

# Protección contra amenazas de seguridad, racionalización de la prestación de servicios



## RESUMEN EJECUTIVO

**Organización:** Gobierno de Castilla-La Mancha

**Sector:** Público

**Ubicación:** España

**Empleados:** 63.000

### Desafío

- Racionalizar la prestación de servicios públicos del gobierno regional
- Identificar los hábitos de navegación de los usuarios para asignar las políticas de seguridad adecuadas
- Actualizar y simplificar la gestión del correo electrónico con una solución de seguridad de correo electrónico fácil de instalar

### Solución

- Cisco Web Security Appliance
- Cisco Email Security Appliance
- Cisco ASA 5585-SSP-60 Adaptive Security Appliance

### Resultados

- Se han reducido significativamente las amenazas de malware, mejorando la experiencia del usuario
- Se ha estabilizado la seguridad del correo electrónico, mejorando drásticamente el rendimiento
- Se han suministrado soluciones fáciles de implantar y gestionar, que ahorran tiempo al personal de TI para que pueda ocuparse de otras tareas

El Gobierno de Castilla-La Mancha asegura el acceso a Internet y al correo electrónico con Web Security Appliance y Email Security Appliance.

## Desafío

El Gobierno de Castilla-La Mancha en España ofrece servicios de salud, educación y gestión para una población muy dispersa de más de dos millones de habitantes. El Gobierno regional emplea aproximadamente a 20.000 trabajadores de la salud, 18.000 educadores, 12.000 teletrabajadores con acceso remoto y 12.000 administradores. El gobierno también es responsable de la gestión de las necesidades agrícolas y económicas de la región.

Un equipo de tan solo cuatro profesionales de TI se encarga de la implantación y gestión de la red de TI y seguridad para toda esta diversidad de empleados en la región más grande de España. Con recursos limitados, el equipo de TI debe confiar en la racionalización de sus operaciones para prestar los servicios de forma segura a los residentes y las empresas de la región.

"Proporcionamos servicios de Internet para maestros, trabajadores sanitarios, así como empleados públicos. Cada grupo tiene sitios web que visitan como parte de su trabajo", comenta Pedro Jesús Rodríguez González, coordinador de Tecnologías de la Información de la Junta de Comunidades, Gobierno de Castilla-La Mancha. "Necesitábamos una solución que pudiese gestionar las diferentes identidades, gestionar las URL de los sitios web que visitaban y, en caso necesario, resolver rápidamente el acceso a las direcciones bloqueadas".

Debido al acceso de diferentes usuarios e identidades a la red, era una preocupación mantener una seguridad elevada de la red. La organización necesitaba una manera más sencilla de controlar los diferentes perfiles de usuarios y asegurarse de que estos podían acceder a los recursos que necesitaban protegiendo al mismo tiempo la red central. También tenían que ser capaces de gestionar de forma centralizada su red, considerablemente ampliada, sin contratar a nuevo personal.

Además, para abordar las necesidades de la creciente región, el equipo de TI también necesitaba encontrar una manera de asegurar su sistema de correo electrónico de 100.000 usuarios y gestionar 500.000 mensajes al día, protegiendo la red contra amenazas de correo electrónico entrantes y salientes.

"Antes teníamos que recopilar la información sobre los problemas de diferentes informes. Con Cisco WSA, cuando un usuario informa de un problema, es fácil ver de qué está hablando y empezar a resolverlo".

---

Pedro Jesús Rodríguez González  
 Coordinador de Tecnologías de la Información, Junta de Comunidades  
 Gobierno de Castilla-La Mancha.

## Solución

El equipo de TI de Castilla-La Mancha buscó una solución que pudiese satisfacer los requisitos de las políticas de identidad y acceso, junto con una fuerte seguridad web adicional. Después de analizar las diferentes opciones del mercado, el equipo de TI seleccionó Cisco® Web Security Appliance (WSA), Cisco Email Security Appliance (ESA) y ASA 5585 Adaptive Security Appliance para ayudarles a abordar las necesidades de la organización. Cisco Identity Services Engine (ISE) y TrustSec® respaldan el uso de los dispositivos inalámbricos que acceden a la red.

Con Cisco WSA, el gobierno cuenta ahora con una mejor defensa contra amenazas, una protección avanzada contra malware, así como visibilidad y control de aplicaciones.

"Antes de la solución de Cisco –sobre todo en lo que se refiere a nuestra gestión de malware y URL– teníamos que dedicar mucho tiempo a la gestión de listas negras y listas blancas. Había una tasa enorme de errores de clasificación, lo que suponía una tasa de disponibilidad baja", afirma Rodríguez González.

Además, el grupo de TI necesitaba informes completos y más sencillos. "Antes teníamos que recopilar la información sobre los problemas de diferentes informes", dice Rodríguez González. "Con Cisco WSA, cuando un usuario informa de un problema, es fácil ver de qué está hablando y empezar a resolverlo".

WSA también proporciona a Castilla-La Mancha un control completo sobre cómo acceden los usuarios finales a Internet. Mediante la identificación de cientos de aplicaciones y más de 150.000 microaplicaciones, WSA ha ayudado al personal de TI a crear políticas que responden a las diferentes necesidades de los empleados de los sectores de la salud, la educación y público. Se pueden permitir o bloquear características específicas como chat, mensajería, vídeo y audio de acuerdo con los requisitos de los distintos departamentos y usuarios, sin la necesidad de bloquear sitios web completos.

Castilla-La Mancha también confía en Cisco Email Security Appliance (ESA) para proporcionar una protección avanzada contra amenazas, bloquear el spam y desarrollar políticas fáciles de aplicar.

"Con más de medio millón de correos electrónicos al día, los volúmenes de spam en constante aumento constituyen un desafío permanente", afirma Rodríguez González.

Gracias a ASA 5585 Adaptive Security Appliance, el equipo de Castilla-La Mancha puede permitir o denegar el acceso desde y hacia las diferentes partes de sus servicios regionales y su red corporativa, cada uno con su propio sitio web.

También señala que esta población activa incluye usuarios que utilizan dispositivos móviles como ordenadores portátiles, mientras que otros utilizan equipos de sobremesa o estaciones de trabajo. Castilla-La Mancha puede abordar las necesidades inalámbricas de ambos protegiendo la red mediante el uso de Identity Services Engine para controlar quién tiene acceso, a qué parte de la red y qué dispositivo utiliza, incluyendo además el uso de Wireless Controller.

## Resultados

Los resultados de las nuevas soluciones se han visto casi de inmediato. El equipo de TI tiene ahora una visión más centralizada y capacidades de generación de informes bajo demanda de toda su red de WSA a través de Content Security Management Appliance. La capacidad de seguir el tráfico de Internet en tiempo real permite al equipo gestionar las amenazas conforme surgen y realizar cambios a medida que las necesidades cambian.



La suma de unos informes más detallados permite a Castilla-La Mancha crear informes específicos de forma segura, incluyendo los sitios web más visitados, el uso del ancho de banda, y los virus y malware que han sido bloqueados.

El equipo puede elaborar informes en función de cómo se clasifican sus sitios web específicos, para conocer qué categoría es la más visitada por los usuarios, como gobierno y legislación, o redes sociales.

WSA ha proporcionado una experiencia en línea mejor y más segura para sus usuarios con un mejor rendimiento, producción y redundancia. Además, los usuarios solo tienen que introducir sus credenciales una vez; el equipo está estudiando aprovechar el inicio de sesión único en el futuro.

Por otra parte, el equipo también tiene como objetivo aprovechar ISE y TrustSec en el futuro con vistas a integrar las redes cableadas para autenticar, autorizar y justificar su uso de VPN. Esto le brindará al equipo de Castilla-La Mancha mayores controles de seguridad.

## Para obtener más información

Para saber más acerca de los productos de seguridad de Cisco utilizados visite:

- <http://www.cisco.com/go/wsa>
- <http://www.cisco.com/go/esa>
- <http://www.cisco.com/go/asa>
- <http://www.cisco.com/go/ise>
- <http://www.cisco.com/go/trustsec>
- <http://www.cisco.com/go/sma>

### LISTA DE PRODUCTOS

#### Seguridad

- Cisco Web Security Appliance
- Cisco Email Security Appliance
- Cisco ASA 5585-SSP-60 Adaptive Security Appliance
- Cisco Content Security Management Appliance
- Cisco Identity Services Engine
- Cisco TrustSec

#### Centro de datos

- Cisco Unified Computing System™
- Cisco Vblock System
- Cisco 6248 and 6124 Fabric Interconnects

#### Routing y Switching

- Cisco 7204 Routers
- Cisco Nexus 3500 Series Switches
- Cisco Catalyst 6509 Switches



Sede Central en América  
Cisco Systems, Inc.  
San José, CA

Sede Central en Asia y Pacífico  
Cisco Systems (USA) Pte. Ltd.  
Singapore

Sede Central en Europa  
Cisco Systems International BV Amsterdam,  
Países Bajos

Cisco cuenta con más de 200 oficinas en todo el mundo. En la página web de Cisco se indican las direcciones y los números de fax y teléfono: [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

 Cisco y el logotipo de Cisco son marcas comerciales registradas o marcas comerciales de Cisco o sus filiales en EE. UU. y otros países. Para consultar un listado de marcas comerciales de Cisco, visite: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Las marcas registradas de terceros mencionadas son propiedad de sus propietarios respectivos. La utilización de la palabra socio no implica una relación de asociación entre Cisco y cualquier otra sociedad. (1110R)