



Estimados,

Nuestra empresa **Sitepro S.A.** tiene más de 25 años de trayectoria en el desarrollo de *Sistemas de Protección de Software y Seguridad Informática*. **En Argentina**, la mayoría de las empresas desarrolladoras que protegen su software utilizan nuestras llaves electrónicas, entre las cuales podemos mencionar a empresas líderes como *Buenos Aires Software, Sistemas Béjerman, Calipso, Waldbott y Asociados*, entre muchas otras.

Contamos con distribuidores en casi toda **Latino América** y en **España**, e importantes cuentas como: *Overtech* en Chile, *Facture* en Colombia, *Edydsi* en Paraguay, *Real Systems y SisCont* en Perú, *Pérez Abreu* en Rep. Dominicana, *Memory* en Uruguay, *Galac* en Venezuela. Varios de nuestros clientes exportan su software a todo el mundo protegiéndolo con nuestras llaves HARDkey®.

**HARDkey®** permite proteger Software controlando efectivamente las licencias que se comercializan (1 HARDkey = 1 Licencia) y potencia la venta por canales y exportación de software. También con HARDkey® se pueden controlar el Leasing ó ventas en cuotas, e implementar comercialización por medio de esquemas de SaaS (Soft as Service).

Nuestras llaves electrónicas HARDkey® tienen 4 Kbytes de memoria disponible para el desarrollador que se pueden utilizar para mejorar los niveles de protección almacenando en ella claves de bases de datos, fórmulas, *código ausente* o incluso un Certificado Digital (o por lo menos sus claves) permitiendo dar seguridad a esquemas de firma digital ó electrónica de documentos y transacciones. En sólo un par de días de trabajo podrán tener nuestras llaves HARDkey integradas a sus desarrollos.

Incorporar las llaves HARDkey® a sus sistemas para validación de accesos de usuarios por dos factores, les permitirá cumplir con la **Norma ISO 17799 / 27001** y la **Norma Circular 52 de la Superintendencia de Entidades Financieras** de Colombia, entre otras normas internacionales de seguridad.

La autenticación por dos factores se realiza mediante “**algo que tengo**” (la llave HARDkey®) y “**algo que conozco**” (una clave personal PIN). Se puede incorporar las HARDkey® en una primera etapa reemplazando en sus sistemas el USUARIO y la PASSWORD de los administradores, de tal

forma que toda operación de configuración sensible que pueda comprometer la integridad de los datos sea realizada sólo por la persona autorizada con su llave HARDkey® de habilitación e ingresando su PIN. Por medio de esta llave se podrá habilitar la configuración de los distintos perfiles de usuarios, indicando en forma opcional para qué usuarios y operaciones críticas se solicitará una llave HARDkey® de habilitación.

Para implementar esto bastará con agregar en la tabla que se define el perfil de los usuarios un campo que contenga el **ID** de la HARDkey® que se asigne a cada usuario que deberán utilizarla para operar los sistemas. Esto sería aplicable a perfiles de directivos, gerentes y supervisores que tengan acceso a parámetros y operaciones críticas. De esta forma sus sistemas se comercializarían con el esquema actual que tienen de protección, agregando un nivel de seguridad adicional con una llave HARDkey® para los administradores, y opcionalmente otras llaves para usuarios críticos. Esto constituye indirectamente **un método adicional de protección de software**.



### A) Esquema de una llave compartida por intranet

En una implementación de este tipo se conecta una llave compartida en un servidor local para lograr que solamente los usuarios de esa intranet estén habilitados a usar las aplicaciones.

En un esquema como este se logra que usuarios ajenos a la organización no tengan acceso a las aplicaciones desde afuera del entorno de la intranet de la empresa.



### B) Esquema de una llave por usuario

También es posible autorizar en forma selectiva el acceso a las aplicaciones entregando una llave personalizada por usuario.

En esquemas como este, cada persona dispone de su llave de autenticación y un PIN de acceso para garantizar la seguridad en caso de robo o extravío del dispositivo.

También se pueden **leer datos** de la base de datos, PC o Servidor donde se instalan sus aplicaciones guardando **una huella** ó **HASH** en la memoria de las llaves HARDkey® evitando que se puedan utilizar llaves de una instalación en otra.

Adicionalmente podrán utilizarse las llaves HARDkey® para que los administrativos, comerciales y técnicos de vuestra empresa sean Autenticados por dos Factores (llave y PIN) en sus sistemas internos y utilitarios de mantenimiento, reemplazando el endeble esquema de usuario y password. Esto puede implementarse especialmente para mantener bajo control los utilitarios de mantenimiento y evitar que los técnicos que se retiran de la empresa puedan seguir utilizándolos al tenerlos anclados a las llaves HARDkey®, incluso pudiendo grabar en su memoria las password de acceso a las bases de datos de sus sistemas para que este dato no pueda ser utilizado para acceder en forma externa, pudiendo comprometer la integridad de los datos y sistemas.



Cátulo Castillo 2630 Piso 2  
(1261) Cdad. de Buenos Aires  
República Argentina

 [www.sitepro.com.ar](http://www.sitepro.com.ar)

 [info@sitepro.com.ar](mailto:info@sitepro.com.ar)

 (+54) 11 3220-0600