ZONEPOINT

FOR MS SHAREPOINT™ LIBRARIES

CONFIDENCIALIDAD Y SEGMENTACIÓN EN MS SHAREPOINT™

ZONEPOINT garantiza la confidencialidad de los documentos colocados en las bibliotecas de MS SharePoint™. El cifrado proporciona esta protección en el origen, en el terminal del usuario. Aplica el derecho a saber segmentando el acceso a los documentos de forma transparente para el usuario. La información sensible publicada o compartida solo será accesible para quienes poseen ese derecho, quedando protegida contra el robo, el espionaje y la divulgación.

Protección de los intercambios internos de documentos

Los empleados colocan, publican y comparten numerosos documentos todos los días en sitios internos como MS SharePoint™, muchas veces sin un verdadero control sobre quienes tendrán acceso a ellos. Aplicando automáticamente la política de cifrado en función de las carpetas, **ZONEPOINT** permite garantizar de forma transparente la segmentación criptográfica entre carpetas y entre grupos de trabajo, asegurando así la confidencialidad de los datos publicados en cada equipo. Esta gestión del derecho a saber puede sincronizarse con los derechos de MS SharePoint™ o Active Directory.

Protección de publicaciones y recursos compartidos entre socios

Las colaboraciones entre empresas (publicaciones científicas, planes para subcontratistas, data rooms financieras, etc.) requieren una plataforma de TI que normalmente controla el jefe de archivo con un nivel de servicio suficiente que generalmente permite gestionar grandes volúmenes a largo plazo. Las soluciones populares de almacenamiento en Internet apenas pueden responder a estas necesidades.

MS SharePoint™ es una solución elegida con frecuencia, pero en este caso de uso, su apertura a Internet y a terceros asociados aumenta el riesgo de acceso incontrolado a los datos. Aplicando una capa de cifrado, **ZONEPOINT** permite garantizar la confidencialidad de los datos, siendo imprescindible debido a la accesibilidad de las bibliotecas a través de Internet.

Confidencialidad entre el operador de TI y el proveedor de hosting

El servidor MS SharePoint™ no forma parte de la zona de confianza: los documentos almacenados se cifran permanentemente. En ningún momento se pasan los datos sin cifrar a los servidores. Los documentos se cifran/descifran localmente en las estaciones de trabajo con la clave del usuario.

Con **ZONEPOINT**, es posible usar un servidor de MS SharePoint™ externo sin riesgo de pérdida de confidencialidad.

Los datos permanecerán cifrados en todo momento en los servidores y durante su transporte. Esto garantiza su confidencialidad entre operadores. La empresa puede elegir la ubicación de sus servidores: internos o externalizados a un tercero.

Gobernanza de cifrado por parte de la empresa

Cualquier documento colocado en una biblioteca se cifra automáticamente de conformidad con la política de seguridad definida por el «propietario» (en el sentido de MS SharePoint™).

ZONEPOINT permite a los responsables de aplicaciones profesionales o de seguridad, controlar, desde sus estaciones de trabajo, la implementación de la estrategia de cifrado.
Pueden delegar todo o parte de estas operaciones a determinados usuarios autorizados.

CERTIFICACIONES

CIFRADO

- Cifrado de las bibliotecas de Microsoft SharePoint™.
- Acceso a los documentos cifrados por el navegador o por el explorador de archivos (webDAV).
- Cifrado transparente para el usuario.
- Cifrado de datos internos o compartidos con el exterior.

AUTENTICACIÓN

- Autenticación mediante certificado (PKI) y/o contraseña.
- Compatible con las tarjetas y tokens de los principales fabricantes (estaciones de trabajo).
- Compatible con Microsoft CSP/CNG.

ADMINISTRACIÓN - TI

- Solución estándar de MS SharePoint™ desplegable en el servidor.
- Agente de software en la estación de trabajo para todas las operaciones criptográficas.
- Despliegue a través de las infraestructuras de TI habituales (SCCM, AD, etc.).
- Sin cambios y sin alteraciones en la gestión de recursos de TI.

ADMINISTRACIÓN - SEGURIDAD

- Políticas de seguridad definidas por los responsables de seguridad.
- Plan de cifrado administrado.
- Supervisión de la aplicación de las políticas de seguridad.
- Mecanismo de recuperación de datos configurable.
- Emergencia de usuarios (pérdida de clave o contraseña).

CARACTERÍSTICAS TÉCNICAS

- Compatible con los servidores **MS SharePoint™ 2019, 2016 y 2013**.
- Navegadores compatibles: **Chrome, Firefox, Edge.**
- Cifrado **AES 256**.
- Acceso mediante **certificados/claves RSA** (hasta 4096 bits) y/o contraseña (con fuerza configurable).
- Compatible las principales **smart card** PKCS#11 (formato tarjeta o USB).
- Compatible con la mayoría de las **PKI** del mercado.
- Aplicación móvil: **ZONEMOBILE** para **iOS** y **Android**

PRIMX
MAKE ENCRYPTION HAPPEN

business@primx.eu – Tel.: 01 77 72 64 80
Officina central: 18 Rue du Général Mouton-Duvernet, 69003 Lyon / Dirección comercial: 21 Rue Camille Desmoulins, 92130 Issy-les-Moulineaux
www.primx.eu