácticas, procedimientos y procesos de gobernanza sobre infraestructura e información crítica.