FLYTECH®

CASO DE ÉXITO

# MUSSAP consigue con Assureon un control total de los ficheros y una seguridad extrema de toda la información.

FLYTECH®

CASO DE ÉXITO

## ¿QUÉ ES MUSSAP?

**Aunque actualmente Mussap es una de las principales aseguradoras de la zona de Cataluña, esta compañía comenzó su andadura en 1932, como una modesta mutua de seguros contra accidentes del trabajo agrícola. A mediados de los años sesenta comenzó a ampliar su campo de actividad más allá del sector agropecuario. Hoy en día dispone de seguros personales ante casos de accidentes o de enfermedad, de vida y jubilación, seguros multiriesgo que protegen hogares y negocios y seguros de automóviles, área que representa los mayores ingresos de la firma, en concreto el 69% de las primas provino de su actividad en este campo.**

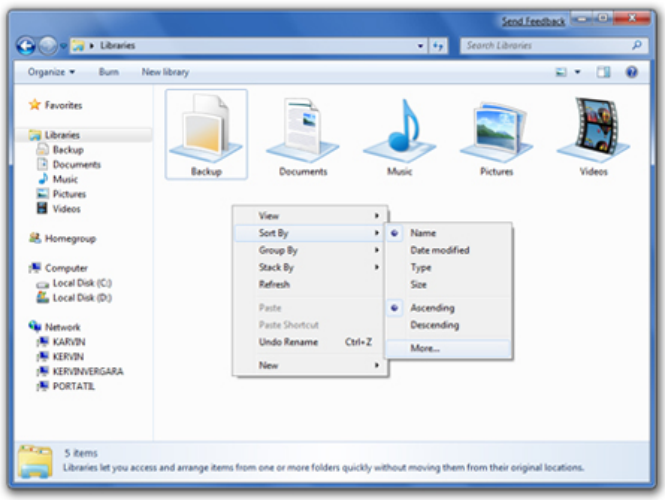
**Mussap ha extendido también su ámbito de acción a las comunidades limítrofes con Cataluña y ya cuenta con sucursales en Valencia, Aragón y Baleares. Ahora sus miras están puestas en seguir expandiéndose por el resto de la península. Para lograr este ambicioso crecimiento con garantías de éxito Mussap ha encontrado un buen aliado en la tecnología.**

## LAS NECESIDADES DE MUSSAP

Mussap, como otras grandes empresas, dispone de muchos departamentos que generan cientos de ficheros diarios nuevos o modificados.

Esta gran cantidad de ficheros necesitaban un control especial, es decir que cada dato guardado en el sistema no fuera como un libro sin clasificar en una gran biblioteca.

Además, toma una vital importancia el control de versiones de Assureon que guarda un mismo fichero tantas veces como ha sido modificado. La encriptación, compresión y chequeo constante de la integridad del fichero también son puntos muy importantes para Mussap.

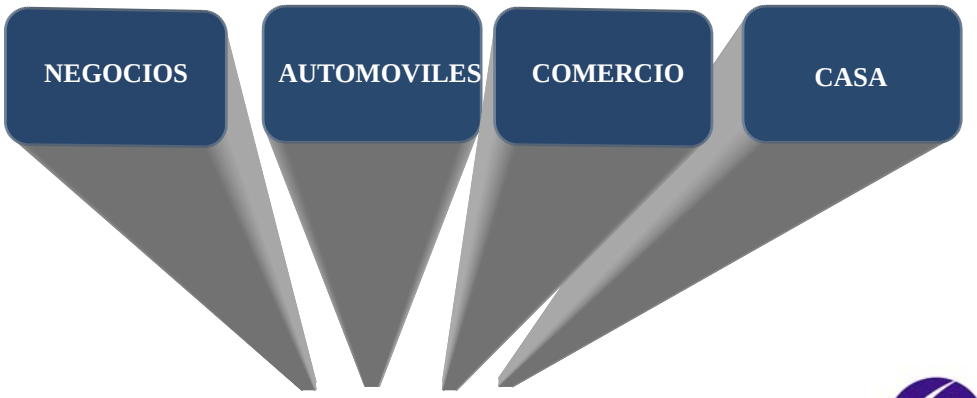



Algo indispensable para Mussap es que el sistema se integrara perfectamente en el actual entorno SAN y en el futuro entorno virtualizado, lo cual cumple perfectamente Assureon.

FLYTECH®

## CASO DE ÉXITO

Con la tecnología ILM de Assureon se ha conseguido que los datos de poco uso no ocupen espacio en el almacenamiento primario, que éste dé un alto rendimiento y al mismo tiempo, se copien automáticamente en Assureon. Estos datos son imposibles de borrar hasta que no se superen los días, meses o años especificados por el administrador, con lo cual se cumplen las leyes que marcan la vida de cierto tipo de datos. Además también se han encriptado datos privados críticos con la tecnología más avanzada. Los usuarios de esta mutua de seguros pueden recuperar datos que hayan borrado accidentalmente o se hayan perdido, incluso sin la intervención del administrador. Este proceso se hace mediante una interfaz web de manera rápida y sencilla.




nexsan TECHNOLOGIES

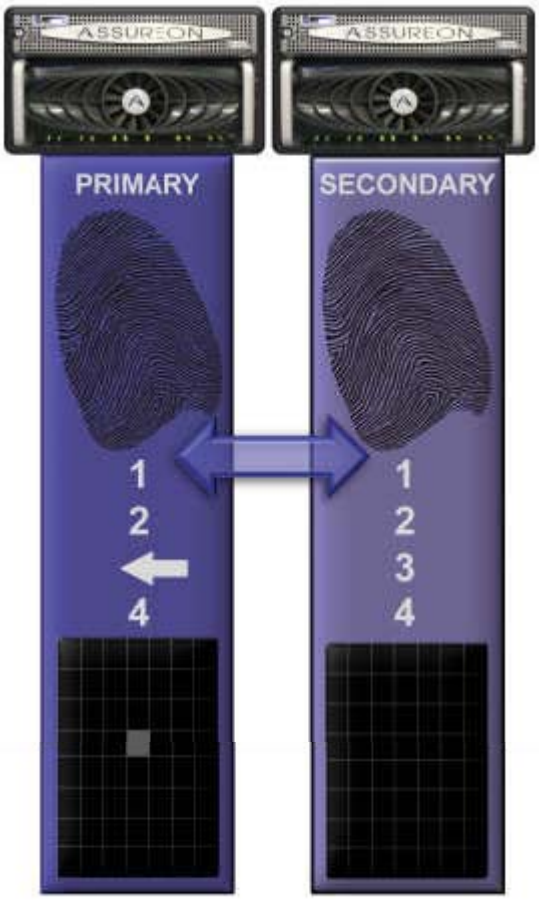
# Assureon™

## Secure Online Disk Archive

# CÓMO FUNCIONA ASSUREON Y DE QUÉ FORMA HA AYUDADO A MUSSAP

Nexsan Assureon es una solución completa que combina una codificación avanzada con almacenamiento dirigido de los contenidos, la tecnología de ILM y otras características de la seguridad en un solo sistema completamente integrado basado en disco.

Cada fichero almacenado en Assureon, tiene un número de serie único y consecutivo. Un listado de esos números de serie, el número de serie asociado a las claves de encriptación y la huella digital electrónica de cada fichero, es construido cada 5 minutos dentro de un fichero denominado archivo de referencia (relación detallada de diferentes partes que componen cada fichero). Este archivo de referencia es enviado al sistema remoto, para poder actuar como evidencia y backup, permitiendo la comprobación de integridad entre ambos sistemas, garantizando la inmutabilidad del archivo original (el archivo de referencia remoto se comprueba con el de origen en el clúster de Assureon). A este proceso se denomina deposito activo del archivo de referencia.




Además según es enviado el archivo de referencia al segundo sistema por salvaguarda y seguridad, cada archivo de referencia es almacenado previamente en el clúster y así la huella digital electrónica del archivo de referencia realiza la primera entrada y habilita las siguientes.

**Assureon asegura la protección de los datos, la confidencialidad, la seguridad, y la gestión de retención.**

De este modo, cada archivo de referencia se encadena consecutivamente de una forma criptográfica (un archivo de referencia modificado o suprimido o la modificación física externa de un archivo de referencia causarían una cadena rota que fácilmente es descubierta). A nivel de administración se define a intervalos, una revisión de cuentas de integridad de datos de una forma comprensiva para controlar toda la información almacenada. Cada número de serie de cada fichero es comprobado de una forma cíclica a la vez que su huella digital electrónica, antes y después de su desencriptación, siendo comparados sus valores durante la creación del fichero original. Cualquier discrepancia o pérdida del fichero es almacenado en logs y automáticamente es reparado desde la copia redundada (en local o remoto). La cadena criptográfica del archivo de referencia es verificada al mismo tiempo para comprobar su total integridad (copia exacta).

Assureon está diseñado con múltiples capas de protección contra modificaciones accidentales o maliciosas de los ficheros almacenados, también dispone de una serie de medidas superpuestas diseñadas para descubrir cualquier modificación impropia de registros. Además ante cualquier discrepancia Assureon repara cualquier fichero corrupto o perdido, inicialmente usando la copia redundada local del mismo fichero o secundariamente del sistema remoto replicado. Todas estas medidas disponen adicionalmente de protección física del dato con técnicas ECC, múltiples caminos de acceso a datos y técnicas RAID hardware.

La integridad arranca en el momento que el primer fichero salvado en el servidor/estación local es movido por el FSW. FSW es un agente que se instala en los servidores y que permite la comunicación con Assureon. Cuando el FSW accede al fichero nuevo o modificado en cualquiera de las carpetas gestionadas por Assureon, lo primero que realiza es calcular una huella digital electrónica criptográfica del fichero, siendo parte de esta, un hash MD5 de 128 bits concatenado con otro hash SHA-1 de 160 bits. Esta dualidad de hash, permiten la no falsificación de la huella digital electrónica criptográfica del fichero, reduciendo la posibilidad de colisiones de hash. Otros sistemas ILM sólo usan MD5.

FSW envía la huella digital electrónica criptográfica del fichero al clúster Assureon, el cual responde con un único número de serie emitido para el nuevo archivo.

FSW usa reglas de retención asociadas a carpetas, asignando retenciones mínimas y nominales (los valores del FSW, como por ejemplo las reglas de retención son configurados por una consola especial del administrador del clúster Assureon, de una forma centralizada). El fichero, el metadato, la retención, la huella digital electrónica y el número de serie son transmitidos al clúster de Assureon. Si es necesario, FSW repite esta transferencia a múltiples nodos de Assureon hasta que los clúster responden que todo ha sido recibido correctamente. Una vez recibida la confirmación, FSW puede convertir la copia del fichero local como acceso directo transparente (apuntando al original copiado en el clúster Assureon), dejarla como esta o borrarla.

**Mussap ejecuta cada 2 horas múltiples tareas de sincronización con FSW de toda la información, aunque podría hacerlo cada 5 minutos si lo deseara.**

Una vez el fichero es recibido por uno de los nodos frontales del clúster Assureon, este envía la información del metadato del fichero para securizarlo con el servicio de marca de tiempo que trabaja dentro del clúster Assureon de una forma cíclica, valida su propia información de horario con fuentes de tiempo seguras externas. La grabación de la marca de tiempo en el metadato es firmada digitalmente y enviada junto al contenido del fichero a una de las instancias del servicio de gestión del almacenamiento que trabaja en los nodos traseros. El servicio de gestión del almacenamiento es el responsable de garantizar que el fichero esta encriptado (si así se desea), replicado en los servicios de almacenamientos locales y remotos, controlando la redundancia de copias, y convirtiéndolo dentro como un objeto CAS (Content Addressed Storage). CAS habilita inmutabilidad; si cualquier parte del contenido del fichero, cambia, es reportado y reparado. Gracias a CAS, el sistema dispone de una indexación total de los ficheros (objetos), a nivel de metadato y contenido. Con esta característica, se pueden realizar de una forma sencilla búsqueda de información en todo el sistema (Assureon Search).

El servicio de gestión del almacenamiento es el único proceso que tiene autorización para borrar datos, y solo se ejecutara el borrado cuando el periodo de retención ha expirado y el administrador lo confirma. Ambas condiciones concurrentes son necesarias para borrar cualquier fichero del sistema. El usuario podría borrar cualquier fichero con derechos para ello, pero el sistema siempre mantendría el fichero hasta que las dos condiciones anteriores se cumplan. Un driver a nivel de Kernel evita cualquier proceso no autorizado de escritura directa en el repositorio de ficheros, mediante el enlace criptográfico único hacia el gestor del almacenamiento. Dicho gestor de almacenamiento, restringe la lectura de ficheros por usuarios no autorizados. Finalmente, el Gestor del Almacenamiento es el responsable de garantizar que el fichero es escrito como mínimo en dos RAID-6 diferentes. Cada sistema hardware RAID de una forma individual tiene un bloqueo para evitar cualquier situación de parada en producción a la vez que no permite cambios que puedan ser destructivos, como por ejemplo cambios en FC ACL, borrado de RAID sets.

Por razones de seguridad, los Gestores de Almacenamiento residen en los nodos traseros del clúster, aislados del contacto directo de la red de usuarios. Estos nodos son appliances dedicados cuya función exclusiva es la ejecución de la política de retención y seguridad. Software ajeno, como aplicaciones de clientes, no se pueden instalar en dichos appliances.

Todos los puertos de red están bajo cortafuegos, con una política extremadamente restrictiva a nivel de puertos y cualquier servicio es borrado o desactivado, para prevenir los posibles puntos de ataques deliberados, tanto internos como externos. El Gestor del Almacenamiento sólo responderá a un número muy pequeño de protocolos propietarios, y a ninguna orden existente de operaciones destructivas como " borrado". Dichos gestores de almacenamiento toman sus propias decisiones en cuanto a si un archivo es un candidato de borrado, y posteriormente presenta la lista al Administrador del sistema, el cual toma la última decisión: borra o mantiene. Cada nuevo fichero introducido en el clúster Assureon, su número de serie, marca de tiempo y huella digital electrónica es añadida al archivo de referencia. Cada 5 minutos, este archivo de referencia es cerrado y almacenado como nuevo fichero. Cuando entra un nuevo fichero, un nuevo archivo de referencia se crea hasta 5 minutos después. Este proceso en cadena de archivos de referencia es extremadamente sensitivo a cualquier inserción, alteración o borrado de ficheros de forma no autorizada. No existen mecanismos actualmente para que los usuarios o administradores rompan esta cadena. Como medida adicional de integridad, este archivo de referencia es transmitido a un servidor de llaves localizado en USA, el cual controla Nexsan, y puede compararse dicho archivo de referencia local con el remoto y viceversa. El servidor de llaves mantiene un servidor de referencia de tiempo Stratum-1. Gracias a esto, se puede evitar el falsificado de la hora del fichero. Por razones de seguridad y privacidad, solo se envía la huella digital electrónica criptográfica y no los propios ficheros originales al servidor de llaves.

Como una función de protección, los procesos de servidor de auditoría, corre en los nodos traseros del clúster Assureon y verifican los números de serie de los archivos secuenciales, cargan una copia del archivo almacenado, calculan de nuevo su huella digital electrónica, y comparan esto con la huella digital electrónica almacenada en el registro de metadato firmado.

El servidor de auditoría también compara las copias no registradas del metadato almacenado en una base de datos SQL con los metadatos firmados oficialmente para confirmar la cadena de los archivos de referencia. Otro chequeo confidencial de integridad, es ejecutado para detectar cualquier tipo de software no autorizado o modificación del que está en ejecución. Si cualquier fichero no se encuentra o esta corrupto, automáticamente el servidor de auditoría lo reemplaza por una de las copias buenas localizadas en local o remoto. Genera Logs completos de las auditorias, los cuales son almacenados permanentemente dentro del Assureon. Cualquier problema es registrado y genera alertas por email al administrador y al servicio de mantenimiento de Nexsan. El servidor de auditoría es tan potente, que puede ser usado en actualizaciones (puede realizar los trabajos de migración, cuando se retira una cabina de almacenamiento RAID por otra de mayor capacidad).

## BENEFICIOS

**Coste-efectivo Escalabilidad**: Assureon tiene un poder de procesamiento que se puede ampliar con independencia de su capacidad de almacenamiento. Esta potencia de procesamiento se ha diseñado en Assureon.

**De alto rendimiento**: la capacidad de almacenamiento en disco de Assureon ofrece el rendimiento requerido. Debido a su red Assureon es totalmente automatizado y basados en disco, por lo tanto la eliminación de engorrosos y caro aspectos de la manipulación, el almacenamiento y la restauración se harán de forma automática.

**Garantizar el cumplimiento**: Assureon utiliza la más altos niveles de cifrado y seguridad de acceso a asegurar la privacidad de los historiales. Assureon posee aseguramiento de la integridad y capacidad. Continuamente realiza dos auditorías en todos los archivados, por lo que garantiza que cada archivo existe en todos los Assureon local o remoto y reproduce cada archivo para verificar la integridad y autenticidad por garantizar todos los bits que coinciden con el contenido de su huella digital. Si Assureon detecta un problema, automáticamente reemplaza el archivo dañado con otro Assureon replicado - ya sea localmente o desde un negocio.

### CONCLUSIÓN

*"Gracias a Assureon, MUSSAP ha conseguido un control total de los ficheros y una seguridad extrema de toda la información."*