OBJETO

En el ámbito de **FMB** y de acuerdo con la aplicación de las **recomendaciones recopiladas en la Normativa: UNE-EN IEC 62443, ISO 27000, ISO 27001**, **CENELEC EN 50126 RAMS y EN 50701 y el Esquema Nacional de Seguridad (CCN),** sobre los criterios del tratamiento de la Ciberseguridad del ámbito OT, el presente documento efectúa una recopilación sobre los conceptos recogidos dentro del listado SuC (Sistem under consideration) necesarios a cumplimentar para la correcta gestión interna de los sistemas ferroviarios operados y/o mantenidos por FMB. Así mismo, el presente documento adjunta un modelo completo de listado SuC y los detalles para su correcta cumplimentación.

DEFINICIÓN DEL SuC

El sistema en consideración (SuC) forma parte del sistema ferroviario, compuesto por subsistemas y componentes que proporcionan la funcionalidad requerida. Las amenazas de ciberseguridad pueden comprometer esta funcionalidad y afectar la seguridad, finanzas o disponibilidad del sistema. Para identificar estas amenazas, es necesario describir el SuC, sus funciones y todas sus interfaces.

Las siguientes reglas se aplican para la descripción del SuC:

- La definición del SuC deberá contener el alcance y los límites del sistema que se va a desarrollar y evaluar.
- El SuC es parte de un sistema operativo para controlar los sistemas técnicos relacionados con el ferrocarril.
- La descripción funcional y arquitectónica del SuC debe seguir el enfoque jerárquico dado en EN 50126-1:2017, 5.2 para identificarlo exactamente, incluidos los bordes y las interfaces externas.

DESCRIPCIÓN FUNCIONAL GENERAL

La ubicación del SuC dentro de la arquitectura ferroviaria indica a qué tipo de sistema pertenece (como material rodante, señalización o infraestructura) y qué funciones principales desempeña. Para identificar las amenazas de ciberseguridad del SuC, incluidas las vulnerabilidades conocidas, es necesario definir sus funciones, límites y la funcionalidad que proporciona. Por lo tanto, la identificación de las funciones principales debe detallarse considerando:

- El objetivo o propósito del SuC, que incluye la definición de sus funciones, límites y las interfaces del sistema.
- Los escenarios operativos que describen cómo se utilizará el SuC y qué actores interactúan o interfieren con él.
- El contexto de implementación y uso.
- La vida útil esperada del SuC, considerando las posibles actualizaciones necesarias en hardware y software.
- Los planes y conceptos de mantenimiento.
- Las restricciones ambientales que afectan al SuC.

CONCEPTOS RECOGIDOS DENTRO DEL *LISTADO SuC*

- **ID*:** identificador único asociado al activo. *Este campo sólo lo completará el personal de TMB.

- **CARACTERÍSTICAS HARDWARE (HW):** características referidas a la parte física del activo donde se aclaran los detalles sobre la procedencia del mismo y otros datos que se requiere para su identificación única dentro del conjunto de activos.

  Los campos que se especifican en este apartado son los siguientes:

  - **Identificador:** conjunto de letras y/o números que sirven para identificar un activo por parte de la empresa.
  - **Descripción:** Explicación del producto. Ejemplo: Ordenador portátil.
  - **Marca**: marca actual a la que pertenece el activo.
  - **Modelo**: modelo al que pertenece el activo.
  - **Nº de serie**: código alfanumérico que identifica el activo, puede contener sólo número o contener letras.
  - **Fabricante** (campo de SAP): empresa que produce el activo.
  - **Proveedor** (campo de SAP): empresa que vende el activo. Puede ser la misma que el fabricante u otra diferente.
  - **Tipo**:
    - *Físico:* activo tangible. Ejemplo: dispositivos como un móvil o un sensor.
    - *Virtual:* activo intangible. Ejemplo: base de datos.
  - **Dirección M.A.C***: identificador único que cada fabricante le asigna a la tarjeta de red de sus dispositivos. Ejemplo: 00:1e:c2:9e:28:6b *Si procede.

- **CARACTERÍSTICAS SOFTWARE (SW):** características de la parte no física del activo, es decir, el conjunto de programas y datos que permite que realice determinas acciones. Puede ser el mismo en diferentes activos.

  Los campos que se especifican en este apartado son los siguientes:

  - **Sistema Operativo*:** Sistema Operativo o software del activo. Ejemplo: Windows. *Si procede.
  - **Versión del Sistema Operativo**: versión actual del sistema operativo. Ejemplo: XP.
  - **Firmware**: firmware instalado en el sistema. Especificar nombre del mismo.
  - **¿Actualización del Firmware?**: si se ha realizado algún tipo de actualización en el firmware del activo, marcar "SI" y especificar la nueva versión. Si no se ha actualizado indicar "NO".
  - **¿Requiere parcheado?:** si se requiere especificar "SI" y el tipo, en caso contrario indicar "NO".

- **DATOS DE COMPRA / MANTENIBILIDAD:** Datos para identificar criterios financieros, ambientales, de impacto social, de gestión de riesgos, calidad de servicio, seguridad y desempeño a lo largo de la vida del activo.

  Los campos que se especifican en este apartado son los siguientes:

  - **Fecha fabricación (campo de SAP**): indicar día, mes y año de la fabricación del activo en formato DD/MM/AA.
  - **Fecha adquisición (campo de SAP)**: indicar día, mes y año de la compra del activo en formato DD/MM/AA.
  - **Fecha PES (campo SAP):** indicar día, mes y año de la puesta en marcha del activo en formato DD/MM/AA.
  - **Fecha inicio de garantía:** indicar día, mes y año del inicio de la garantía del activo en formato DD/MM/AA.
  - **Fecha fin de garantía:** indicar día, mes y año del fin de la garantía del activo en formato DD/MM/AA.
  - **Valor de adquisición (campo de SAP)**: valor de compra (en **euros**) del activo.
  - **Fiabilidad de referencia:** previsión de la capacidad para ejecutar correctamente una función sostenida en el tiempo del activo. Desde el punto de vista de conocer los posibles modos de fallo del sistema, su probabilidad de ocurrencia asociada y el efecto a su funcionalidad. Valor del equipo o de la media de la familia del activo.
  - **Años de ciclo de vida:** previsión de tiempo en el cual el activo realizará su funcionamiento de forma nominal.

- **EMPLAZAMIENTO:** localización de los diferentes activos en relación al espacio físico o virtual y en referencia a un sistema.
  Los campos que se especifican en este apartado son los siguientes:

  - **Ubicación:** localización específica, física o virtual, dónde se encuentra el activo.
  - **Servicio esencial al que pertenece:** servicio de referencia al que corresponde el activo.

- **INTERFACES:** El SuC puede verse comprometido mediante el acceso a través de sus interfaces, tanto humanas como técnicas. Estas interfaces pueden permitir que dispositivos no autorizados se conecten al sistema, o que se acceda a través de redes de comunicación. Para proteger el SuC, es importante contar con una lista completa de todas sus interfaces, que incluya la definición de:

  - **Función interfaz:** función para la que se utiliza cada interfaz.
  - **Protocolo de transporte:** protocolo utilizado (como TCP o UDP), si está disponible.

- **Tipo de conexión física:** tipo de conexión como cable de cobre, fibra óptica o inalámbrica.
- **Datos funcionales:** datos que se manejan por la interfaz.
- **Impacto:** impacto en caso de pérdida de confidencialidad, integridad o disponibilidad.
- **Función sistemas adyacentes:** función que tienen los sistemas vecinos.
- **Interfaces organizacionales:** interfaces que interactúan con el SuC.

- **OBSERVACIONES:** texto libre para incluir, si se desea, cualquier aclaración al respecto de lo comentado anteriormente.

COMMON PLATFORM ENUMERATION (CPE)

Se trata de un estándar que permite identificar de manera única y estandarizada software, hardware y sistemas operativos. Este sistema de nomenclatura facilita la comunicación sobre productos de tecnología de la información, especialmente en el contexto de seguridad informática y gestión de vulnerabilidades.

El formato general de un CPE es:

cpe:cpe_version:[part]:[vendor]:[product]:[version]:[update]:[edition]:[language]:[sw_edition]:[target_sw]:[target_hw]:[other]

Componentes del CPE:

1. **cpe:** Indica que es un identificador de CPE.
2. **cpe_version:** Es la versión del formato CPE. Actualmente, la versión más utilizada es 2.3.
3. **part:** Tipo de producto, que puede ser:
   - *a (application)* para aplicaciones.
   - *o (operating system)* para sistemas operativos.
   - *h (hardware)* para hardware.
4. **vendor:** Nombre del proveedor o fabricante del producto.
5. **product:** Nombre del producto.
6. **version:** Versión del producto (puede ser un rango o un asterisco * si no se especifica).
7. **update:** Actualización o parche específico (puede ser un rango o un asterisco * si no se especifica).
8. **edition:** Edición del producto (por ejemplo, "Professional", "Enterprise").
9. **language:** Idioma del producto (por ejemplo, "en" para inglés).
10. **sw_edition:** Edición específica del software, si corresponde (generalmente se utiliza para software empresarial).
11. **target_sw:** Software de destino, que puede ser afectado por el producto.
12. **target_hw:** Hardware de destino, que puede ser afectado por el producto.
13. **other:** Cualquier otro atributo adicional que no se haya cubierto en los campos anteriores.