# Información sobre seguridad con TeamViewer

© 2011 TeamViewer GmbH, Última actualización: 5/2011

# Grupo destinatario

Este documento va dirigido a administradores de redes corporativas. La información contenida en este documento es de índole técnica y muy detallada. Basándose en esta información, los profesionales de TI obtendrán una idea amplia sobre la seguridad del software antes de usar TeamViewer. Sírvase distribuir este documento entre sus clientes para resolver posibles cuestiones sobre seguridad.

Si usted no se considera dentro del grupo destinatario, la información divulgativa de la sección "La empresa / el software" le ayudarán a hacerse una idea.

# La empresa / el software

## Quiénes somos

La TeamViewer GmbH tiene su sede en la ciudad del sur de Alemania Göppingen (cercana a Stuttgart) y fue fundada en 2005. Nos dedicamos exclusivamente al desarrollo y la venta de sistemas seguros para colaboración basada en Internet. Un comienzo y un crecimiento rápidos han hecho posible que en un período corto de tiempo se hayan alcanzado varios millones de instalaciones del software TeamViewer y la presencia de usuarios en más de 200 países en todo el mundo. Actualmente, el software está disponible en más de 30 idiomas.

## Nuestro concepto de seguridad

TeamViewer es usado millones de veces en todo el mundo para ofrecer ayuda espontánea a través de internet o para acceder a ordenadores no ocupados (p. ej. soporte remoto para servidores). En función de cómo se haya configurado TeamViewer, podrá controlar el ordenador remoto como si estuviera sentado justo delante de él. Si el usuario que ha iniciado sesión en un ordenador remoto es un administrador de Windows, Mac o Linux, también recibirá permisos de administrador en ese ordenador.

Resulta obvio que una funcionalidad de tal capacidad a través de internet (con sus consiguientes riesgos para la seguridad), deberá estar convenientemente protegida contra los diversos ataques posibles. De hecho, la seguridad es el foco de atención del resto de nuestros objetivos de desarrollo para garantizar el acceso seguro a su ordenador y también en nuestro propio interés: millones de usuarios de todo el mundo confiarán únicamente en una solución segura y sólo una solución segura nos garantizará el éxito a largo plazo como empresa.

## Gestión de la calidad

A nuestro modo de ver, la gestión de la seguridad resulta impensable sin un sistema establecido de gestión de la calidad. TeamViewer GmbH es uno de los pocos proveedores del mercado que cuentan con un sistema de gestión de la calidad certificado conforme a ISO 9001. Nuestro control de calidad cumple con los estándares reconocidos en el plano internacional. Nuestro sistema de control de calidad es revisado cada año por medio de auditorías externas.

## Evaluación experta externa

Nuestro software TeamViewer ha recibido el sello de calidad cinco estrellas (valor máximo) de la Asociación Federal de Expertos y Consultores de TI (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). Los consultores independientes de la BISG e.V. examinan la calidad, seguridad y propiedades de servicio de los productos de fabricantes cualificados.

## Inspección relativa a la seguridad

Las empresas alemanas FIDUCIA IT AG y GAD eG (ambas operadoras de centros de procesamiento de datos para alrededor de 1200 bancos) inspeccionaron a TeamViewer por temas relativos a la seguridad y han homologado TeamViewer para el uso en estaciones de trabajo en bancos.

## Referencias

En el momento en que se actualizó la información por última vez TeamViewer estaba en uso en más de 100.000.000 ordenadores. Grandes consorcios internacionales de todo tipo de sectores (incluidos los extremadamente sensibles como el bancario y otras instituciones financieras) usan ya TeamViewer con éxito.

Si lo desea, puede consultar nuestras referencias en internet para obtener una primera impresión del nivel de acogida del que goza nuestra solución. Probablemente estará de acuerdo en que puede suponerse que la mayoría de las empresas tenían requisitos similares en cuanto a seguridad y disponibilidad antes de decidirse, luego de un intensivo estudio, por TeamViewer. Para que se forme usted mismo su criterio, también le ofrecemos algunos detalles técnicos en los siguientes párrafos.

# Creación y funcionamiento de una sesión en TeamViewer

## Creación de una sesión y tipos de conexiones

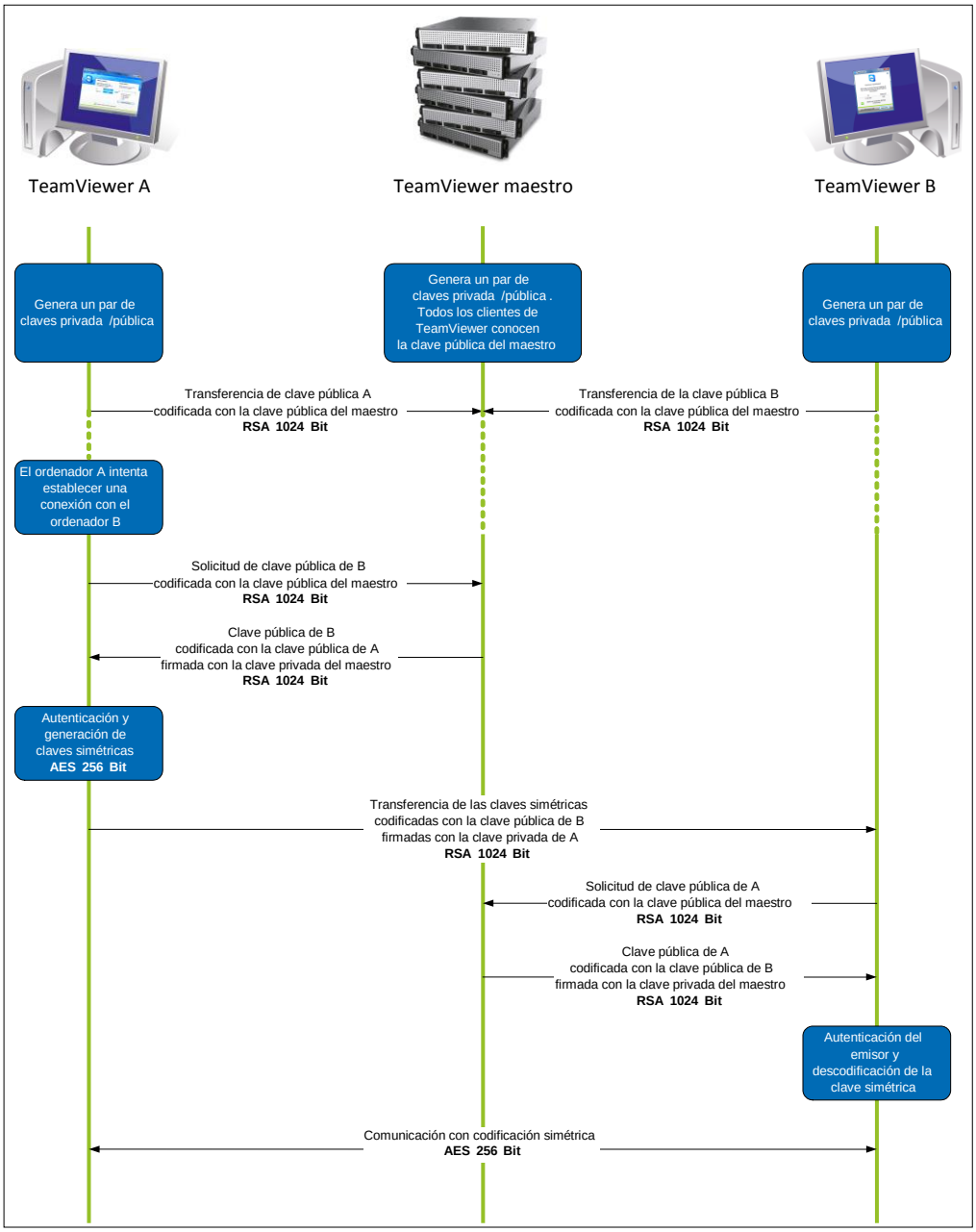
Al crear una sesión, TeamViewer determina el mejor tipo de conexión. Después de que nuestros servidores maestros efectúan la autenticación, en el 70% de los casos se establecerá directamente la conexión a través de UDP o TCP (incluso con gateways estándar, NAT y firewalls). El resto de conexiones se direccionan a través de nuestra red de routers altamente redundante vía TCP o http-tunnelling. No tiene que abrir ningún puerto para trabajar con TeamViewer.

Como se describe más adelante en el apartado "Cifrado y autenticación", ni siquiera nosotros, que somos los operadores de los servidores de enrutamiento, podemos leer el tráfico de datos cifrados.

## Cifrado y autenticación

TeamViewer funciona con un sistema de cifrado completo que se basa en intercambio de clave pública/privada RSA y codificación de sesión AES (256 bit). Esta tecnología se usa de modo similar para https/SSL y puede considerarse completamente segura de acuerdo con el estándar actual. Como la clave privada no abandona nunca el ordenador cliente, se asegura por medio de este procedimiento que los ordenadores interconectados (incluidos los servidores de enrutamiento de TeamViewer) no podrán descifrar el flujo de datos.

Cada cliente de TeamViewer ha implementado ya la clave pública del cluster maestro y puede, de este modo, cifrar mensajes para el servidor maestro y comprobar la firma del mismo. La PKI (Public Key Infrastructure) previene eficazmente los ataques de intermediario o MitM ("Man-in-the-middle"). A pesar del cifrado, la contraseña no se envía nunca directamente, sino a través de un procedimiento de desafío-respuesta y únicamente se guarda en el ordenador local.




*Cifrado y autenticación de TeamViewer*

## Validación de las ID de TeamViewer

Las ID de TeamViewer son generadas automáticamente por el mismo TeamViewer conforme a ciertas características de hardware. Los servidores de TeamViewer comprueban la validez de la ID antes de realizar cualquier conexión, de modo que no es posible generar ni utilizar ID falsas.

## Protección contra ataques de fuerza bruta

Cuando un cliente potencial pregunta sobre la seguridad de TeamViewer, seguramente preguntará también por el cifrado. Parece lógico que lo más temido sea el riesgo de que un tercero pueda llegar a conocer el mecanismo de conexión o de que se intercepten los datos de acceso a TeamViewer. En realidad, muy a menudo se trata de ataques muy elementales que suelen ser los más peligrosos.

En el contexto de la seguridad informática, los ataques de fuerza bruta suelen consistir en intentos para averiguar por el método de tanteo una contraseña que protege un recurso. Con el crecimiento de la potencia de los ordenadores estándar, el tiempo necesario para averiguar incluso contraseñas largas se ha reducido considerablemente.

Como defensa contra los ataques de fuerza bruta, TeamViewer aumenta exponencialmente la latencia entre los intentos de conexión. Para 24 intentos se necesitan 17 horas. La latencia vuelve a iniciarse sólo tras introducir la contraseña correcta.

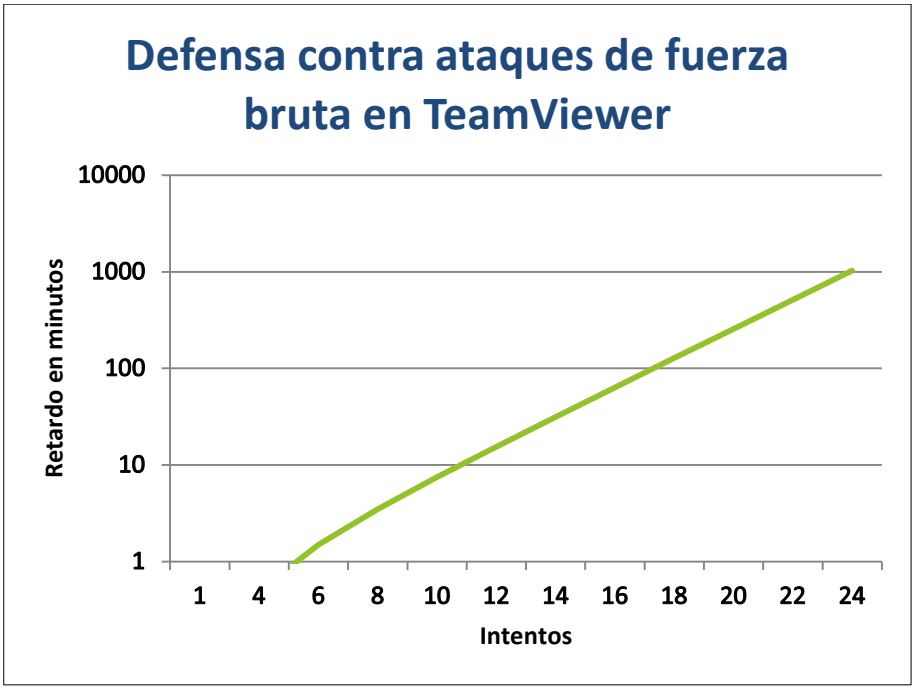



*Tabla: Tiempo transcurrido tras los intentos de conexión durante un ataque de fuerza bruta.*

## Code Signing

Otra función adicional de seguridad es que todos nuestros productos de software van firmados con VeriSign Code Signing. Gracias a ello, el editor del software siempre podrá ser fácilmente identificado. Si el software cambia, la firma digital queda automáticamente inutilizada.
Incluso los módulos Teamviewer personalizables se firman dinámicamente durante su generación.

## Datacenter y backbone

Estos dos temas están relacionados tanto con la disponibilidad como la seguridad. Los servidores centrales de TeamViewer está ubicado en un centro de datos ultramoderno con conexión redundante múltiple y fuentes de alimentación redundante. Se usa exclusivamente hardware de marca (Cisco, Foundry, Juniper).

El acceso al centro de datos sólo es posible tras una comprobación exhaustiva de la identidad a través de una única puerta de entrada. Nuestros servidores están protegidos contra ataques desde dentro mediante CCTV, detección de intrusos, vigilancia 24 horas y personal de seguridad in situ.

## Seguridad de la aplicación en TeamViewer

### Lista negra y lista blanca

Especialmente si se usa TeamViewer para el mantenimiento de ordenadores desatendidos (es decir, TeamViewer se instala como servicio de Windows), puede resultar interesante, aparte del resto de mecanismos para garantizar la seguridad, restringir el acceso a estos ordenadores a un número específico de clientes.

Con la función de lista blanca, se puede indicar expresamente qué ID de TeamViewer tienen permiso de acceso a este ordenador, mientras que con la función de lista negra se pueden bloquear determinadas ID de TeamViewer.

### Sin modo invisible

No hay ninguna función que permita el funcionamiento de TeamViewer completamente en segundo plano. Incluso si la aplicación funciona como servicio de Windows en segundo plano, TeamViewer estará siempre visible por medio de un icono en la bandeja del sistema.

Tras establecer la conexión, habrá siempre un pequeño panel de control visible sobre la bandeja del sistema; TeamViewer no se ha diseñado para controlar de forma oculta ordenadores o personal.

### Protección por contraseña

Para ayudar de forma espontánea a clientes, TeamViewer (TeamViewer QuickSupport) genera una contraseña de sesión (una contraseña de un solo uso). Si su cliente le comunica su contraseña, podrá conectarse al ordenador del cliente introduciendo la ID y la contraseña. Tras el reinicio de TeamViewer en el lado del cliente se genera una nueva contraseña de sesión, de modo que otra persona sólo podrá acceder a sus ordenadores si se le invita explícitamente.

Al utilizar TeamViewer para el soporte remoto de ordenadores no ocupados (p. ej. servidores), se fija una contraseña individual que asegura el acceso a este ordenador.

### Control de acceso entrante y saliente

Puede configurar de modo individual los modos de conexión de TeamViewer. Así, por ejemplo, podrá configurar su soporte remoto u ordenador para presentaciones de forma que no sean posibles conexiones entrantes.

Al limitar la capacidad total sólo a las funciones realmente necesarias se están eliminando posibles puntos débiles para ataques potenciales.

## ¿Tiene más preguntas?

Si tiene alguna duda, responderemos con mucho gusto a su llamada al +34 931 842 346 (España) o +1 800 951 4573  (EE.UU.) o a su correo a support@teamviewer.com.

## Contacto

TeamViewer GmbH
Kuhnbergstr. 16
D-73037 Göppingen
Germany
service@teamviewer.com

Trade register: Ulm HRB 534075