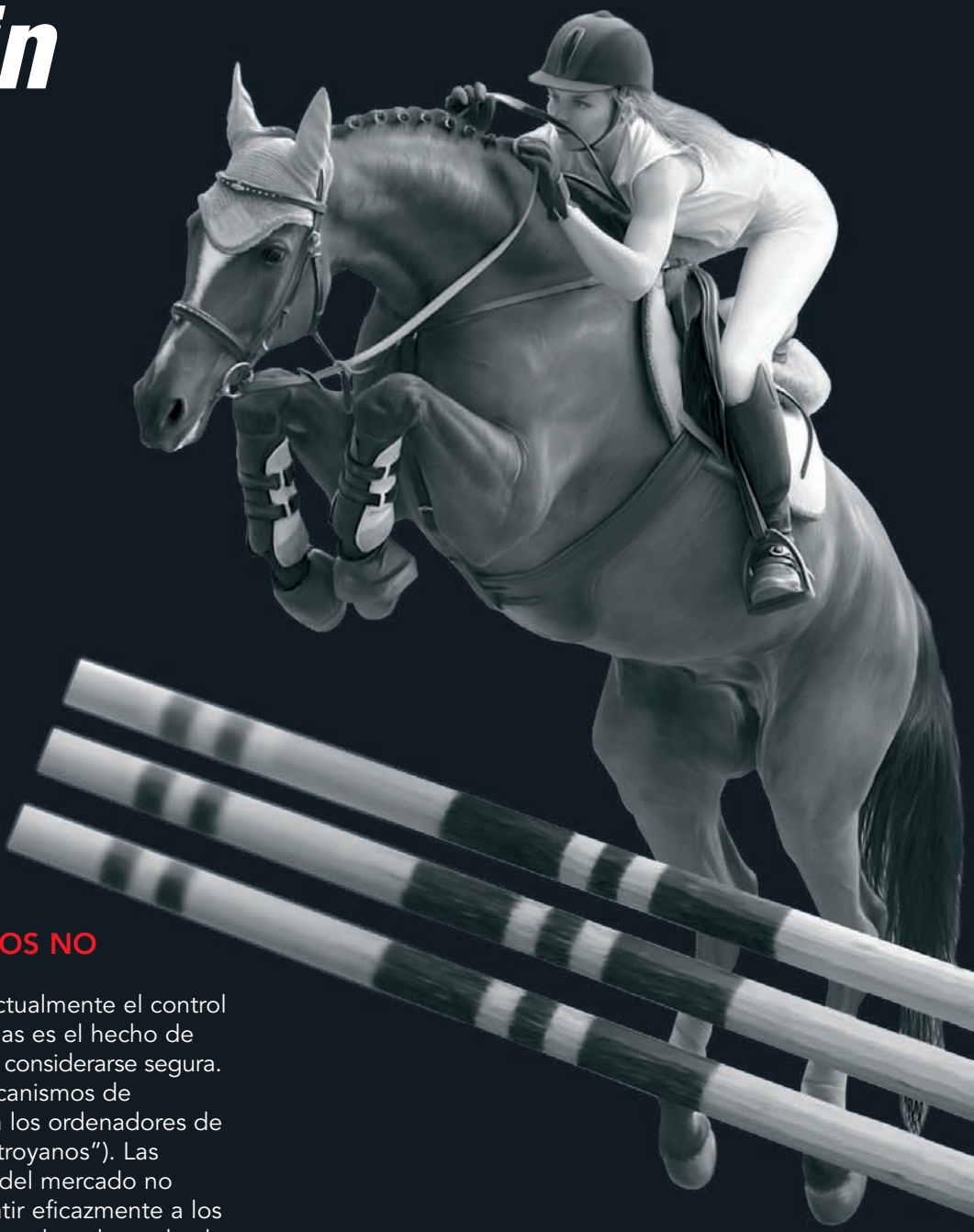
codelogin



UN MURO QUE LOS TROYANOS NO PODRÁN SALTAR

El mayor desafío al que se enfrenta actualmente el control de acceso remoto seguro a los sistemas es el hecho de que la plataforma de acceso no puede considerarse segura. Esto es así por la proliferación de mecanismos de introducción de software malicioso en los ordenadores de acceso (comúnmente denominados "troyanos"). Las aplicaciones anti-virus y anti-gusanos del mercado no pueden, por diversos motivos, combatir eficazmente a los troyanos. Garantizar por tanto que los ordenadores desde los cuales se accede remotamente a los sistemas están libres de troyanos es, en el mejor de los casos, una labor complicada cuando los ordenadores están bajo control de una organización que gestiona la seguridad, y en el peor de los casos, una labor imposible si son ordenadores públicos o personales bajo control del usuario.

codelogin utiliza el teléfono móvil del usuario para garantizar un acceso remoto seguro desde cualquier ordenador incluso en presencia de troyanos, y todo ello de una manera amigable y sencilla para el usuario.

GMV
Isaac Newton, 11 P.T.M. Tres Cantos 28760 Madrid
www.gmv.es marketing.tic@gmv.com

www.facebook.com/infoGMV
@infoGMV_es

gmv® INNOVATING SOLUTIONS

AERONÁUTICA | ESPACIO | DEFENSA | SANIDAD | SEGURIDAD | TRANSPORTE | TELECOMUNICACIONES | TECNOLOGÍAS DE LA INFORMACIÓN

codelogin

Las amenazas en que se concreta la presencia de troyanos pueden resumirse hoy en día en dos grandes grupos:

- El robo de credenciales u otra información sensible utilizada para el acceso.
- La ejecución de operaciones y/o transacciones fraudulentas sin conocimiento del usuario.

Los desarrollos clásicos han intentado paliar la primera amenaza utilizando dispositivos de autenticación fuerte, bien basados en claves de un solo uso, bien basados en infraestructuras de clave pública. Ambas soluciones presentan el inconveniente de requerir una amplia gestión, generalmente mucho mayor que la gestión tradicional de usuario y clave.

En cuanto a la segunda amenaza, la única manera de paliarla es utilizar plataformas y canales alternativos que se consideren seguros (en el sentido de confiables). Incluso la disponibilidad de sistemas de autenticación robusta sólo consigue que el troyano, que controla el ordenador cliente sin conocimiento del usuario, pueda acceder libremente al sistema, para que seguidamente pueda ejecutar las transacciones que desee de manera encubierta.

SEGURIDAD Y USABILIDAD

codelogin utiliza el teléfono móvil del usuario como "token" de autenticación, como plataforma de ejecución segura, como repositorio de claves privadas y como canal de comunicación alternativo, autenticado y cifrado, utilizando específicamente tecnologías adecuadas para minimizar las necesidades de gestión asociadas.

codelogin únicamente requiere que el teléfono móvil del usuario esté equipado con cámara y tenga acceso a Internet, bien mediante red móvil o WiFi. ***codelogin*** es tan sencillo de usar como hacer una foto con el móvil y tiene múltiples ventajas:

- ***codelogin*** permite el acceso seguro a cualquier usuario a un sistema local o remoto utilizando tecnologías de autenticación fuerte (doble factor: "algo que tienes" y "algo que sabes").
- ***codelogin*** utiliza como dispositivo de autenticación el teléfono móvil habitual del usuario (que proporciona el "algo que tienes" sin necesidad de adquirir un token adicional).
- ***codelogin*** proporciona acceso al sistema sin que el usuario tenga que utilizar ningún periférico del ordenador desde el cual se accede (ni el teclado ni el ratón).
- ***codelogin*** evita que el software malicioso, residente en el ordenador cliente, manipule transacciones sensibles del usuario o realice transacciones fraudulentas.

MÍNIMA GESTIÓN Y FÁCIL DESPLIEGUE

Un gran obstáculo al despliegue de sistemas robustos de autenticación hasta ahora ha sido la complejidad de gestión que representa su implantación y mantenimiento. Por todo ello, el diseño de ***codelogin*** incluye características únicas con el objeto de mejorar sustancialmente su despliegue y gestión posterior:

- Permite compatibilizar el acceso seguro con el acceso clásico mediante clave, posibilitando un despliegue progresivo y permitiendo el acceso en casos puntuales en los que no se disponga del móvil o de cobertura.
- Proporciona acceso basado en tecnologías de clave pública que no requieran el despliegue y la gestión de certificados, eliminando de la ecuación la complejidad de su gestión.
- Permite que el sistema al cual se accede pueda habilitarse para el uso de ***codelogin*** realizando el mínimo de cambios posibles en el mismo.
- Mantiene la experiencia de usuario a la hora de realizar transacciones en el sistema.
- Simplifica al máximo la gestión de la identidad del usuario y la gestión remota de la aplicación móvil.

CARACTERÍSTICAS TÉCNICAS

- ***codelogin*** incluye módulos de gestión de la identidad fácilmente integrables en cualquier plataforma y aplicaciones para su despliegue en los teléfonos móviles más utilizados.
- Seguridad equivalente a 1024 bits RSA.
- Tecnología de clave pública basada en la Identidad.
- Disponibles para teléfonos iPhone, Android, Windows Mobile y BlackBerry, entre otros.