

# Prevención frente a la pérdida de datos en organizaciones sanitarias en España: Umivale un caso de éxito



## Umivale

### Perfil de Cliente

Entidad colaboradora con la Seguridad Social española. Su misión es optimizar la salud de sus empresas asociadas.

### Industria

Sanidad pública.

### Ámbito Tecnológico (IT)

750 endpoints con Microsoft Windows 10, más 65 server 2008, junto a varios navegadores y aplicaciones comunes, como Adobe software y Office 2010 y 2013.

### Desafíos

- Proteger los datos personales y, en especial, los referentes a la salud.
- Proteger datos en reposo, datos en uso, y datos en movimiento.
- Prevención ante la extracción de datos, cumplimiento legislativo, y, en general, un mejor control de los datos confidenciales.
- Reducir los costes operativos de sistemas o IT. Evitar otros costes asociados por incumplimientos normativos.

### Soluciones de Intel Security

- McAfee VirusScan® Enterprise
- McAfee® Complete Data Protection—Advanced Suite
- McAfee DLP Endpoint
- McAfee Endpoint Threat Protection
- McAfee ePolicy Orchestrator software

El analista en seguridad informática de la mutua colaboradora con la Seguridad Social, Umivale, está convencido de que la información personal y de atención sanitaria de los pacientes está plenamente protegida gracias a McAfee® Complete Data Protection—Advanced Suite, McAfee® ePolicy Orchestrator® (McAfee ePO™) y otras tecnologías finales Intel Security endpoint.

Raul Marín, analista de seguridad y uno de los responsables del servicio de microinformática de la mutua Umivale, cree firmemente que él y su equipo tienen la obligación con las empresas asociadas a Umivale y con los empleados de la mutua de prestar un servicio que ayude a custodiar los datos personales y confidenciales, referidos a la asistencia sanitaria.

Con sede en Valencia, España, Umivale tiene alrededor de 700 empleados y brinda apoyo a más de 55,000 empresas de todos los tamaños y de todos los sectores—desde multinacionales, hasta medianas y pequeñas empresas. Umivale es una entidad colaboradora con la Seguridad Social española (Social Security), y, por lo tanto, Umivale debe de cumplir estrictamente con las obligaciones regulatorias relativas a los datos de atención sanitaria y a la privacidad de los trabajadores.

Desde su cargo en Umivale, Marín está “constantemente atento a las amenazas que pueden colocar a la organización en peligro o que pueden ocasionar una fisura o brecha en la seguridad de los datos. No podemos de ninguna manera permitirnos comprometer la privacidad y el bienestar de los más de 600,000 trabajadores que protegemos. Ante todo, estamos comprometidos con nuestros asociados a mantener la privacidad y la seguridad de sus datos. Nuestros mutualistas saben que contamos con un alto nivel de protección de la información.”

## Regido por las Mejores y Más Rigurosas Prácticas

Marín y su equipo son exhaustivos a la hora de aplicar el nivel más elevado posible de seguridad en todos los dispositivos electrónicos. Umivale concentra su infraestructura en el fabricante Microsoft. Esto incluye 750 endpoints con Windows 10, más 65 server 2008, junto a varios navegadores y aplicaciones comunes, como Adobe software y Office 2010 y 2013.

En Umivale, el despliegue de aplicaciones está centralizado, recayendo tal actividad única y exclusivamente en los servicios de informática; mientras que la actividad de las aplicaciones esta monitorizada. “La infraestructura desplegada no permite operar a los usuarios fuera de los parámetros establecidos. Esto protege tanto a la organización, como al propio usuario, ya que evita posibles responsabilidades ante operativas equivocadas. Toda modificación está sujeta a una estricta gestión del cambio y todo ha sido diseñado con la prevención como prioridad básica.”

Además de la monitorización de las actividades de los sistemas, el servicio de microinformática garantiza que todas las estaciones de trabajo cuenten con las últimas actualizaciones propias del antivirus (.DAT). Además, mediante una adecuada configuración de las reglas de protección de acceso y estandarización global de los puestos de trabajo, han reducido el

*“Las soluciones Intel Security DLP ofrecen una amplia gama de capacidades y cumplen con todos nuestros criterios: prevención ante la extracción de datos incontrolada, cumplimiento legal y mejor control del acceso a los datos confidenciales. El tratamiento de información confidencial mediante dispositivos móviles y otros canales también se ha visto notablemente mejorada con las soluciones de Intel security.”*

—Raul Marin, Analista de Seguridad Principal en Umivale

### Resultados

- Monitorización de los flujos de entrada y salida de información sensible en la organización.
- Incrementar la protección ante los ataques y disponer de datos estadísticos e informes que permitan una mejora continua de los procedimientos de seguridad.
- Utilización mejorada de políticas mediante conjuntos de normas personalizadas y preconfiguradas.
- Análisis del volumen y contextos de la utilización de las terminologías orientadas al tratamiento de la salud.
- Protección de datos más rápida.

riesgo de verse afectados por amenazas de última generación, como ransomware y el CryptoLocker.

### Soluciones Integradas de Seguridad Intel Respaldo las mejores prácticas de seguridad de Umivale

Marín y su equipo han podido cumplir con sus estrictas metodologías a través de la implementación de varias tecnologías de Intel Security durante más de 18 años. “La mejor prueba de la eficacia de las soluciones de Intel Security es que hemos tenido muy pocos incidentes a lo largo de estos años.” Actualmente, las estaciones de trabajo del usuario y de los servidores están protegidas por McAfee VirusScan Enterprise y McAfee Endpoint Threat Protection. La integración con el software McAfee ePO provee de seguridad y de una visibilidad centralizada sobre el comportamiento del usuario y las amenazas potenciales.

“Con la consola de McAfee ePO, podemos detectar y responder rápidamente al malware que pudiera llegar vía archivos y podemos observar cuántas veces un antivirus ha sido activado durante un periodo de tiempo para tener una perspectiva histórica,” afirma Marín. “También valoramos la protección de acceso basada en normas, que, por ejemplo, no permite que un archivo ejecutable resida en la carpeta temporal, ni tampoco la instalación de protectores de pantalla no autorizados por los usuarios. Los productos de Intel Security también nos han protegido de ataques basados en ransomware cifrados. Hemos tenido varias instancias de esto, y hemos podido mitigar todo con éxito.”

Al parecer de Marín, la implementación de los productos de Intel Security ha resultado rentabilizada, ya que ha reducido los costes operativos de sistemas de IT de Umivale, y ha evitado otros costes asociados por incumplimientos. “Hemos podido impedir cientos de ataques con estas soluciones, y esto no hubiese sido posible sin los exhaustivos y detallados informes y estadísticas que permiten generar las herramientas disponibles en el software McAfee ePO.”

### La prevención ante la pérdida de datos que proporciona McAfee Data Loss

#### Prevention incrementa la seguridad de los datos de salud

Con el tiempo, el equipo de microinformática ha protegido la infraestructura de la mutua a través de antivirus, antispysware, firewall, zonas militarizadas (DMZ), análisis de tráfico de red, protección de acceso y cifrado para el correo electrónico. No obstante, mantener el control sobre los datos confidenciales ha sido siempre un gran desafío para la organización, que maneja cientos de miles de registros sobre la atención sanitaria de pacientes todos los días.

Como dice Marín, “A medida que los usuarios crean documentos y los comparten, siempre existe un porcentaje de datos sobre los que no se tiene control. El correo web, el uso de smartphones y otras tendencias de tecnologías populares, han abierto nuevos vectores de amenaza. Es imposible restringir el flujo de datos porque la creación y el intercambio de los mismos es clave para los servicios que ofrecemos, y es por esto que decidimos investigar las soluciones de prevención de pérdida de datos de Intel Security.”

Marín evaluó las soluciones de prevención de pérdida de datos (DLP) de varios proveedores. Descubrió que la mayoría de estos tienen una consola de gestión para sus productos de antivirus, pero no para DLP. Además, observó que los conjuntos de políticas no incluían las de aplicaciones. “Las soluciones Intel Security DLP ofrecen una amplia gama de capacidades y cumplen con todos nuestros criterios: prevención ante la extracción de datos, cumplimiento legislativo y en general un mejor control de los datos confidenciales. El tratamiento de información privada mediante dispositivos móviles y otros canales también se ha visto notablemente mejorada con las soluciones de Intel Security,” afirma Marín.

Después de esta exhaustiva comparativa, se decidió implementar en Umivale McAfee Complete Data Protection—Advanced Suite y McAfee DLP Endpoint. Ahora, desde microinformática están seguros de que todos los endpoints están debidamente protegidos. También tienen la capacidad de identificar y clasificar rápidamente los datos confidenciales basándose en la ubicación del documento, el autor, el contenido y otras características.

Otro beneficio es que se consigue monitorizar los flujos de entrada y salida de información sensible de la organización. El resultado de estas actividades es lograr un conocimiento que con posterioridad se aplicará a las políticas de seguridad, ajustando al máximo su eficacia. La integración con el software McAfee ePO simplifica la gestión de DLP y provee a los equipos de gestión de una visión unificada de todo el ámbito de Umivale y una visión general de la seguridad.

“Con los productos de Intel Security DLP podemos determinar normas para lograr un tratamiento adecuado de la información no estructurada. Ha sido fantástico poder asegurar que los correos con información referente a la salud han sido encriptados en todos los casos,” afirma Marín.

### Construcción sobre una **Sólida Base de Protección de Datos**

Después de un periodo de tiempo trabajando con las soluciones de Intel Security DLP, Marín y su equipo desarrollaron sus propias herramientas que se integraron en el software McAfee ePO y prolongan sus capacidades para identificar información confidencial, incluso de una mejor manera.

El proceso comienza agregando terminología propia referente a salud. Estos contenidos se encuentran en el 80% de los documentos que fluyen en la operativa diaria de Umivale, y se han incorporado a la gestión a través de diccionarios nativos de las herramientas de Intel Security. Gracias a ello, el equipo de microinformática puede usar la consola de McAfee ePO para cuantificar las veces que aparece una palabra o frase relacionada con las terminologías de salud en los archivos tratados.

También pueden analizar con suma facilidad los contextos en los que se han utilizado dichos términos, con el objeto de separar aquellos que no tienen un significado propiamente sanitario (falsos positivos); y por último, estas herramientas propiedad de Umivale facilitan la identificación de acciones anteriores y posteriores realizadas sobre dichos archivos. Esto solamente es posible gracias a las capacidades de integración de la arquitectura abierta y conectada de Intel Security.

“En conjunto, los productos de Intel Security y, en especial DLP solutions nos brindaron ventajas distintivas en muchas áreas. En un nivel organizacional, estas tecnologías nos ayudaron a tomar mejores decisiones y a mejorar nuestros procesos”, sostiene Marín. “Lo más importante es que contamos con una mejor comprensión de lo que sucede en la organización, podemos responder más rápidamente si ocurren incidentes y podemos pulir nuestras políticas con mayor precisión.”

