CASO DE USO

ZONECENTRAL

CONTROLAR EL ACCESO A LA INFORMACIÓN

Caso de la entidad Inversiones de un banco de negocios, en plena expansión internacional.

REQUISITOS

Todos los datos de la estructura se centralizan en **un mismo servidor de archivos**, que se replica para gestionar eficazmente los recursos. **Cada usuario dispone de una carpeta en el servidor de archivos** en la que trabaja y realiza las copias de seguridad de sus datos a diario. **Cada servicio dispone también de una carpeta reservada**, que hasta ahora solo podía segmentarse con los derechos de Microsoft.

Garantizar que los datos de este banco - actualmente accesibles al equipo de TI - sean **únicamente inteligibles para las personas autorizadas**, es indispensable. La solución, por tanto, **no debe interferir con las tareas del equipo de TI**.

SOLUCIÓN

La solución **ZONECENTRAL** fue elegida para este proyecto, pues permite cifrar:

+ Todas las unidades de red Y: que conducen a las carpetas personales de los usuarios en el servidor
+ Las carpetas «Escritorio», «Mis Documentos» y TEMP de los usuarios.
+ Las distintas carpetas de cada servicio en el servidor de archivos.

EXPERIENCIA

ORGANIZACIÓN

Con el fin de garantizar el éxito de esta mejora en la seguridad, la estructura ha establecido una organización interna destinada a separar completamente los roles de la Dirección de los Sistemas de Información (DSI) de los del equipo de Seguridad de los Sistemas de Información (SSI). Se han establecido numerosos procedimientos entre los equipos de DSI y SSI con el fin de garantizar que ninguno de ellos tenga el pleno control sobre los datos cifrados.

De esta forma, son dos los equipos en cuestión:

+ El equipo 1, dependiente de la DSI, asigna y retira los derechos de modificación y lectura al otro equipo, antes y después de sus intervenciones.
+ El equipo 2, del SSI, determina las zonas a cifrar o a dejar sin cifrar, disponiendo también del derecho a añadir o retirar accesos criptográficos en las zonas cifradas.

SERVICIO DE TI

El servicio de TI garantiza el despliegue del producto y las políticas de seguridad a través de la GPO. Además, garantiza la gestión de los archivos (copia de seguridad y restauración) así como la gestión de los derechos de Microsoft de los usuarios y los miembros del servicio de SSI.

SERVICIO DE SSI

Cuando es necesario realizar una modificación en la gestión del cifrado de **ZONECENTRAL** (añadir/eliminar accesos, crear zonas sin cifrar, etc.) es obligatorio enviar una solicitud por correo electrónico al servicio de SSI Tras este intercambio, el equipo de SSI solicita al de TI que le conceda los derechos de modificación en el lugar deseado, para realizar la intervención.

USUARIOS

Los usuarios solo tienen que introducir el código PIN de su SmartCard al abrir la sesión.

+ VENTAJAS

El cifrado que se aplica con **ZoneCentral es transparente para los usuarios:** no afecta a sus rutinas de trabajo diarias. Además, la solución permite realizar **una segmentación técnica total de los roles** de cada equipo, permitiendo así la protección de los datos sensibles, tanto de forma interna como externa. Finalmente, las políticas de seguridad aplicadas son complementarias a los derechos NTFS de Microsoft.

2023.06

PRIMX
MAKE ENCRYPTION HAPPEN

business@primx.eu - T.: +33 (0)1 40 95 24 84
Officina central: 18 Rue du Général Mouton-Duvernet, 69003 Lyon / Dirección comercial : 21 Rue Camille Desmoulins, 92130 Issy-les-Moulineaux
www.primx.eu