ORIZON

FOR CLOUD STORAGES

CONFIDENCIALIDAD DE LOS DOCUMENTOS EN EL CLOUD

ORIZON garantiza la confidencialidad de los archivos colocados en el Cloud. El cifrado proporciona esta protección en el origen, en el terminal del usuario. Permite el derecho a saber: los datos están protegidos contra accesos no deseados del proveedor de Cloud, de los empleados o de personas externas.

Soberanía de la empresa sobre sus datos

Los servicios de sincronización de archivos en el **Cloud** o en un sistema interno de tipo ***EFSS***, para el almacenamiento, el intercambio y para realizar copias de seguridad, exponen los datos al robo, la divulgación y el espionaje durante su transporte y almacenamiento. La empresa deja de tener un control total sobre quién puede acceder a sus datos y no es consciente de la porosidad ni del nivel de exposición a los riesgos (interferencia, piratería informática y violaciones de la seguridad, personal del proveedor del Cloud, etc.). El derecho a saber que garantiza el cifrado proporciona una respuesta fuerte y matemática que asegura que la información solo la puedan conocer las personas autorizadas, conservando al mismo tiempo la flexibilidad y la elasticidad del Cloud.

Datos sincronizados protegidos

ORIZON protege automáticamente los documentos almacenados por los usuarios en el Cloud. De hecho, los archivos se cifran en cuanto se crean, y en tiempo real, en la ubicación de origen. Permanecen codificados durante la sincronización y durante el almacenamiento en el proveedor de hosting (incluso durante el transporte). Solo el o los usuarios autorizados podrán descifrarlos (con las claves apropiadas) en el terminal que elijan. Así, solo estos últimos *entenderán* el contenido de esos documentos.

Intercambios de documentos confidenciales

ORIZON cifra automáticamente todos los documentos sincronizados. Si se realiza un intercambio, como consecuencia, se aplicarán automáticamente los derechos criptográficos, única y específicamente para quienes poseen el derecho. El derecho a saber también se garantiza en los recursos compartidos en el Cloud, y **ORIZON** garantiza la segmentación de esta información entre usuarios, servicios y proveedores, pero especialmente con el proveedor de servicios de Cloud. Además, incluso los socios externos pueden trabajar con los documentos cifrados que se comparten con ellos mediante la versión gratuita y multiplataforma de **ORIZON**.

No afecta la experiencia del usuario

Con un diseño deliberadamente transparente, **ORIZON** conserva la discreción y no supone ningún cambio para los usuarios en sus rutinas laborales. Se mantiene la colaboración y la ubicuidad del acceso a los datos (en la oficina, en casa, desde un teléfono o una tableta). Puede cifrarse cualquier tipo de archivo sin ninguna interacción con el usuario.

Gobernanza de seguridad

ORIZON aplica la política de cifrado definida por la empresa: recursos compartidos o no, sincronización de todas las carpetas o solo una carpeta «caja-fuerte». Pueden aplicarse diversos tipos de claves de acceso (Smart-Cards, certificados, contraseñas, etc.), así como accesos de recuperación.

Solución ligera y no estructurante

ORIZON no implica ningún cambio. Solo está presente en las estaciones de trabajo o terminales móviles, se despliegue a través de las infraestructuras de TI habituales, disponibles en las tiendas de aplicaciones.

CONECTORES

OneDrive

Dropbox

CIFRADO

- Cifrado por zonas de carpetas sincronizadas.
- Cifrado sobre la marcha y transparente para los usuarios.
- Cifrado de los datos compartidos de forma interna o externa.

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

- Agente de software en cada estación de trabajo, sin componentes en el servidor.
- Despliegue a través de las infraestructuras de TI habituales (SCCM, AD, etc.), disponibles en las tiendas de aplicaciones.
- 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 la mayoría de soluciones EFSS del mercado (OneDrive™, Google Drive, Box, Dropbox™, etc.).
- **Windows** 7 a 10+.
- Cifrado **AES 256**.
- Acceso mediante **certificados/claves RSA** (hasta 4096 bits) y/o contraseña (con fuerza configurable).
- Compatible con las principales **smart card** PKCS#11 (formato tarjeta o USB).
- Compatible con la mayoría de las **PKI** del mercado.

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