**REQUERMIENTOS DE SEGURIDAD**

Este sección especifica los requerimientos de seguridad que serán satisfechas

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Nivel seguridad 1** | **Nivel seguridad 2** | **Nivel seguridad 3** | **Nivel seguridad 4** |
| **Especificación del modulo criptográfico** | Especificación del modulo criptográfico, limite criptográfico, algoritmos aprobados y modos aprobados de operación. Descripción del modulo criptográfico, incluyendo todos los componentes de hardware, software y firmware. Declaración de las políticas de seguridad de los módulos | | | |
| **Puertos e interfaces del modulo criptográfico** | Interfaces necesarias y opcionales. Especificaciones de todas las interfaces y de todas las entradas y salidas de los recorridos de los datos. | | Puertos de datos para parámetros de seguridad críticos sin protección, lógicamente o físicamente separado de otros puertos de datos | |
| **Roles, servicios y autenticación** | Separación lógica de los roles y servicios necesarios y opcionales | Autenticación del operador basado en roles o identidad | Autenticación del operador basado en identidad | |
| **Modelo de estado finito** | Especificaciones del modelo de estado finito. Estados opcionales y necesarios. Diagrama de transición de estado y especificación del estado de las transiciones | | | |
| **Seguridad física** | Producción de equipo de calidad | Evidencia de manipulación | Detección de manipulación |  |
| **Entorno operacional** |  |  |  |  |
| **Administración de claves criptográficas** |  |  |  |  |
| **EMI / EMC** |  |  |  |  |
| **Auto-pruebas** |  |  |  |  |
| **Garantía del diseño** |  |  |  |  |
| **Atenuación de otros ataques** |  |  |  |  |