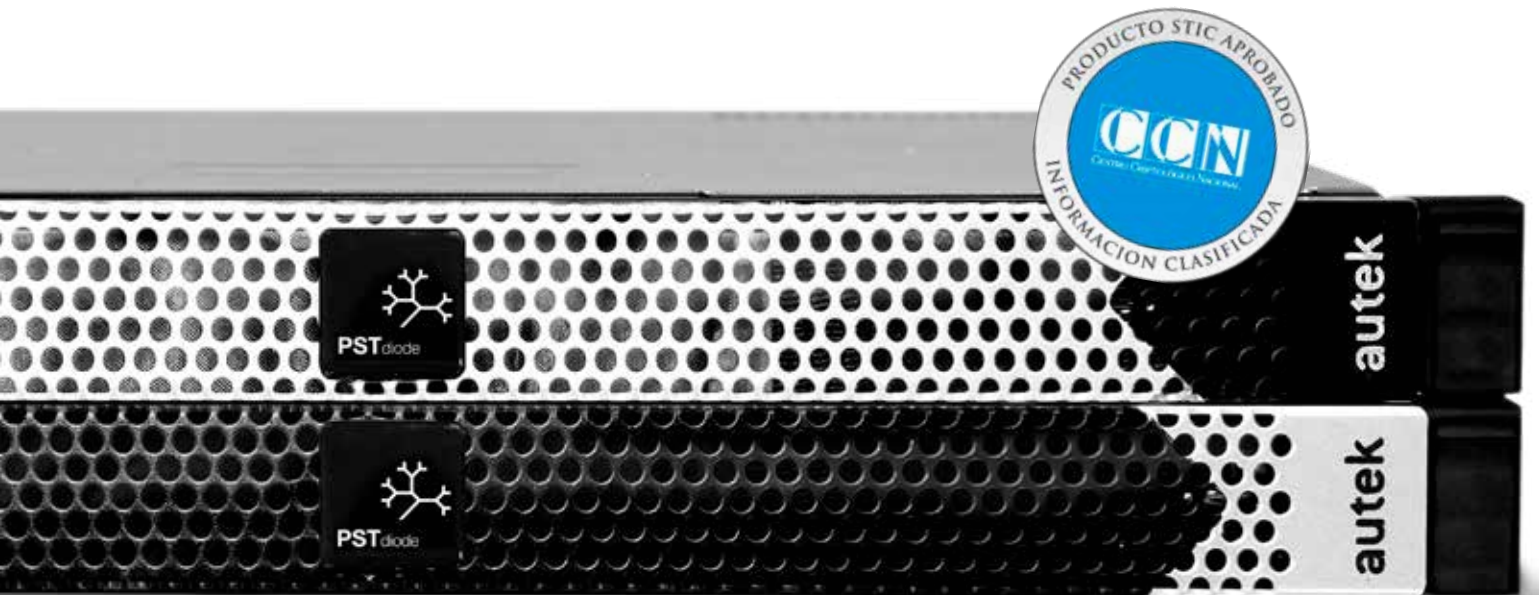


**PST**diode

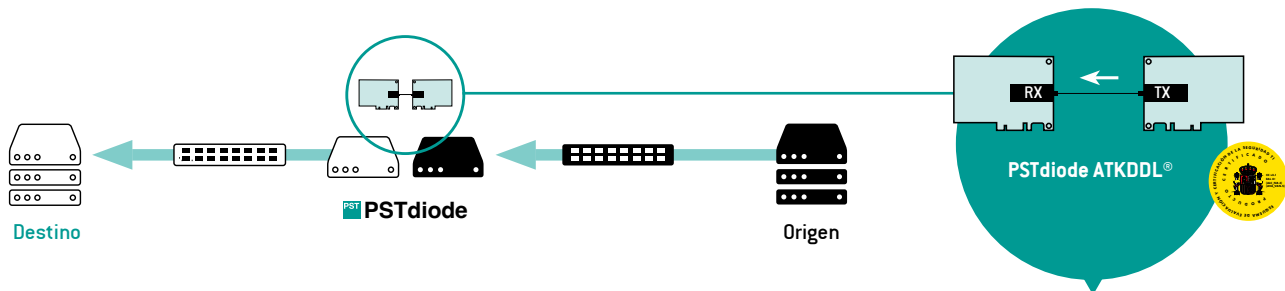


Introducción - Especificaciones técnicas

# Diodo de datos hardware



## VISIÓN GENERAL



PSTdiode transfiere información en un único sentido entre dos dominios de seguridad aislados con garantía física de transmisión unidireccional.

PSTdiode está formado por dos *appliances* de 19" con la parte correspondiente del hardware de comunicación unidireccional en cada uno de ellos y con todo el software necesario instalado (firmware). El firmware de los *appliances* está

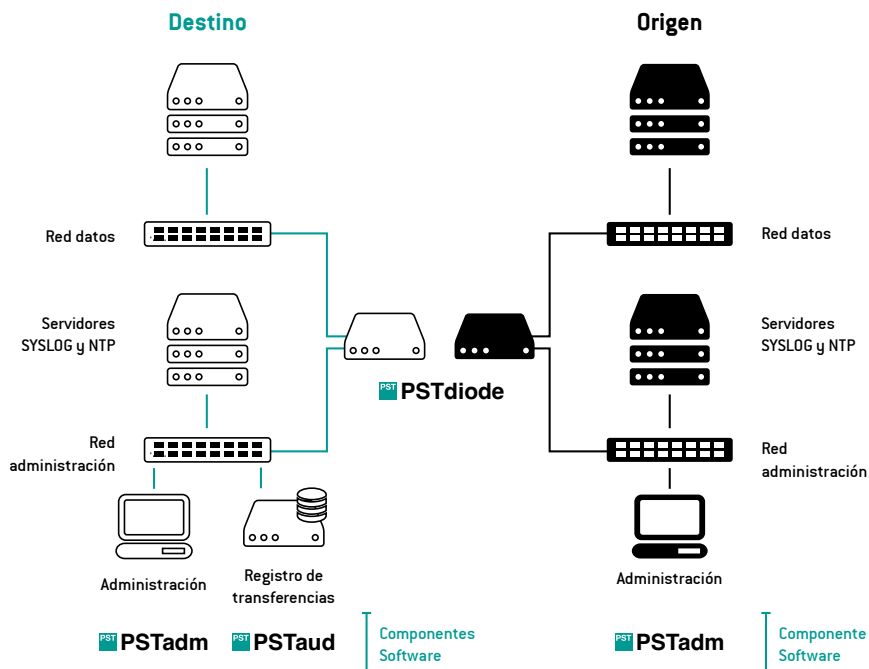
personalizado y securizado, se ejecuta desde una partición de solo lectura y se incluye una herramienta de control de integridad de la partición. El firmware es fácilmente actualizable y se mantiene la configuración en el proceso.

El sistema se configura remotamente una vez establecidos, en ambos *appliances*, los parámetros de red y PKI mediante una interfaz local.

Basado en el dispositivo de comunicación unidireccional PSTdiode ATKDDL® desarrollado por Autek Ingeniería y certificado Common Criteria EAL 4+ [AVA\_VAN.5, ALC\_FLR.3].

Este dispositivo se compone de una tarjeta transmisora (TX) y una tarjeta receptora (RX) unidas mediante un cable de fibra óptica.

**EL SISTEMA SE INTEGRA CON LA INFRAESTRUCTURA EXISTENTE: NO ES NECESARIO INSTALAR PROXIES, NI SERVIDORES DEDICADOS ADICIONALES.**



Se incluyen dos componentes software adicionales, uno para la administración (PSTadm) y otro para el registro de transferencias (PSTaud), que funcionan en ordenadores de propósito general. PSTadm permite distintos ro-

les de administrador, gestionados mediante autenticación basada en certificados. El sistema registra todas las transferencias realizadas a través del servicio de registro de transferencias (PSTaud); este registro puede realizar-

se en una base de datos o en ficheros. Adicionalmente el sistema envía información de funcionamiento y de seguridad mediante eventos de SYSLOG en ambas redes.

## TRANSFERENCIA ACTIVA DE FICHEROS

El servicio 'Entrada de ficheros' de PSTdiode transfiere ficheros en un único sentido, de manera activa entre dos dominios de seguridad aislados.

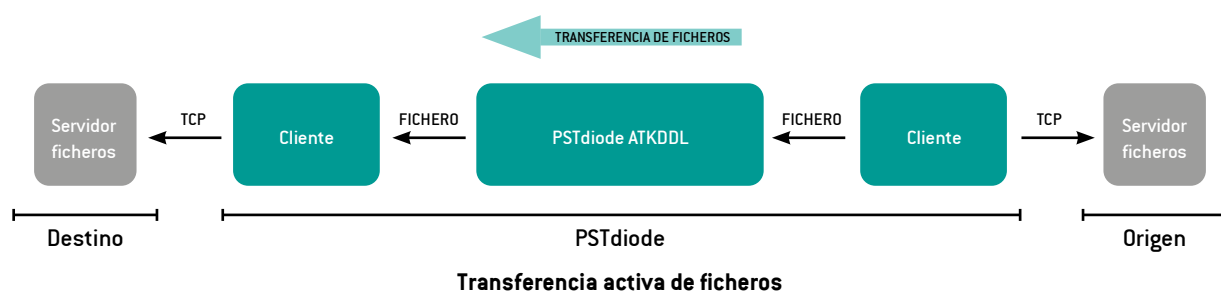
La transferencia de ficheros se define mediante canales. Un canal establece la correspondencia entre un origen de datos [servidor, ruta] y un destino [servidor, ruta].

El sistema se integra con la infraestructura existente, cada uno de los *appliances* accede a servidores de ficheros mediante protocolos estándar.

El *appliance* origen accede a los servidores de ficheros, como cliente de los protocolos (FTP, FTPS, SFTP ó SMB) cada cierto tiempo y transfiere el contenido al *appliance* destino. El *appliance* destino recibe los ficheros y los transfiere a los servidores de ficheros, también como cliente del protocolo.

El sistema permite configurar diferentes opciones de transferencia por canal:

- Modo recursivo: Se comprueban los subdirectorios dentro del origen.
- Repetición inteligente: Se repite el envío (número de veces e intervalo configurables) pero no se vuelven a subir al destino los ficheros ya transferidos correctamente.
- Cuarentena: Los ficheros enviados se mueven a una ubicación temporal en el origen.
- Borrado automático: Permite borrar los ficheros transferidos.
- Filtrado de ficheros: Capacidad de filtrar por nombre, extensión o tamaño.



## CARACTERÍSTICAS

Organización en canales	<p>El flujo de datos se configura mediante canales de comunicación.</p> <p>Un canal establece la relación entre un directorio en un servidor de ficheros en la red de origen y un directorio en un servidor de ficheros en la red de destino.</p> <p>Los canales permiten una monitorización visual e intuitiva.</p> <p>Los canales trabajan en paralelo y pueden ser activados y desactivados independientemente.</p>
Prioridad de los canales	<p>La prioridad de los canales permite establecer los recursos dedicados (frecuencia de acceso al servidor, número de ficheros por ciclo, capacidad de almacenamiento temporal, etc.) al canal mediante tres niveles: alto, medio y bajo.</p>
Protocolos soportados	FTP, FTPS, SFTP y SMB.
Número máximo de canales	50
Tamaño máximo de fichero	50 GB
Capacidades de filtrado	Filtrado por nombre del fichero, extensión o tamaño.

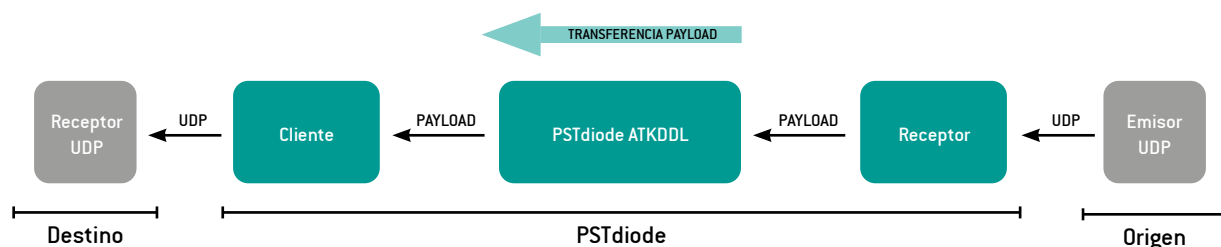
## TRANSFERENCIA 'PAYLOAD' UDP

El servicio 'Entrada UDP' de PSTdiode transfiere el contenido de paquetes UDP ('payload') de la red origen a la red destino. Su baja latencia permite el uso en aplicaciones de 'tiempo real' (streaming).

La transferencia de UDP se define mediante canales. Un canal establece la correspondencia entre un puerto de escucha en el *appliance* origen y un receptor del paquete UDP (servidor, puerto) en la red destino.

El *appliance* origen espera paquetes UDP en el puerto configurado y transfiere el 'payload' al *appliance* destino. El *appliance* destino crea un nuevo paquete y envía el 'payload' al receptor configurado.

El sistema permite establecer filtros de tamaño y origen por canal. Además soporta la recepción y envío unicast y multicast.



Transferencia 'payload' UDP

## CARACTERÍSTICAS

Organización en canales	<p>El flujo de datos se configura mediante canales de comunicación.</p> <p>Un canal establece la correspondencia entre un puerto en el <i>appliance</i> origen y un receptor del paquete UDP (servidor, puerto) en la red destino.</p> <p>Los canales permiten una monitorización visual e intuitiva.</p> <p>Los canales trabajan en paralelo y pueden ser activados y desactivados independientemente.</p>
Protocolos soportados	UDP
Métodos de transmisión	Recepción y envío unicast o multicast en ambos dominio.
Número máximo de canales	10
Retardo medio típico	150 milisegundos
Capacidades de filtrado	Filtrado por tamaño y origen.

## CARACTERÍSTICAS GENERALES

Topología	Dos <i>appliances</i> , cada uno conectado a un dominio de seguridad, la comunicación entre ambos se realiza exclusivamente a través de fibra óptica.
Topología de administración	Interfaz de administración separada (configurable) en ambos <i>appliances</i> .
Despliegue	<i>Appliances</i> listos para usar. El sistema se configura remotamente una vez establecidos, en ambos <i>appliances</i> , los parámetros de red y PKI mediante una interfaz local.
Administración	El sistema se monitoriza mediante PSTadm desde el dominio de destino. La administración remota del <i>appliance</i> del dominio de origen sólo es necesaria para cambios de configuración y solución de problemas.
Roles de administración	El sistema permite definir 4 roles diferentes de administración: <ul style="list-style-type: none"> <li>• Administrador raíz</li> <li>• Administrador de seguridad</li> <li>• Administrador de servicios</li> <li>• Administrador de monitorización</li> </ul>
Estado y notificaciones de error	El sistema envía eventos de SYSLOG de funcionamiento y seguridad de manera independiente.
Registro de transferencias	Es posible registrar la información de las transferencias realizadas en ficheros o base de datos. Se realiza mediante un componente software separado (PSTaud) que funciona en un ordenador de propósito general ubicado en la red destino.
Sincronización automática de hora	El sistema permite configurar la sincronización de hora a través de servidores NTP en ambos dominios.
Tasa de transferencia	La tasa de transferencia del dispositivo PSTdiode ATKDDL es 1 Gbps.

## SEGURIDAD

Topología	Interfaz de administración dedicada e independiente que permite separar todo el tráfico de administración del tráfico de datos en ambos <i>appliances</i> .
Estado y notificaciones de error	Los eventos de seguridad se pueden tratar de manera separada.
Comunicaciones de administración	Solo los administradores autorizados, mediante certificados digitales, pueden administrar el sistema. Las comunicaciones de los componentes software con los <i>appliances</i> están protegidas mediante TLS con autenticación del extremo remoto. Se registran todos los accesos y operaciones realizados por los administradores del sistema.
Garantía de integridad del firmware	Todo el software (incluido el sistema operativo) se ejecuta desde una partición de solo lectura, cuya integridad puede ser verificada en cualquier momento.

## DATOS TÉCNICOS DE LOS APPLIANCES

### Conexiones

Interfaz de video	VGA 15 pines
Interfaz teclado	USB tipo A
Interfaz red de datos	RJ45 (Ethernet 10/100/1000 Mbps)
Interfaz red de administración	RJ45 (Ethernet 10/100/1000 Mbps)

### Características físicas

Dimensiones	4,28 cm (1U) x 48,2 cm (19") x 57,36 cm
Peso	9,20 kg

### Alimentación

Conector	IEC-60320-C14
Potencia	450W
Disipación de calor máxima	1725 BTU/hr
Tensión	100-240 V AC, 50/60 Hz

### Temperatura

Funcionamiento	De 0°C a 45°C
Almacenamiento	De -40°C a 65°C

## IDENTIFICACIÓN

### Referencia (Part Number)

### NSN

PSTdiode U2	5895-33-219-0484	Sistema completo. Incluye <i>Appliance</i> Origen y <i>Appliance</i> Destino.
PSTd-U2	5895-33-219-0485	<i>Appliance</i> Destino (frontal blanco).
PSTs-U2	5895-33-219-0486	<i>Appliance</i> Origen (frontal negro).

## CERTIFICACIONES Y APROBACIONES



Certificado Common  
Critería EAL 4+  
(AVA\_VAN.5, ALC\_FLR.3)



Producto STIC aprobado  
para el manejo de  
información clasificada



Incluido en el catálogo NIAPC

Autek Ingeniería, S.L.  
Av. Burgos 9, of.1. E-28036 Madrid (España)  
Tel. +34 915 974 629  
info@autek.es | www.autek.es

