TeamViewer se toma en serio **la protección de datos**

Como empresa alemana, estamos dedicados a cumplir el nivel de seguridad alemán más alto. Contamos con varias medidas para garantizar la seguridad de sus datos, la privacidad de su negocio y la protección frente al fraude. Además de proteger sus datos a través del cifrado y la autenticación de dos factores, el usuario también tiene acceso a otras funciones útiles para mantener la seguridad durante su trabajo diario.

Seguridad TeamViewer

El ID de TeamViewer
Es exclusivo para su dispositivo, se genera automáticamente y se verifica antes de cada sesión.

El nivel de seguridad más alto del mundo
Nuestro centro de datos principal cumple con los estándares de seguridad industrial ISO 27001.

Protección de ataques
Con TeamViewer, el lapso de tiempo entre intentos de conexión fallidos crece exponencialmente y solo se elimina cuando la contraseña dada es correcta. También se protegen de los ataques los dispositivos que reciben el acceso remoto, y sus usuarios.

La contraseña de TeamViewer
TeamViewer genera automáticamente una nueva sesión dinámica después de cada servicio reiniciado de TeamViewer. También existe una funcionalidad opcional que le permite configurar contraseñas dinámicas en cada sesión. La contraseña es alfanumérica y está formada por 6 caracteres, lo que implica más de 2,1 mil millones de combinaciones posibles.

Protocolo de Seguridad Remoto (SRP)
TeamViewer usa el protocolo SRP para la autenticación y el cifrado de contraseñas. La contraseña nunca se envía por Internet, ni siquiera encriptada; por ello, provee una protección óptima de los accesos externos. Las contraseñas reciben una codificación adicional en el backend.

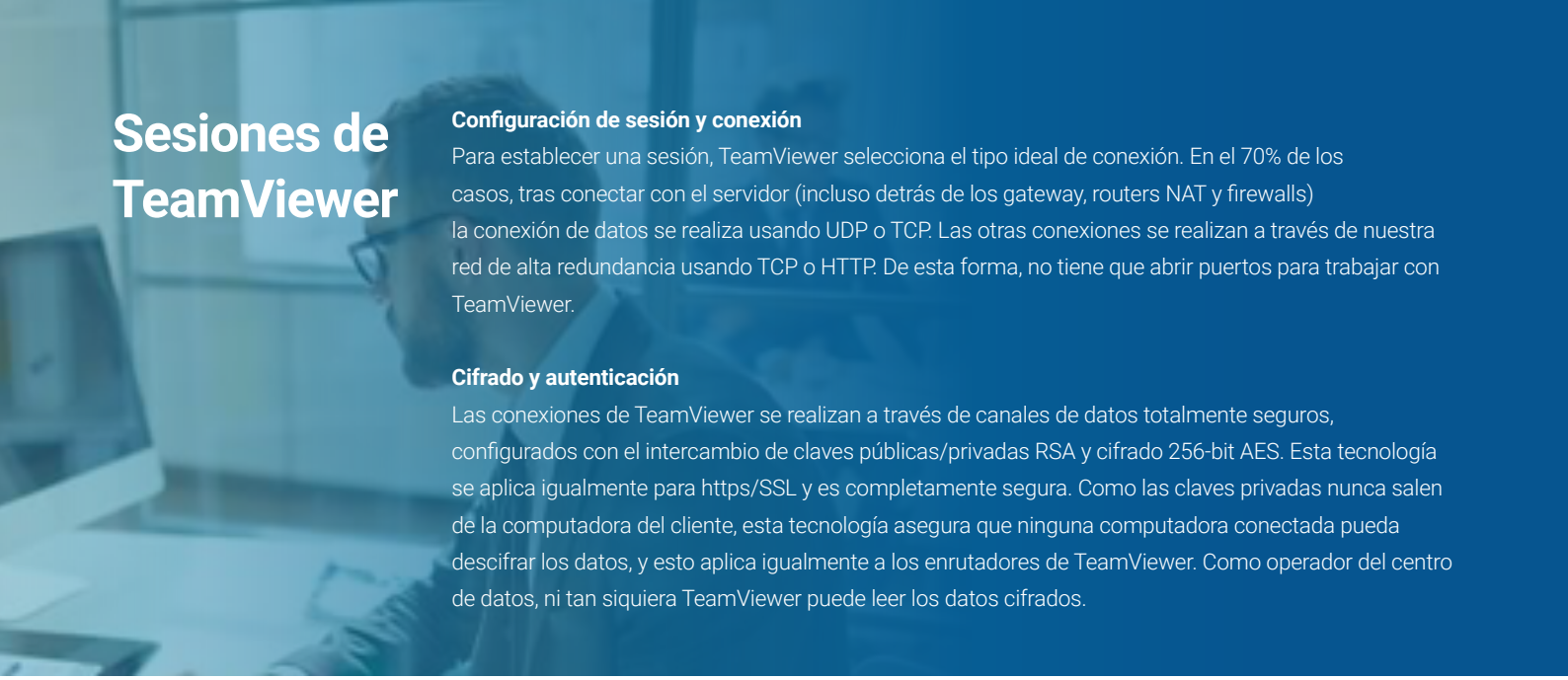
Cifrado
Todas las interacciones a través de TeamViewer incluso las transferencias de archivos, VPN, chats etc., están protegidas no autorizadas por el cifrado end-to-end con clave de 4096-bit RSA pública/privada.

Acceso Condicional*
Con el Acceso Condicional puede mejorar las normas de acceso remoto para prevenir actividades no autorizadas y ajustar las reglas de seguridad.

Autenticación de dos factores
En este caso, el login se produce con un código nuevo y único, generado cada vez por un algoritmo y ofrecido desde un celular.

**Disponible con TeamViewer Tensor.*
Se aplican términos y condiciones

AICPA SOC · A-LIGN HIPAA · südcert ISO 9001 · digicert · ISO ISO/IEC 27001



Sesiones de TeamViewer

Configuración de sesión y conexión

Para establecer una sesión, TeamViewer selecciona el tipo ideal de conexión. En el 70% de los casos, tras conectar con el servidor (incluso detrás de los gateway, routers NAT y firewalls) la conexión de datos se realiza usando UDP o TCP. Las otras conexiones se realizan a través de nuestra red de alta redundancia usando TCP o HTTP. De esta forma, no tiene que abrir puertos para trabajar con TeamViewer.

Cifrado y autenticación

Las conexiones de TeamViewer se realizan a través de canales de datos totalmente seguros, configurados con el intercambio de claves públicas/privadas RSA y cifrado 256-bit AES. Esta tecnología se aplica igualmente para https/SSL y es completamente segura. Como las claves privadas nunca salen de la computadora del cliente, esta tecnología asegura que ninguna computadora conectada pueda descifrar los datos, y esto aplica igualmente a los enrutadores de TeamViewer. Como operador del centro de datos, ni tan siquiera TeamViewer puede leer los datos cifrados.

Cumplimiento y protección de datos

Dispositivos de confianza

Requiere autenticación la primera vez que cada nuevo dispositivo intente el login en una cuenta existente de TeamViewer.

Integridad de datos

Ofrecemos la protección necesaria contra los cibercriminales. El sistema analiza constantemente los comportamientos en la cuenta de un usuario y si detecta algo extraño, genera una nueva contraseña automáticamente.

Permitidos/bloqueados

Esta función ofrece una protección especial si TeamViewer está instalado en computadoras que reciben acceso remoto sin supervisión. La lista de permitidos determina cuales clientes tienen acceso. La lista de bloqueados decide cuales ID de TeamViewer son bloqueados.

ISO/IEC 27001

Nuestro principal centro de datos está certificado con ISO/IEC 27001, que representa el nivel internacional de seguridad y control.

ISO 9001:2015

TeamViewer está certificado con la ISO 9001:2015 para la Calidad de Gestión de Sistemas (QMS).

General Data Protection Regulation (GDPR)

El 25 de mayo de 2018, la ley europea General Data Protection Regulation (Regulación General de Protección de Datos) (GDPR) entró en vigor, reflejando la importancia de la protección de datos en el mundo digital de nuestro tiempo. Como compañía internacional, TeamViewer es consciente de la importancia que tiene la protección de la información personal para nuestros clientes y por eso, cumplimos plenamente con la GDPR. Para descubrir más sobre el cumplimiento de la ley de protección de datos, visite nuestra base de conocimiento.

HIPAA, HITECH y Certificado SOC2

TeamViewer ha recibido certificaciones HIPAA, HITECH y SOC2 a través de A-LIGN, un proveedor estadounidense de seguridad. Mientras que HIPAA y HITECH son esenciales para asegurar la confidencialidad y seguridad de datos de información electrónica de salud (PHI), la SOC2 es un marco de presentación de informes para las organizaciones no financieras, con el propósito de aumentar la educación de los clientes sobre los 5 Principios de la Confianza de Servicios (Trusted Service Principles, TSP).

TeamViewer

TeamViewer US
5741 Rio Vista Dr
Clearwater, FL 33760
EE.UU.

¡Conectémonos!

TV-DS-ES-MX-032021-2