# Pasarelas de intercambio seguro de información

## 1. ¿Qué es una pasarela de intercambio seguro de información?

Las pasarelas de intercambio seguro de información son dispositivos de protección de perímetro especialmente diseñados para controlar el intercambio de información entre sistemas con diferentes niveles de clasificación y evitar así que se establezcan flujos de información no autorizados.

Como dispositivos de protección de perímetro, son más seguros que un cortafuegos o un proxy, ya que separan físicamente dos sistemas, impiden que se establezcan conexiones de ningún nivel dentro de las capas del modelo OSI y analizan el contenido de la información de acuerdo a unas reglas previamente definidas. Esto permite implementar eficientes mecanismos de defensa en profundidad y neutralizar o minimizar el efecto de las APT[1].

## 2. ¿Qué funcionalidades de seguridad aporta?

Aunque existen diferentes implementaciones, que dependen de las necesidades del sistema y de las características de la información que van a intercambiar, de manera genérica las pasarelas de intercambio seguro de información aportan las siguientes funcionalidades de seguridad:

- Separación de redes. Ruptura de la continuidad de los protocolos de comunicaciones entre dos redes interconectadas en todas las capas del modelo OSI. Así, las pasarelas suelen estar formadas por dos unidades, una que se conecta a la red interna (la que se protege) y otra a la externa, unidas por un dispositivo pasivo de lectura y escritura. Ambas unidades se comunican mediante un protocolo desarrollado *ad-hoc*, que impide que utilicen simultáneamente los mismos recursos. De esta forma, se asegura que nunca se establece una conexión TCP/IP entre las entidades origen y destino, independientemente de la configuración software del dispositivo, ni que a la red externa lleguen paquetes con información de la red interna.

[1] *Advanced Persistent Threat.* Amenazas persistentes avanzadas

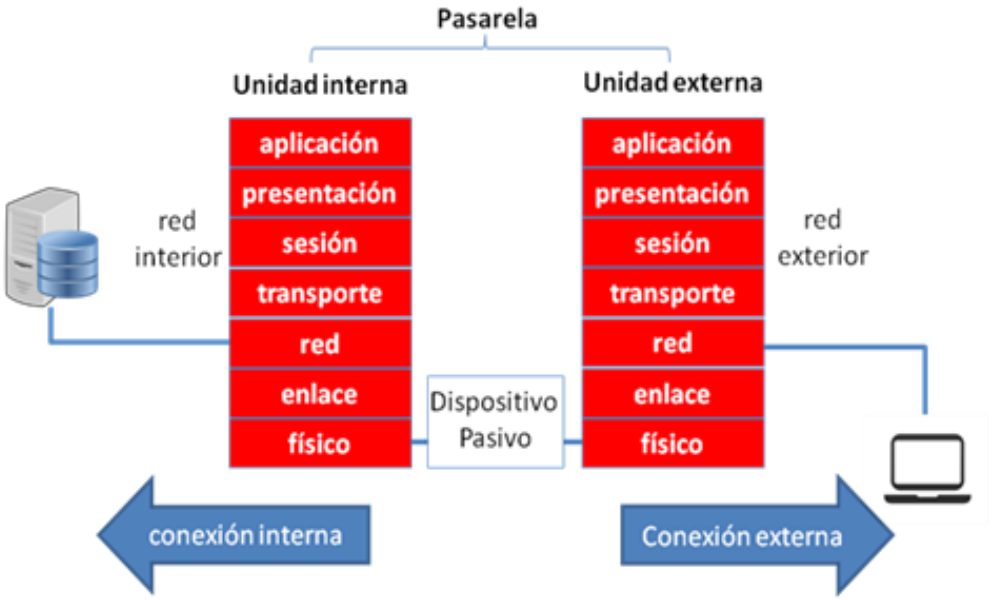


Figura 1. Pasarela de intercambio seguro

- Filtrado de contenidos. Las pasarelas analizan el contenido del paquete y permiten el paso de información siempre que cumpla las reglas de filtrado definidas, tanto para la entrada como para la salida. También posibilitan la utilización de mecanismos de firma digital, solos o en combinación con otros basados en etiquetado de información sensible, para el control de flujo de información, de tal manera que solo aquello que se encuentre firmado pueda salir de la red interna. Este control basado en firma digital está enfocado a sistemas que manejan información a la que se le exige un nivel muy alto de confidencialidad.
- Separación de flujos de información de entrada/salida.
- Sanitización de la toda la información relativa a la red interna.

## 3. ¿Cuándo es necesario utilizar este tipo de productos?

### 3.1 Organismos afectados por el ENS

Las pasarelas de intercambio seguro no se exigen en el Esquema Nacional de Seguridad; no obstante, pueden ser una opción recomendable para algunos organismos, dependiendo de los entornos y activos esenciales a proteger. Para más información puede consultar la guía CCN-STIC-811 "Interconexión en el ENS".

### 3.2 Organismos que manejen información clasificada

En el caso de que disponga de un sistema que maneje información nacional clasificada o equivalente puede consultar la guía CCN-STIC-302 "Interconexión de sistema de las tecnologías de la información y las comunicaciones que manejan información nacional clasificada en la administración" para obtener más información sobre cuándo se debe utilizar una pasarela de intercambio seguro de información.

## Contacto


| | |
|---|---|
| **Correo electrónico CCN-PYTEC** | ccn-pytec@cni.es |
| **Twitter** | **@CCNPYTEC** |
| **LinkedIn** | **https://www.linkedin.com/company/CCN-PYTEC** |