DELL Technologies

Puerta de enlace de conexión segura

Nuestra tecnología integra la protección de datos y la prevención de amenazas en una experiencia de asistencia segura y automatizada

Hasta un

60 %

de los líderes de tecnología informática encuestados por Forrester aprovechan la tecnología de conectividad para reducir riesgos[1]

También se implementa como una versión de conexión directa para un tipo determinado de hardware de Dell EMC y un plugin de servicios en OpenManage Enterprise para servidores PowerEdge. Dell Technologies Services tiene el compromiso de implementar capacidades de seguridad basadas en los mercados, las normativas y la información de los clientes, que contribuyen a que nuestros productos se ajusten a los objetivos de seguridad y los requisitos de cumplimiento de normas de nuestros clientes.

Contenido

1. Introducción:

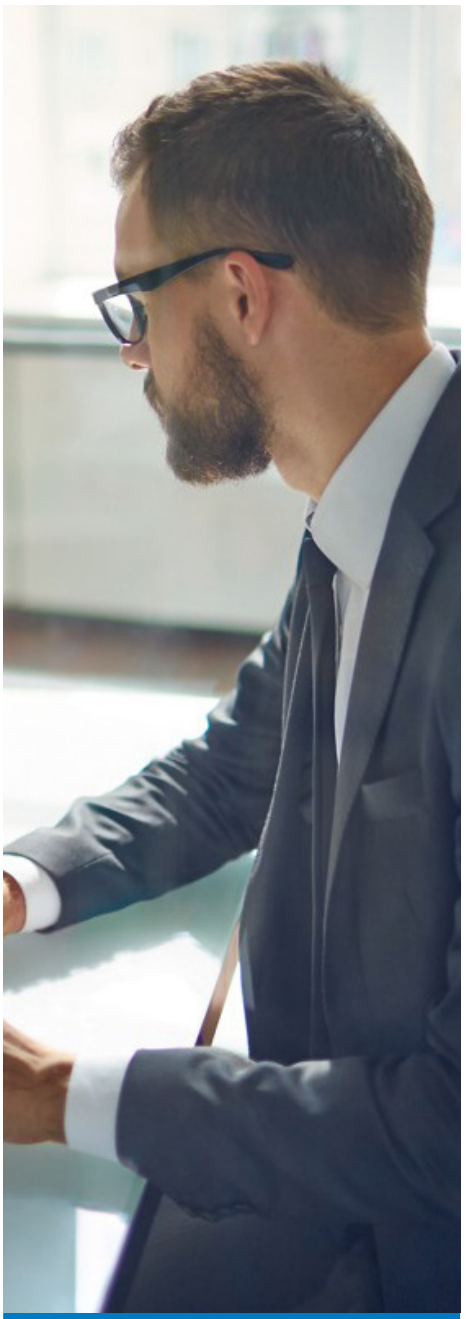
En el mundo hiperdigital actual, los líderes de innovación de éxito están recurriendo a los proveedores de servicios de tecnología informática para externalizar la asistencia en este campo. De acuerdo con un estudio de Forrester Consulting encargado por Dell Technologies Services[1], el 59 % de los directivos de tecnología informática afirman que colaborar con un proveedor de servicios de tecnología informática adecuado les ayuda a cambiar la dedicación del tiempo de su personal de operaciones diarias a iniciativas estratégicas.

Como proveedor de servicios de TI líder, Dell Technologies Services tiene el compromiso de garantizar que sus servicios y tecnologías de asistencia informática no sean posibles fuentes de amenazas de seguridad. Todos los días, hacemos todo lo que está en nuestra mano para minimizar los riesgos para nuestros clientes provenientes de los productos Dell EMC implementados en sus entornos. En este artículo se analiza cómo se integra la seguridad en el diseño, la implementación y el funcionamiento de la conectividad para la puerta de enlace de conexión segura a fin de garantizar una experiencia de asistencia informática automatizada y segura para una infraestructura de centro de datos compleja.

Basándose en más de 25 años de tecnología de asistencia informática pionera, la arquitectura de seguridad de la puerta de enlace de conexión segura se ha desarrollado para evitar las incursiones de amenazas y proteger la integridad de los datos. Mientras, nuestra tecnología supervisa de forma continua los dispositivos de los clientes en caso de problemas e inicia una resolución acelerada:

- Solo utilizamos los datos de telemetría y eventos de sistemas activos.
- Ciframos los datos del estado del sistema para su transmisión por Internet a través de HTTPS mediante el protocolo de seguridad de capas de transporte (TLS).
- Nuestros ingenieros de asistencia técnica autorizados utilizan la autenticación de varios factores para acceder de forma remota y resolver problemas en los sistemas conectados.
- Procesamos, almacenamos y utilizamos los datos de telemetría y eventos en nuestras ubicaciones utilizando las prácticas de seguridad líderes en el sector.

Además, analizamos rigurosamente las medidas de seguridad integradas en toda la arquitectura y los procesos de la puerta de enlace de conexión segura con múltiples proveedores de primera clase, como Secureworks, para garantizarle una experiencia privada y segura de confianza.



La ciberataques y el fraude o el robo de datos se encuentran entre las diez principales preocupaciones de los consejeros delegados[2]

2. Acerca de la puerta de enlace de conexión segura

Dell Technologies ofrece una tecnología de conectividad segura que elimina las conjeturas de la prevención de problemas, lo que le proporciona más tiempo para centrarse en los proyectos más importantes. Las ediciones de dispositivo virtual y aplicación proporcionan una conexión bidireccional segura entre su entorno y Dell Technologies Services, ideal para monitorizar dispositivos de Dell EMC en todo su centro de datos, incluidos el almacenamiento de datos, los servidores, las redes, la CI/HCI y la protección de datos, todo en un solo lugar.

También puede implementar nuestra tecnología de forma flexible como versión de conexión directa de determinados productos de Dell EMC y con un plugin de servicios en OpenManage Enterprise para servidores PowerEdge. Visite Dell.com/Support y verifique las opciones de conectividad compatibles para hardware y software específicos de Dell EMC.

Los datos son la esencia de la puerta de enlace de conexión segura. Aprovechamos los datos del estado del sistema de los entornos de los clientes y los correlacionamos con años de datos de incidentes e ingeniería de los equipos de asistencia técnica y de campo, así como de los fabricantes de componentes.

Consulte los elementos notificables de la puerta de enlace de conexión segura y del plugin de servicios de OpenManage Enterprise para obtener más detalles acerca de la información sobre el estado del sistema que se recopila.

Al utilizar sofisticados modelos de IA, incluido el aprendizaje automático, nuestra tecnología de conectividad puede encontrar y aplicar patrones para detectar con precisión y a la primera el problema correcto sobre el que actuar. Identifica los problemas de hardware y software, crea un caso e inicia el contacto con nosotros para empezar a resolver un fallo antes de que se convierta en un costoso problema. Si está conectada mediante la puerta de enlace de conexión segura, también predice fallos en los discos duros y los planos posteriores del servidor. En función del tipo de problema, la alerta también puede iniciar un envío automático de piezas.

Además, la tecnología permite una comunicación bidireccional segura para los agentes de asistencia técnica autorizados para acceder de forma remota a los dispositivos administrados con el fin de identificar los problemas y resolverlos.

SEGURIDAD PARA LA CONECTIVIDAD

Se llevan a cabo evaluaciones de terceros sobre la seguridad de la puerta de enlace de conexión segura y su infraestructura de asistencia.

Las evaluaciones de la aplicación incluyen el transporte de datos y la seguridad de la API, el análisis estático y dinámico del código fuente, los controles cruzados de las vulnerabilidades y las exposiciones comunes (CVE) y del Proyecto de seguridad de aplicaciones web abiertas (OWASP) y las bibliotecas y los productos de terceros.

Las evaluaciones de la infraestructura incluyen los dispositivos de red internos y externos, los servidores y los proveedores de servicios.

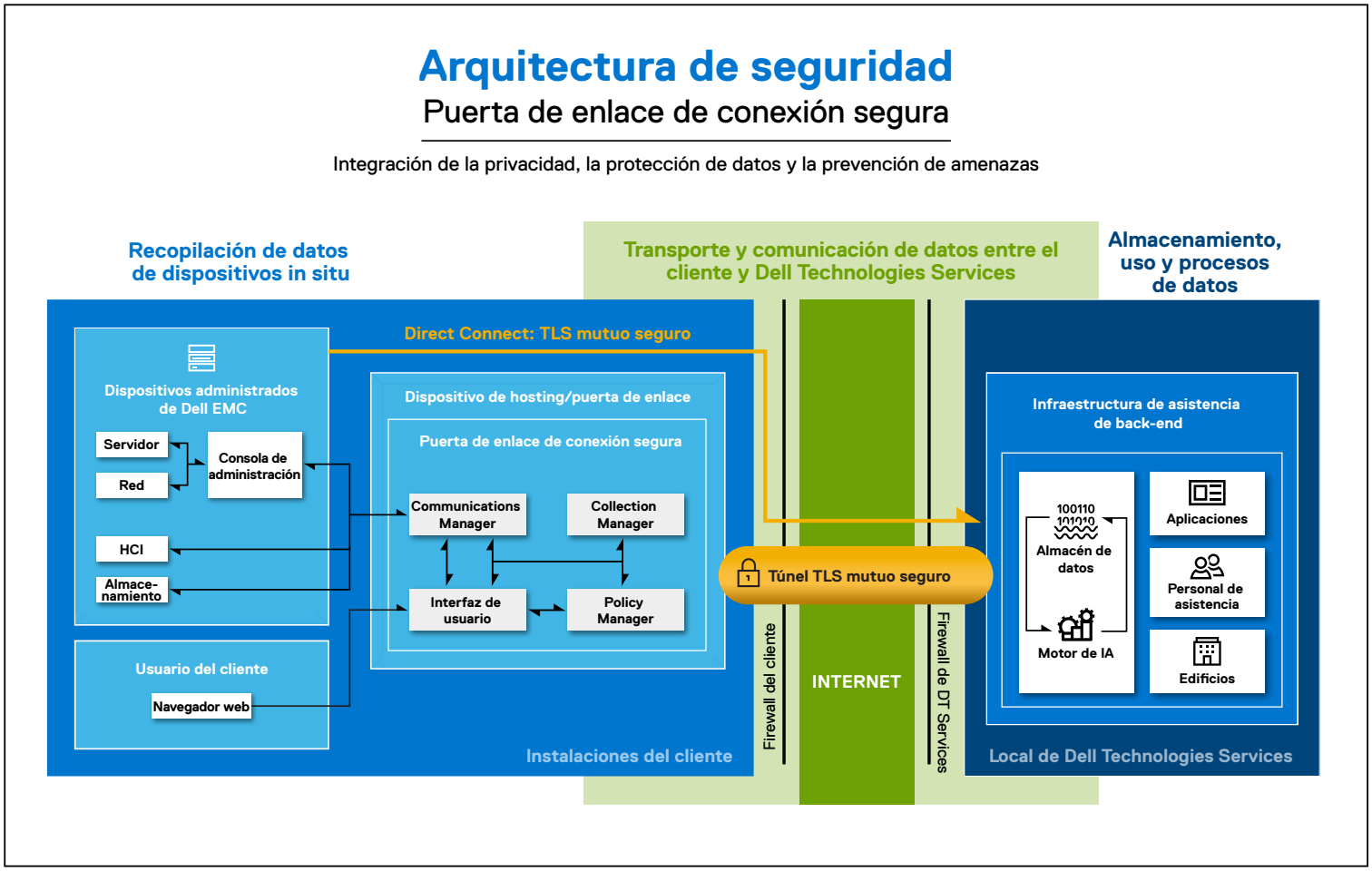
3. Descripción general de la arquitectura de seguridad

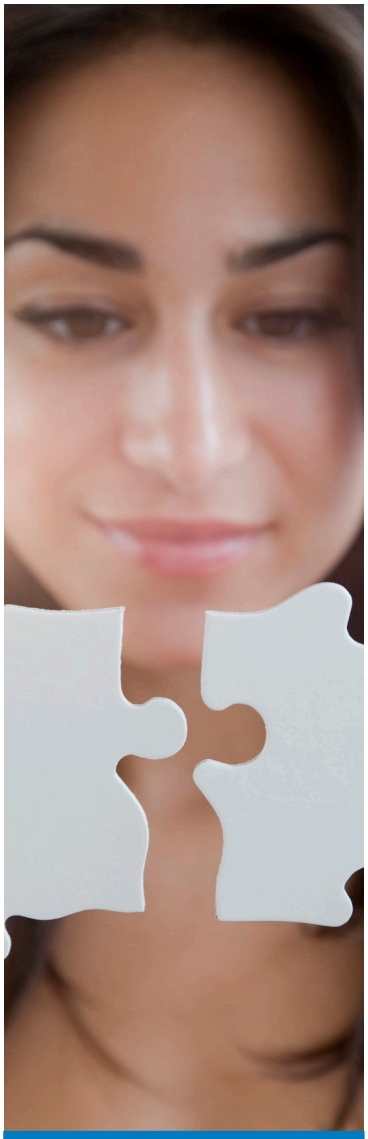
Dell Technologies Services tiene el compromiso de minimizar el riesgo de amenazas de seguridad en nuestra tecnología de conectividad automatizada, proactiva y predictiva. Nuestra arquitectura de seguridad está diseñada para cumplir los rigurosos estándares del sector y se ajusta a las prácticas de seguridad medibles y repetibles en cada paso del desarrollo y la implementación de los productos. Consulte la sección 4 para obtener más información.

En el diagrama A siguiente se proporciona una descripción general de la arquitectura de seguridad de la puerta de enlace de conexión segura. En las secciones siguientes, se analiza la manera en la que nuestra tecnología solo recoge los datos de sistema de los dispositivos de Dell EMC gestionados que se necesitan para diagnosticar y corregir los problemas y, a continuación, trata esos datos con la máxima seguridad y privacidad:

- Recopilación de datos de dispositivos in situ
- Transporte y comunicación de datos
- Almacenamiento, uso y procesos de datos en Dell Technologies Services

Diagrama A:





Los clientes ganan un nivel adicional de seguridad para la recopilación de datos in situ gracias a las capacidades de auditoría del administrador de directivas en la puerta de enlace de conexión segura.

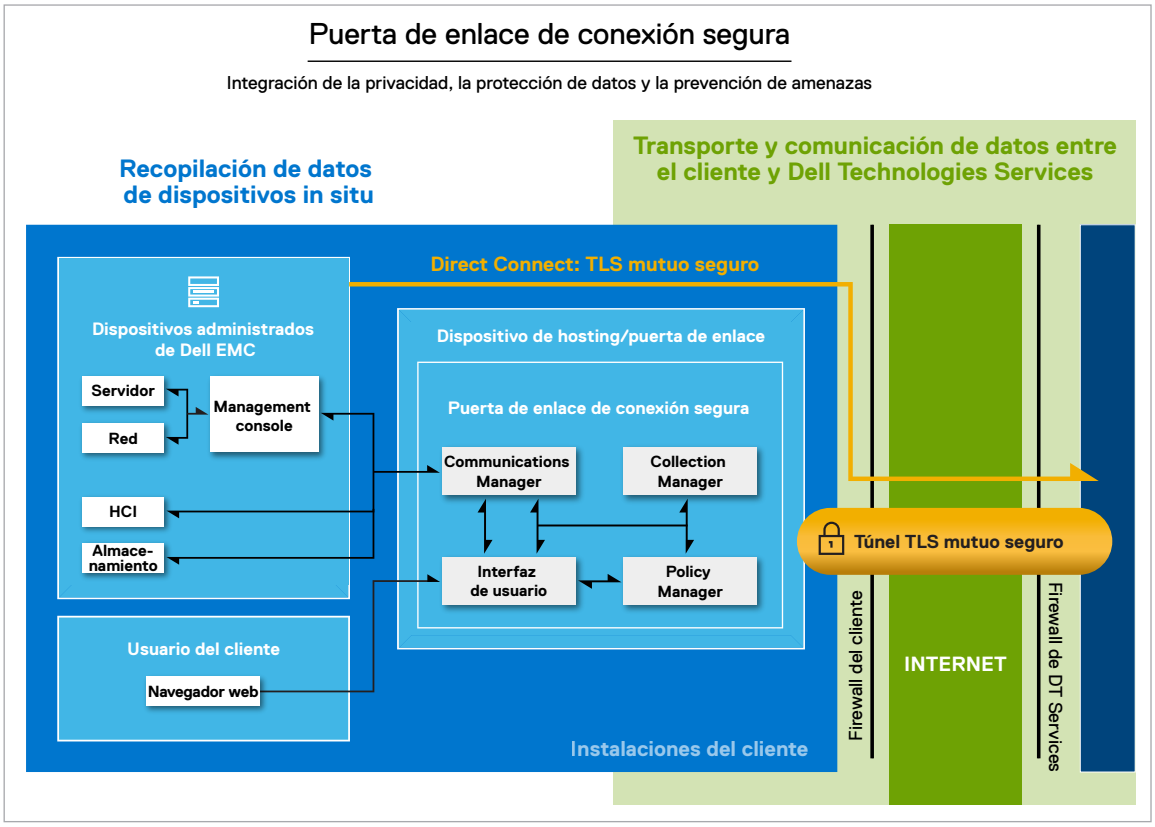
4. Detalles del enfoque de seguridad de la puerta de enlace de conexión segura

4.1. Recopilación de datos in situ segura

Minimización de los puntos de acceso del firewall

La puerta de enlace de conexión segura agrega las comunicaciones entre los dispositivos Dell EMC y actúa como un punto único de entrada y salida en el firewall de un cliente para toda la actividad de servicios remotos basados en IP (véase el diagrama B). Al minimizar los puntos de acceso del firewall para la tecnología de asistencia informática remota, Dell Technologies reduce el riesgo para la seguridad a través del firewall de la empresa.

Diagrama B: (fragmento del Diagrama A – Arquitectura de seguridad):



Como puerta de enlace in situ, la puerta de enlace de conexión segura se implementa virtualmente en un hipervisor proporcionado por el cliente. Cada servidor de puerta de enlace actúa como proxy y transporta información desde los dispositivos gestionados y viceversa. La puerta de enlace de conexión segura también puede poner en cola eventos de Connect Home en el caso de que se produzca un fallo temporal en la red local. Estos servidores de puerta de enlace tienen su propia interfaz de usuario web basada en el sistema operativo subyacente.

Para algunos clientes, la versión de conexión directa es conveniente para la implementación heterogénea de varios productos de hardware de Dell EMC. Esta solución actúa como un único punto de comunicación seguro a través del firewall del cliente. Se integra en el entorno operativo del producto y, por lo tanto, no requiere un servidor independiente para proporcionar soporte remoto de entrada y funcionalidad Call Home.

Minimización de los puntos de acceso del firewall (continuación)

Para los clientes con un centro de datos PowerEdge que utilicen la consola de administración de sistemas de OpenManage Enterprise, el plugin de servicios integrado es una opción de implementación alternativa. Este plugin de conectividad, que se encuentra dentro del dispositivo virtual de OpenManage Enterprise, se ejecuta en un hipervisor proporcionado por el cliente. Actúa como una capa de automatización de servicios desde dispositivos de chasis y de servidores gestionados, y proporciona una conexión directa única y segura con el back-end de Dell Technologies Services.

Actuar como intermediario de comunicaciones seguro

La puerta de enlace de conexión segura funciona como intermediario de comunicaciones entre los dispositivos gestionados, el administrador de directivas y la infraestructura de asistencia de back-end de Dell Technologies Services. Los servidores de puerta de enlace en los que se implementan son controladores HTTPS. La puerta de enlace aprovecha diferentes métodos de comunicación, como la detección de dispositivos, la gestión de eventos, la recopilación de datos de telemetría y la administración de datos de telemetría. Los tipos de mensajes incluyen:

- Sondeo del latido del estado del dispositivo
- Transferencia de archivos de datos (Connect Home)
- Transferencia de datos de uso de licencias
- Solicitudes de autenticación de usuarios
- Sincronización de administración de dispositivos

Todos los mensajes se protegen mediante varios protocolos. En una sección posterior, examinaremos de cerca la seguridad adicional integrada en el transporte y la comunicación de datos de la puerta de enlace de conexión segura, incluido el uso del protocolo HTTPS con túneles de seguridad de capas de transporte (TLS) de extremo a extremo y el cifrado estándar en el sector.

Control por el cliente de los requisitos de autorización y los permisos de acceso

Si la puerta de enlace de conexión segura supervisa los dispositivos en un centro de datos del cliente, el cliente puede optar por utilizar el administrador de directivas para controlar los requisitos de autorización de las conexiones de acceso remoto, las ejecuciones de scripts de diagnóstico y otras actividades relacionadas. Los clientes pueden establecer permisos de acceso para el personal, así como para los ingenieros de asistencia técnica que se conectan de forma remota para diagnosticar y solucionar problemas.

La seguridad de la administración de autorizaciones y permisos está garantizada por las siguientes funciones del administrador de directivas:

- La puerta de enlace de conexión segura sondea regularmente el administrador de directivas para verificar cambios en los permisos y almacena en caché los permisos localmente. En el caso del administrador de directivas:
  - La caché del conjunto de reglas se renueva automáticamente con las actualizaciones de configuración tras su último ciclo de sondeo.
  - Está configurado para recibir mensajes como proceso de escucha HTTPS en un puerto específico y acordado.
- Cuando la puerta de enlace de conexión segura recibe una solicitud de acceso remoto o cualquier otra acción, aplica la política recibida de la caché del administrador de directivas.
  - Los permisos se pueden asignar jerárquicamente con políticas basadas en tipos de dispositivos o modelos específicos en un tipo de dispositivo.
  - Los clientes pueden aceptar o rechazar la acción solicitada a través de la interfaz de usuario web del administrador de directivas. También pueden crear filtros para establecer restricciones adicionales a las autorizaciones y las acciones.

Registros y pistas de auditorías

Los clientes disfrutan de un nivel adicional de seguridad para la recopilación de datos in situ gracias a las capacidades de auditoría del administrador de directivas en la puerta de enlace de conexión segura. El administrador de directivas registra todos los eventos y conexiones de servicios remotos, las ejecuciones de scripts de diagnóstico y las operaciones de transferencia de archivos de asistencia. A continuación, los almacena en su base de datos como archivos de registro de auditoría de texto plano. Realiza un seguimiento del acceso a sí mismo (al administrador de directivas), de los cambios en las políticas y de todas las actividades de autorización o denegación de acceso.

Los clientes tienen toda esta información al alcance de la mano, ya que:

- Las auditorías se visualizan a través de la interfaz de usuario web del administrador de directivas y no se pueden modificar.
- Los registros de auditoría también se pueden configurar para que se transmitan a un servidor syslog en su entorno.

Puerta de enlace de conexión segura

Suites de cifrado TLS 1.2 compatibles:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Opción de seguridad de control de dispositivos

Como los clientes no siempre habilitan el administrador de directivas para la gestión de permisos y autorizaciones, la puerta de enlace de conexión segura proporciona características de seguridad relacionadas a través de la opción de control de dispositivos.

Los clientes pueden:

- Crear grupos personalizados en función del tipo de dispositivo, del grupo de administradores, de la organización o de la unidad de negocio, de la ubicación física del dispositivo o de cualquier otro criterio que elijan.
- Definir los permisos y derechos de acceso específicos de estos grupos de dispositivos.

Todas las operaciones de administración de dispositivos, incluida la actividad remota de los ingenieros de asistencia técnica, quedan registradas. También deben ser aprobadas en el back-end por un agente de asistencia técnica.

De este modo, los clientes mantienen un control y una transparencia completos de los dispositivos administrados a través de la puerta de enlace de conexión segura.

Autenticación de dos factores y gestión de certificados digitales

La autenticación es un componente importante de la recopilación de datos in situ segura. La puerta de enlace de conexión segura utiliza un certificado digital como prueba de identidad de su implementación en el servidor de puerta de enlace del cliente. El certificado vincula la identidad del servidor de puerta de enlace a un par de claves que se utiliza para cifrar y autenticar la comunicación con el back-end. La autoridad de certificación (CA) de Dell Technologies Services es el repositorio central de la infraestructura clave de la puerta de enlace de conexión segura.

La administración de certificados digitales se utiliza para automatizar la inscripción del certificado digital a través de nuestra autoridad de certificación privada. Esta:

- Permite la generación y la autenticación programáticas de cada solicitud de certificado.
- Garantiza que el certificado solo se emite e instala en el servidor de puerta de enlace. El certificado no se puede copiar y utilizar en otro equipo.

La puerta de enlace de conexión segura se conecta y autentica mediante el certificado digital implementado en nuestra infraestructura de asistencia de back-end. Los agentes de asistencia técnica se conectan a la puerta de enlace de conexión segura en el entorno del cliente mediante la autenticación de dos factores.

4.2. Transporte y comunicación de datos seguros

Túnel de comunicación seguro

La puerta de enlace de conexión segura inicia todas las comunicaciones entre el cliente y la infraestructura de asistencia de back-end de Dell Technologies Services como salida desde el sitio del cliente. Crea un túnel de comunicación seguro de extremo a extremo utilizando el cifrado de 256 bits de seguridad de capas de transporte (TLS) estándar del sector a través de Internet y la autenticación de certificados digitales firmada por Dell Technologies Services. Esta última se detalla en la sección anterior sobre la recopilación de datos in situ segura.

En consecuencia, las conexiones de la puerta de enlace de conexión segura tienen las propiedades siguientes:

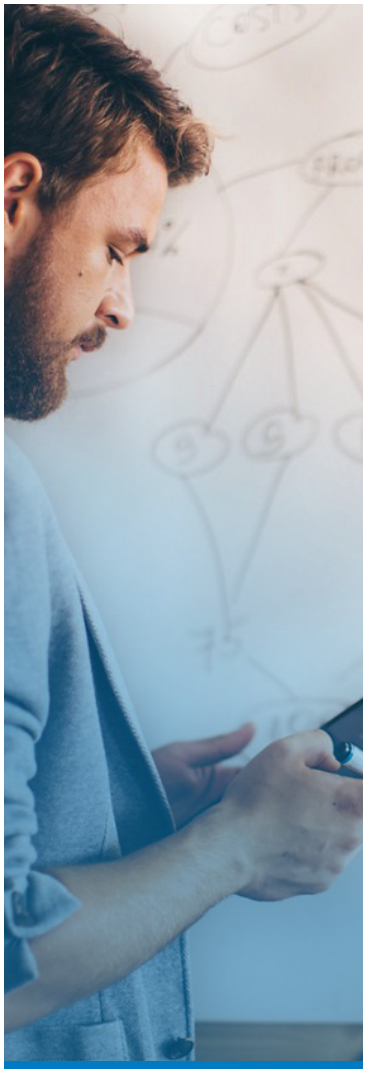
- **Transferencia de datos fiable:** cada mensaje transmitido incluye una comprobación de integridad del mensaje mediante un código de autenticación de mensajes para evitar una pérdida o una alteración de los datos no detectadas durante la transmisión.
- **Sesión privada y segura a través de TLS:** el cifrado simétrico mediante algoritmos estándar del sector genera claves exclusivas para cada conexión. Las comunicaciones no se pueden modificar durante la negociación sin ser detectadas.
- **Partes autenticadas:** puesto que esta conexión es segura, identifica a las partes comunicantes y las autentica con criptografía de clave pública. Este enfoque evita la suplantación y los ataques de tipo Man-in-the-Middle (MITM).

Comunicaciones mediante el túnel TLS seguro

El servidor de puerta de enlace utiliza el túnel TLS para garantizar un entorno seguro para las siguientes funciones: sondeo de latido, notificación remota y acceso remoto. En esta sección y según el diagrama C, examinamos más detenidamente estos procesos y protocolos de comunicación básicos para disfrutar de la experiencia automatizada, proactiva y predictiva de nuestra tecnología.

Sondeo de latido

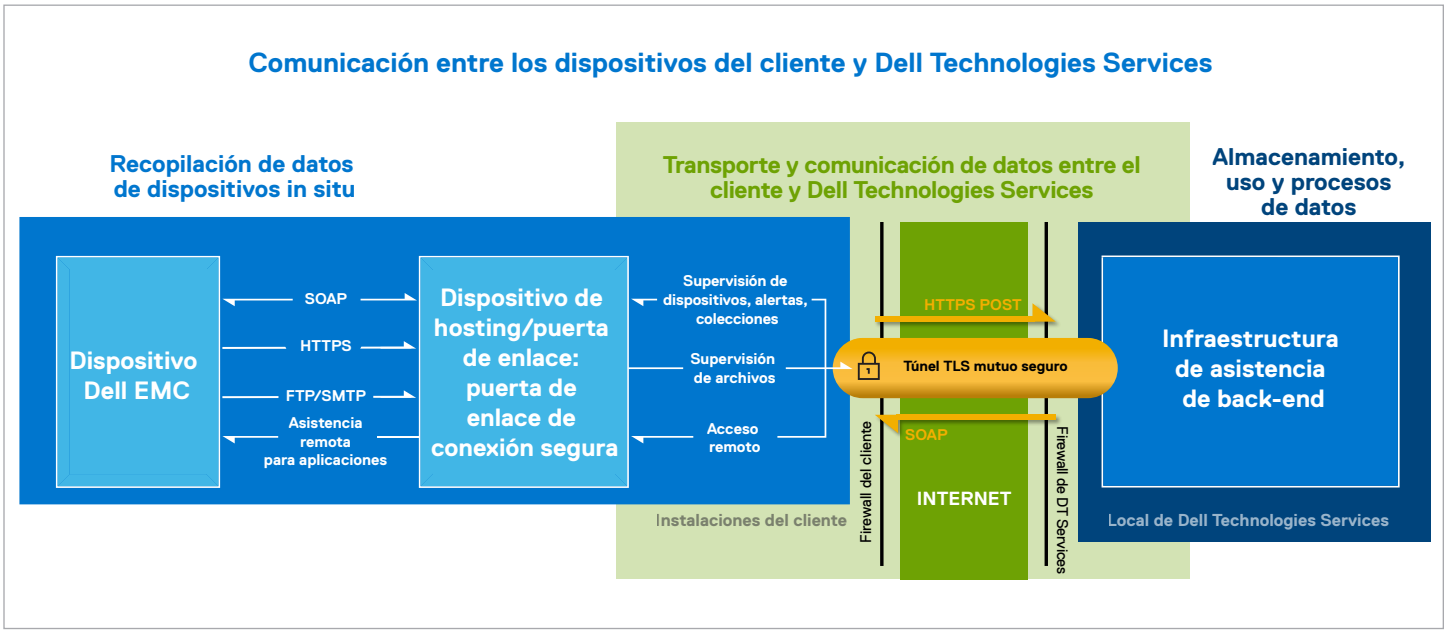
Los sistemas de los clientes deben estar conectados para beneficiarse de la experiencia de la puerta de enlace de conexión segura. El sondeo de latido comprueba el estado de la conectividad de los dispositivos y comunica regularmente los datos de telemetría recogidos al back-end. Los datos también identifican el servidor de puerta de enlace en el que se ha implementado la puerta de enlace de conexión segura.



La autenticación líder en el sector protege las conexiones contra suplantaciones y ataques de tipo Man-in-the-Middle.

Comunicaciones mediante el túnel TLS seguro (continuación)

Diagrama C: arquitectura de seguridad



Función de notificación remota o Connect Home

La puerta de enlace de conexión segura sirve como vía segura para que los dispositivos envíen archivos de eventos al back-end. Estos contienen errores, alertas, condiciones de advertencia, informes de estado, datos de configuración y estados de ejecución de scripts.

- Cuando se genera una alerta, también se genera un archivo de evento, que se envía a la puerta de enlace.
- La puerta de enlace de conexión segura recibe el archivo a través de los servicios de proceso de escucha HTTPS.
- En el caso de los productos heredados que utilizan procesos de escucha FTP o SMTP para la puerta de enlace de conexión segura, los archivos se cifran y se transfieren.
- La puerta de enlace comprime el archivo y lo envía al back-end a través del túnel TLS. A continuación, elimina el archivo del directorio del proceso de escucha.
- Acto seguido, el archivo se descomprime en el back-end para su análisis.
- La puerta de enlace de conexión segura también puede enviar los archivos al back-end a través del túnel de comunicación cifrado. Además, la puerta de enlace puede configurarse para utilizar los canales de conmutación por error, a saber, FTPS o el servidor de correo electrónico del cliente.

Los datos de supervisión del sistema se recopilan de diversos componentes de un sistema activo para permitir que Dell Technologies Services proporcione una experiencia de asistencia adaptada, inteligente y acelerada. El identificador del sistema, que es necesario para identificar el sistema específico en el que se trabaja, es la única información sobre la empresa recopilada de los dispositivos. Cuando determinamos que una pieza debe enviarse proactivamente, utilizamos la información de contacto existente que se ha almacenado de forma segura en los servidores de Dell Technologies.

En los documentos sobre elementos notificables de la puerta de enlace de conexión segura y el plugin de servicios de OpenManage Enterprise puede encontrar una lista completa de los datos de supervisión que se recopilan de un sistema activo, incluidos los datos que se recopilan fuera del ciclo rutinario de 24 horas.

Acceso remoto

Nuestros equipos de asistencia técnica también acceden de forma remota a los dispositivos que se encuentran en el sitio del cliente para solucionar problemas o realizar acciones específicas en los mismos. La mensajería asincrónica garantiza que la sesión de acceso remoto se inicie mediante la puerta de enlace de conexión segura desde el sitio del cliente. A continuación, se establece una sesión de acceso remoto segura de la siguiente forma:

- Tras la autenticación de la sesión en el back-end de Dell Technologies Services, un agente de asistencia técnica solicita acceso a los dispositivos, incluido el número de solicitud de servicio, si está disponible, y otros identificadores de dispositivo o usuario.
- La solicitud de acceso remoto se pone en cola en el back-end hasta que la puerta de enlace envía el mensaje de latido del dispositivo al back-end para recuperarlo.
- En respuesta, el servidor de back-end envía una respuesta que incluye la información de la solicitud, la dirección del servidor de back-end y un identificador de sesión exclusivo para conectarse a la puerta de enlace.
- La puerta de enlace de conexión segura utiliza su repositorio local para determinar la dirección IP local del dispositivo. A continuación, comprueba la política almacenada en caché del administrador de directivas para examinar los permisos de conexión.
- Si se permite, la puerta de enlace de conexión segura establece una conexión TLS persistente independiente con el servidor de back-end. La conexión TLS siempre se inicia mediante la puerta de enlace de conexión segura. El servidor de back-end nunca puede iniciar una conexión de entrada con el servidor de la puerta de enlace. Esto garantiza que no haya vulnerabilidades frente a ataques externos.

La comunicación se transmite a través del túnel entre la puerta de enlace de conexión segura y el servidor de back-end hasta que finaliza o se supera el tiempo de espera tras un período de inactividad.

Seguridad de la red

Todos los componentes de supervisión de red se encuentran detrás de un firewall y son administrados por nuestro equipo de seguridad de la red. El tráfico de red se controla de forma estricta. Todo el tráfico de entrada se transmite a través de puertos específicos y solo se envía a las direcciones de la red de destino apropiadas.

4.3. Almacenamiento, uso y procesos de datos seguros

Seguridad para el almacenamiento y el uso

Seguridad física

Dell Technologies Services aloja la mayoría de los datos de la puerta de enlace de conexión segura, incluidos los componentes de la aplicación, los sistemas, las redes y la seguridad, en un centro de datos con sede en Estados Unidos diseñado para mantener altos niveles de disponibilidad y seguridad. Los datos están protegidos mediante el uso de una amplia variedad de medidas, incluida la seguridad física. Sus características son, entre otras:

- Guardias de seguridad en las instalaciones
- Cámaras
- Entradas falsas
- Barreras para vehículos
- Diseño de estacionamiento especializado
- Cristales y paredes antibalas
- Uso de un edificio sin letreros

El acceso a los centros de datos en los que está alojada la infraestructura está restringido al personal autorizado. El acceso se controla mediante una tarjeta inteligente.

Seguridad lógica

Los datos generados por la puerta de enlace de conexión segura se almacenan de conformidad con la Política de privacidad de Dell.

El acceso lógico a la infraestructura de Dell Technologies Services (servidores, equilibradores de carga, recursos compartidos de red, etc.) está restringido a través de herramientas internas que se auditan y evalúan según las directrices de TI:

Seguridad lógica (continuación)

- **Seguridad de servidores y bases de datos:** los servidores y los componentes del sistema operativo residen en imágenes estándares que han sido sometidas a revisiones de seguridad. Existen revisiones periódicas de las actualizaciones de seguridad utilizadas por la aplicación, incluidas las publicadas por Microsoft y otros proveedores de software. Cuando se emiten actualizaciones de seguridad esenciales, se prueban por primera vez en imágenes que no son de producción y, por lo general, se aplican a los servidores activos de forma oportuna para evitar riesgos.
- **Auditoría:** se mantienen registros de los dispositivos monitorizados, solo accesibles para la infraestructura y las aplicaciones autorizadas de Dell Technologies Services. Estos registros dejan constancia de todos los intentos de iniciar sesión o acceder al sistema operativo o a la consola de servidor web de la puerta de enlace de conexión segura.

Las estructuras administradas por el departamento de tecnología informática se refuerzan utilizando las recomendaciones del Center for Internet Security (CIS). También se implementan las directrices de seguridad estándar del sector en todos los servidores y equipos de red.

Por último, el ecosistema de la puerta de enlace de conexión segura emplea una alta disponibilidad local en el centro de datos y en una infraestructura idéntica en un centro de datos independiente. Las únicas excepciones son las tecnologías intrínsecamente de alta disponibilidad, como los clústeres de Big Data y las clouds privadas. Para los análisis de datos, Dell Technologies Services aprovecha los entornos de cloud que controlamos y gestionamos íntegramente, incluidas las clouds privadas, híbridas y públicas.

Utilizamos un proceso de desarrollo seguro y repetible para los productos y las aplicaciones

Autenticación

La puerta de enlace de conexión segura utiliza Dell MyAccount para la autenticación con Dell Technologies Services y los grupos de inicio de sesión del sistema operativo para la autenticación en el equipo.

A los grupos que tienen acceso a los componentes de la puerta de enlace de conexión segura, como el equipo de administración de bases de datos y el equipo de asistencia operativa, se les asignan derechos de acceso y obligaciones independientes. Todas las actualizaciones del entorno de producción pasan por un procedimiento de control de cambios definido que incorpora controles y contrapesos.

Seguridad para los procesos

Comunidad consciente de la seguridad

Ofrecemos un plan de estudios en seguridad basado en funciones de múltiples niveles para formar a empleados nuevos y existentes acerca de las prácticas recomendadas de seguridad específicas del trabajo y sobre el uso de los recursos pertinentes. Dell Technologies se esfuerza por crear una cultura orientada a la seguridad en toda la comunidad. Además, nuestra comunidad para desarrolladores forma parte del programa de Security Champion de Dell, diseñado para favorecer las pruebas de seguridad en nuestras prácticas de desarrollo de software.

Desarrollo

Nuestro **estándar de ciclo de vida de desarrollo seguro (SDL)** interno es una referencia común para las organizaciones de productos de Dell Technologies a fin de evaluar las actividades de desarrollo seguras de los productos y las aplicaciones en función de las expectativas del mercado y las prácticas del sector. Define los controles de seguridad que los equipos de productos deben adoptar mientras desarrollan nuevas características y funciones. El SDL incluye tanto las actividades de análisis como los controles proactivos normativos en áreas de riesgo clave. Las actividades de análisis, como el modelado de amenazas, el análisis de código estático, el escaneo y las pruebas de seguridad, están destinadas a detectar y abordar los fallos de seguridad durante todo el ciclo de vida del desarrollo. Los controles normativos están diseñados para garantizar que los equipos de desarrollo programen defensivamente a fin de evitar los problemas de seguridad específicos más frecuentes, incluidos los que se encuentran en el top 10 del Proyecto de seguridad de aplicaciones web abiertas (OWASP) o en el top 25 de SANS. La puerta de enlace de conexión segura ha adoptado

Desarrollo (continuación)

el marco de madurez de Dell SDL para la implementación de controles de seguridad en línea con los estándares del sector.

El código de la puerta de enlace de conexión segura se desarrolla a partir de la metodología de desarrollo ágil. El código se integra de forma continua utilizando el software de automatización estándar del sector. Las versiones del código se registran y se controlan mediante permisos de grupo seguros.

Todas las versiones de software se someten a una evaluación de la seguridad de acuerdo con nuestras políticas de seguridad, que incluye:

- Evaluación de vulnerabilidades mediante pruebas de penetración
- Pruebas de seguridad de terceros con varios de los mejores proveedores de su clase, como Secureworks
- Evaluación de las soluciones de autenticación, autorización y gestión de la identidad
- Todas las bibliotecas y los componentes de terceros se escanean con soluciones líderes del sector para el análisis de la composición de software. Además, se comunican las recomendaciones de seguridad de Dell con mejoras específicas en este campo.
- Clasificación de datos con nuestra organización de seguridad global. Este proceso aúna privacidad y seguridad para garantizar que los datos electrónicos estén protegidos.

Las aplicaciones también se someten a auditorías y controles de seguridad.

Gestión de los cambios

El proceso de gestión de cambios de Dell Technologies sigue las prácticas recomendadas de la Fundación ITIL según lo dictado por nuestro consejo de gestión de cambios corporativos. Todos los cambios se gestionan a través de tickets de solicitud de cambio. Quienes acceden a nuestro sistema para iniciar los cambios deben someterse a la formación de ITIL, así como familiarizarse con el SDL. Todas las actualizaciones y mejoras aplicadas a la infraestructura de back-end se controlan mediante su versión, para un seguimiento y una trazabilidad apropiados. El equipo emplea un proceso de creación automatizado para aplicar nuevas compilaciones o revocar cualquier compilación o reparación en caliente que se hayan implementado.

La aplicación instalada en el local de un cliente puede actualizarse en función de las preferencias de este. Cada versión promocionada en Dell.com/support contiene información sobre los cambios introducidos con cualquier limitación conocida.

Nuestro equipo de gestión de productos prepara todas las nuevas características y cambios, y estos se priorizan mediante un proceso de cambios del plan de acción que pasa por el consejo de control de cambios para su revisión y aprobación.

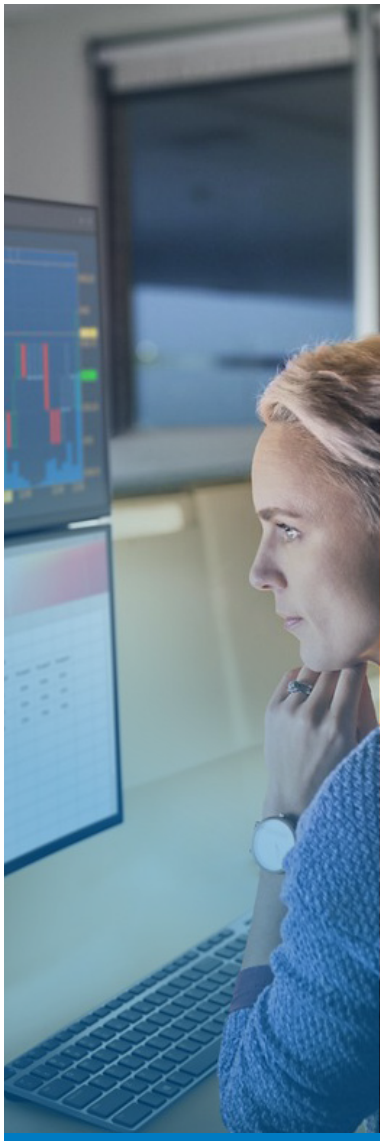
Gestión de riesgos de la cadena de suministros

Dell Technologies sigue las prácticas recomendadas líderes en el sector en cada una de las fases del ciclo de vida planificar-adquirir-realizar-entregar-devolver. Adoptamos un enfoque integral para proteger nuestra cadena de suministros, incluidos los estándares de SCRM y las prácticas recomendadas internacionales, con el fin de seguir siendo un proveedor de TIC de confianza en el mercado global.

Obtenga más información sobre las prácticas de garantía de la cadena de suministros aquí.

Creación de informes de incidentes

Cualquier persona de Dell Technologies que observe actividad sospechosa o sospeche un problema o una amenaza de ciberseguridad debe notificar el incidente inmediatamente a nuestro equipo de respuesta ante incidentes de seguridad (CSIRT). Esto incluye puntos débiles o brechas en los procesos de seguridad que puedan afectar a nuestro entorno o provocar un incumplimiento en los sistemas o los datos. Luego, el CSIRT inicia una investigación completa del incidente y la persona que haya notificado el incidente proporciona todos los artefactos y detalles necesarios para que el CSIRT lleve a cabo la investigación. El CSIRT utiliza el plan de respuesta ante incidentes del CSIRT, que detalla un proceso formal para responder y resolver Dell incidentes de ciberseguridad internos y no orientados al cliente. Estos incidentes pueden presentar amenazas potenciales para activos de Dell, redes de ordenadores o equipos de procesamiento de datos, así como para la información de Dell y sus filiales, personal, proveedores de servicios, socios o clientes.



Colaboración del sector en las prácticas recomendadas de seguridad de productos

Respuesta a vulnerabilidades

Dell Technologies se esfuerza por ayudar a nuestros clientes a minimizar los riesgos asociados a las vulnerabilidades de seguridad de nuestros productos proporcionándoles la información, la orientación y la mitigación oportunas para hacer frente a las amenazas de las vulnerabilidades. Nuestro equipo de respuesta ante incidentes de seguridad de productos (PSIRT) es responsable de coordinar la respuesta y la divulgación de todas las vulnerabilidades de los productos que nos han sido comunicadas. Todas las divulgaciones de vulnerabilidades de productos de Dell Technologies están disponibles en el sitio web.

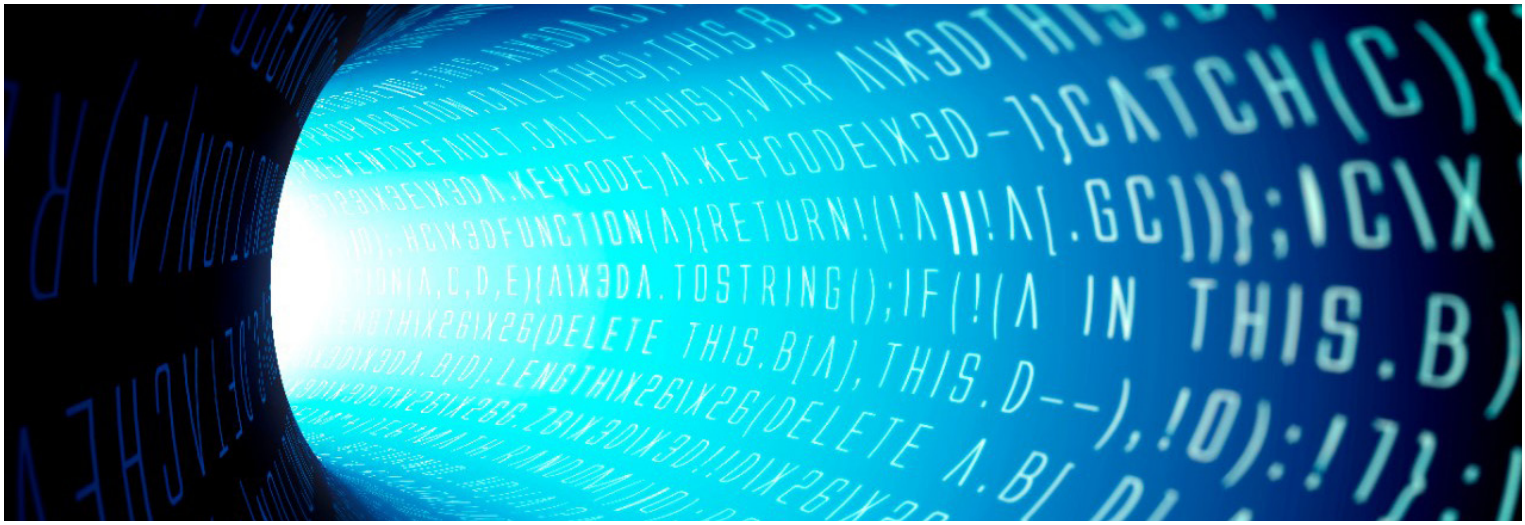
Más información sobre nuestra política de respuesta ante vulnerabilidades

Afiliaciones en el sector

Dell Technologies participa en varios grupos del sector para colaborar con otros proveedores líderes en la definición, la evolución y el intercambio de las prácticas recomendadas en materia de seguridad de los productos y en el fomento de la lógica del desarrollo seguro. Entre los ejemplos de colaboración en el sector se incluyen:

- Dell, a través de su entidad EMC, cofundó y en la actualidad preside la junta directiva de Software Assurance Forum for Excellence in Code (SAFECode). Entre el resto de miembros del consejo se cuentan representantes de Microsoft, Adobe, SAP, Intel, Siemens, CA y Symantec. Los miembros de SAFECode comparten y publican prácticas de seguridad y formación sobre software.
- Dell Technologies es miembro activo de The Forum for Incident Response and Security Teams (FIRST). FIRST es una organización de primer nivel y un líder global reconocido en la respuesta ante incidentes y vulnerabilidades.
- Participamos activamente en The Open Group Trusted Technology Forum (OTTF). OTTF lidera el desarrollo de un marco y un programa de integridad global de la cadena de suministros.
- Dell fue una de las primeras 9 empresas evaluadas por el proyecto Building Security In Maturity Model (BSIMM) en 2008 y ha seguido participando en dicha iniciativa. Un representante de Dell Technologies forma parte del Consejo Consultivo de BSIMM.
- Los empleados de Dell fueron miembros fundadores del IEEE Center for Secure Design, que se lanzó bajo la iniciativa de ciberseguridad del IEEE para ayudar a los arquitectos de software a comprender y abordar frecuentes defectos de diseño de seguridad.

Visite el Centro de seguridad y confianza para obtener recursos y soluciones destinados a responder a sus dudas sobre seguridad empresarial.



Estándares de seguridad del sector

Nuestros empleados participan activamente en los organismos normativos y en los consorcios del sector, que se centran en el desarrollo de estándares de seguridad y en la definición de prácticas de seguridad para todo el sector, entre los que se incluyen:

- Cloud Security Alliance (CSA)
- Distributed Management Task Force (DMTF)
- The Forum for Incident Response and Security Teams (FIRST)
- International Committee for Information Technology Standards (INCITS)
- Organización Internacional de Normalización (ISO)
- Grupo de Trabajo de Ingeniería de Internet (IETF)
- The Open Group
- Organización para el Desarrollo de Normas de Información Estructurada (OASIS)
- Software Assurance Forum for Excellence in Code (SAFECode)
- Storage Networking Industry Association (SNIA)

Certificación ISO 9001

Dell Technologies cuenta con la certificación ISO 9001. La empresa lleva a cabo periódicamente auditorías y revisiones de cumplimiento normativo trimestrales en todos sus centros de desarrollo y fabricación.

5: Conclusión

Nuestra tecnología de conectividad proporciona una experiencia de asistencia en tecnología informática fluida, con alertas proactivas y predictivas automatizadas que garantizan el máximo tiempo de actividad para la infraestructura esencial de los centros de datos. Los clientes que se asocian con Dell Technologies Services pueden estar seguros de nuestro compromiso con proporcionar una experiencia segura, privada y de confianza para la recopilación, la comunicación, el transporte, el uso y el almacenamiento de sus datos de telemetría.

Si tiene alguna duda o desea más información, visite **DellTechnologies.com/SecureConnectGateway**

1 Fuente: "The Role Of IT Services Providers Expands To Strategic Collaboration", estudio encargado por Dell Technologies y realizado por Forrester Consulting en su nombre, abril de 2021

2 Fuente: Informe de riesgos globales del Foro Económico Mundial 2021. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf