Descripción general de la seguridad de SupportAssist for Business PCs

Cinco preguntas clave que puede tener acerca de la seguridad de SupportAssist y sus respuestas.

SupportAssist le permite automatizar el soporte de Dell Technologies mediante la identificación de problemas de hardware y software en todo su equipamiento de PC. SupportAssist aborda los problemas de rendimiento y estabilización del sistema, reduce las amenazas de seguridad, monitorea y detecta las fallas de hardware y automatiza el proceso de interacción con el equipo de soporte técnico de Dell.

SupportAssist también recopila de manera proactiva datos de telemetría de sus PC y proporciona información valiosa sobre la utilización y corrección de estas en función de su plan de servicio.

Contenido

I: Introducción

Una falla en una laptop puede ser algo perturbador y frustrante. Estos problemas pueden afectar gravemente la productividad de un empleado, a menudo, en el peor momento posible. Debido a esto, los directores de sistemas de información de empresas se preocupan cada vez por la calidad y el tiempo de actividad de sus equipamientos de PC.

Muchos han recurrido a la tecnología más reciente y avanzada, que utiliza la información valiosa obtenida a partir de la ciencia de datos, para procesar miles de millones de puntos de datos y ayudar a los administradores de TI a ser más eficientes. La información del estado del sistema de los sistemas de usuario final se envía al departamento de TI DE la empresa o a un proveedor de hardware o software para resolver o prevenir problemas rápidamente. Dell ProSupport Plus con tecnología de conectividad SupportAssist le notifica sobre los discos duros defectuosos y le brinda una vista única de todo su equipamiento de PC desde el portal de TechDirect.

Si bien esta tecnología es necesaria para garantizar el tiempo de actividad y la eficiencia, los directores de sistemas de información a veces plantean preguntas sobre la información que recolecta y cómo la maneja.

Las siguientes preguntas se consideran críticas:

- ¿Qué datos recopila SupportAssist?
- ¿Cómo se protegen estos datos a medida que se transmiten al departamento de TI de la empresa o al proveedor de computadoras?
- Una vez que llega a su destino, ¿los datos se almacenan de tal manera que permanecen privados y seguros?
- ¿Cómo cumple Dell con el Reglamento General de Protección de Datos (RGPD) y otros estándares?

En este documento se analizan estas y otras preguntas relacionadas como medio para evaluar las tecnologías basadas en la ciencia de datos. Proporciona una breve descripción general de cómo SupportAssist, como parte de ProSupport Suite for PCs, ofrece un servicio de soporte integral capaz de predecir y resolver problemas antes de que ocurran. También proporciona un análisis detallado de cómo Dell Technologies Services protege la confidencialidad de la información en sus procesos, transporte y almacenamiento de datos.

II: Acerca de SupportAssist

SupportAssist es la tecnología de conectividad inteligente de Dell[1] que permite a las organizaciones recibir soporte técnico automatizado para todo su equipamiento de PC. Monitorea los dispositivos de los usuarios finales, detecta proactivamente los problemas de hardware y software y proporciona información valiosa sobre el uso de los sistemas.

Cuando se detecta un problema, SupportAssist abre un caso de soporte automáticamente con el soporte técnico, según el plan de servicio. El tipo de problema determinará si la alerta inicia una solicitud de soporte técnico o activa un despacho automático de piezas. SupportAssist recopila los datos de hardware y software que utiliza el equipo de soporte técnico para solucionar los problemas.

Dell ProSupport Suite for PCs ofrece las funcionalidades de soporte más completas en una sola solución, sin necesidad de acumular servicios.[2] Más información.

Características clave

- Detección proactiva y predictiva de todo el equipamiento para una resolución de problemas más rápida
- Análisis rápido de las puntuaciones de estado, de experiencia con las aplicaciones y de seguridad en una sola pantalla
- Biblioteca de scripts creados por Dell para automatizar tareas y solucionar problemas en todo el equipamiento
- Automatice la creación y la implementación de catálogos personalizados de actualizaciones para el BIOS, los controladores, el firmware y las aplicaciones de Dell
- Flexibilidad para personalizar las vistas y los paneles en TechDirect

Las características disponibles varían de acuerdo con el plan de soporte adquirido para las PC.

- Con ProSupport Plus, los usuarios finales reciben el conjunto completo de características de SupportAssist, incluidas la detección predictiva de problemas y la prevención de fallas.

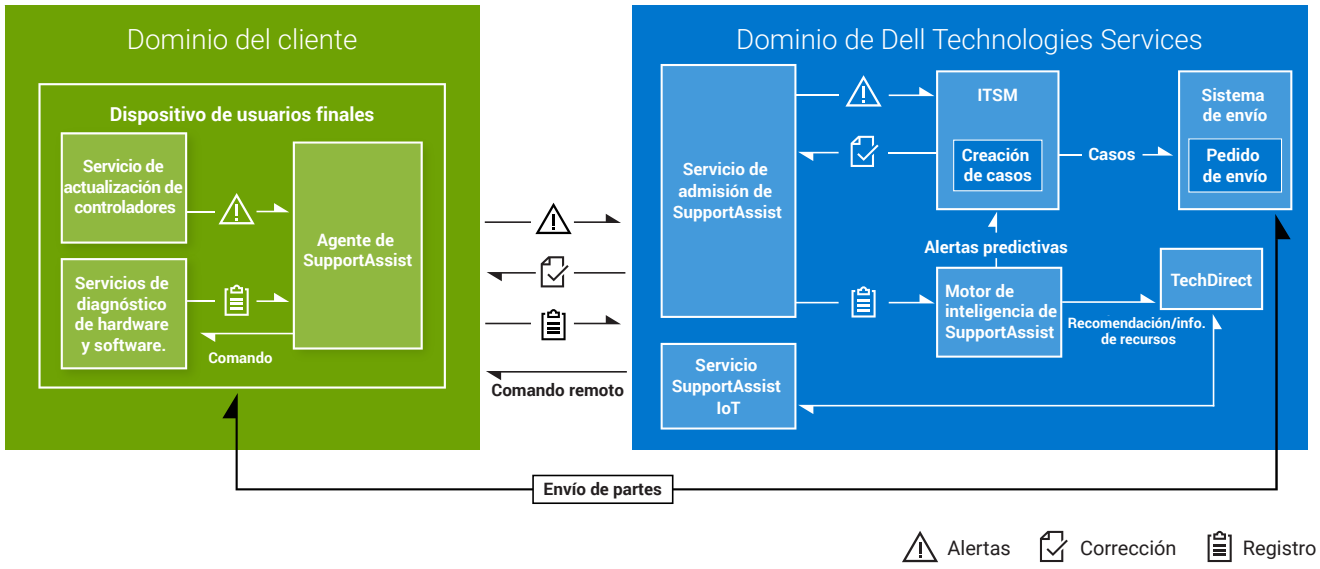
Para obtener una lista completa de las características y funcionalidades, consulte la Guía del administrador.

III. Arquitectura de SupportAssist

SupportAssist consta de un conjunto de servicios que monitorea los sistemas de manera continua y ejecuta evaluaciones del estado basadas en programas en un dispositivo. Esta información se transmite a los servidores de Dell Technologies para analizar los datos y ofrecer recomendaciones.

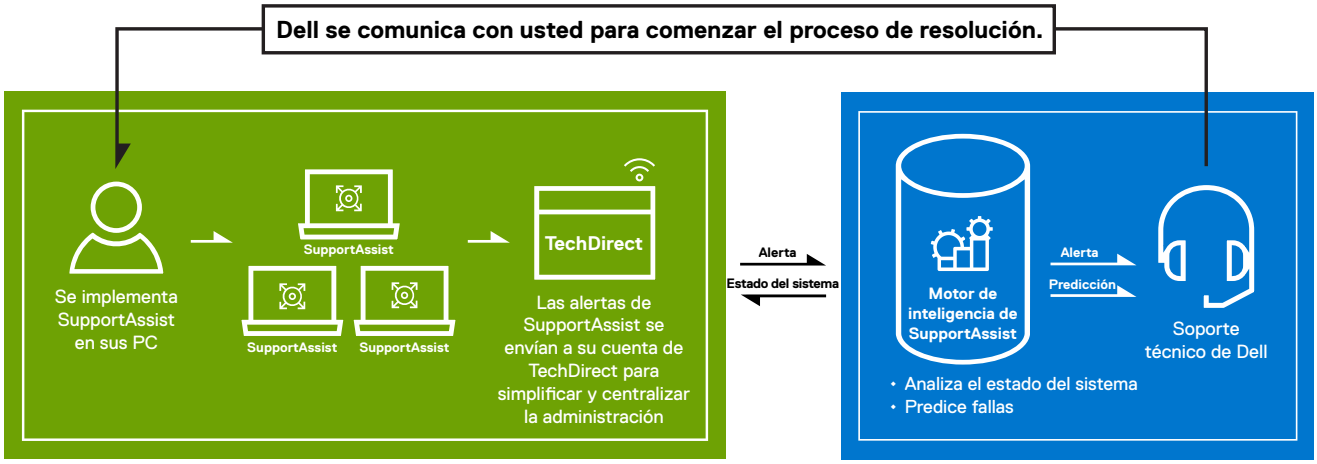
A fin de obtener una lista completa de los requisitos de red, terminales, puertos, firewalls o gateways para la implementación y corrección de SupportAssist, consulte nuestra Guía de implementación. Dell desarrolla, prueba y firma nuestros scripts de corrección, los que luego confirma antes de la ejecución.

Arquitectura de SupportAssist



Administre SupportAssist de forma centralizada mediante TechDirect

Las alertas de SupportAssist se pueden enviar a la cuenta de TechDirect de una organización para simplificar y centralizar la administración. Las organizaciones con un plan de servicio ProSupport o ProSupport Plus también pueden optar por reenviar alertas automáticamente a Dell Technologies Services.



Administre SupportAssist de forma centralizada mediante TechDirect (continuación):

La información valiosa de SupportAssist, un componente analítico muy útil, recopila datos de utilización del sistema que se pueden consultar en TechDirect. Esto incluye la utilización de la CPU, el espacio libre en el disco, la capacidad máxima de la batería, el tiempo de ejecución de la batería y muchos más datos útiles. TechDirect puede mostrar esta información para todos los sistemas, para los sistemas de un grupo de dispositivos específico o para un sistema individual. Los clientes pueden identificar los problemas de rendimiento y tomar mejores decisiones comerciales (por ejemplo, actualizar o reemplazar hardware).

IV. Seguridad de SupportAssist

Una organización puede tener preguntas sobre el tipo de datos que SupportAssist recopila y cómo se maneja esa información. En esta sección, se brindarán respuestas para estas preguntas, y se mostrará que SupportAssist recolecta solo los datos necesarios para solucionar los problemas de los clientes y luego los administra con un nivel óptimo de seguridad.

¿Qué datos recopila SupportAssist?

¿Cómo se protegen los scripts de corrección?

¿Cómo almacena y transporta SupportAssist los datos de manera segura?

¿Qué hace SupportAssist con los datos?

¿Cuáles son las políticas y prácticas de seguridad de Dell Technologies?

¿Qué datos recopila SupportAssist?

SupportAssist recopila automáticamente los datos necesarios para solucionar un problema y los envía de manera segura al equipo de soporte técnico. Estos datos nos permiten proporcionar una experiencia de soporte adaptable, inteligente y acelerada.

La etiqueta de servicio, necesaria para identificar el dispositivo específico del usuario final en el que se trabaja, es la única información sobre la empresa que se recopila de los dispositivos. Cuando SupportAssist determina que una pieza debe enviarse proactivamente, Dell utiliza la información de contacto existente que se almacenó de forma segura (mediante encriptación, políticas de retención, etc.) en los servidores de Dell Technologies.

La siguiente información del sistema se recolecta y envía una vez cada 24 horas como parte del monitoreo de rutina del sistema:

- **Versión del esquema:** es la versión del esquema utilizado para el monitoreo de rutina del sistema.
- **Versión del agente:** es la versión de SupportAssist implementada en el sistema.
- **Etiqueta de servicio:** es el identificador único del sistema.
- **Modelo del sistema:** nombre del modelo del sistema
- **Información de registro:** es el estado de registro de SupportAssist.
- **Versión de OS:** versión del sistema operativo que se ejecuta en el dispositivo
- **Versión de SP:** Service Pack del sistema operativo
- **Fecha UTC:** es la fecha y hora en la que se envió la información de monitoreo del sistema de rutina a Dell Technologies Services.
- **Versión del BIOS:** versión del BIOS instalado en el sistema
- **Estado:** estado de la alerta según la gravedad, por ejemplo, advertencia
- **Descripción:** información sobre la falla del sistema, por ejemplo, uso elevado de la CPU
- **Espacio libre en el disco duro:** espacio libre disponible en el disco duro del sistema
- **Uso de la memoria:** es la cantidad de memoria del sistema utilizada.
- **Uso de CPU:** es la cantidad de CPU utilizada.
- **Fecha local:** es la fecha y hora del sistema.
- **Fecha del último reinicio:** fecha y hora en que el sistema se reinició por última vez
- **Fecha en la que se ejecutó la actualización de Windows:** es la fecha y hora en la que se actualizó Windows por última vez en el sistema.
- **Conteo de BSOD en 24 horas:** cantidad de instancias de pantalla azul en las últimas 24 horas
- **Información de alerta:** identificador único de la alerta

Para obtener más información sobre los datos de monitoreo del sistema recopilados de un sistema activo, visite nuestra página Dell.com aquí.

Toda la información se transmite a través de canales seguros.

¿Cómo se protegen los scripts de corrección?

Antes de cargarse a la plataforma de corrección, todos los scripts de corrección creados por Dell se firman con certificados de Dell y se someten a pruebas y validación exhaustivas para garantizar que funcionen según lo previsto sin producir resultados inesperados. Esto sirve como base para verificar la autenticidad del script antes de la ejecución. Por ejemplo, si se modifica o reemplaza un script en el terminal, la validación de la firma del certificado fallará y SupportAssist bloqueará la ejecución del script. Esto evita la ejecución de código no autorizado o potencialmente dañino. Estos scripts no pueden ser modificados por nadie fuera de Dell, lo que garantiza su integridad. Se recomienda probar scripts en un grupo designado de PC antes de una implementación más amplia.

Se sigue un proceso diferente para los scripts de flujo de trabajo personalizados. Cuando los clientes cargan sus propios scripts, el sistema de corrección acepta scripts sin firmar y scripts firmados con un certificado del cliente. La integridad de estos scripts se conserva mientras se encuentran en tránsito a las PC y cuando se almacenan en reposo. Se recomienda probar scripts personalizados en un grupo específico de PC antes de una implementación más amplia.

TechDirect Connect and Manage admite la creación de sitios y grupos, lo que permite a los clientes validar scripts personalizados y creados por Dell en máquinas de prueba. Toda la información de la consola de corrección está protegida dentro de los límites del grupo de usuarios en TechDirect, accesible solo para los usuarios con funciones adecuadas asignadas por el administrador del grupo de usuarios. Los resultados también se pueden exportar a un archivo CSV para su análisis posterior.

¿Cómo almacena y transporta SupportAssist los datos de manera segura?

Los datos que se envían de SupportAssist a Dell Technologies Services se cifran con cifrado de 256 bits y se transfieren de manera segura con el protocolo de seguridad de capa de transporte (TLS).

Se genera una clave de cifrado durante la ejecución en cada máquina mientras se instala el paquete. La clave de cifrado se utiliza junto con la sal para cifrar la información instalada. Se utiliza un algoritmo estándar de la industria para cifrar los datos en reposo.

En criptografía, la sal son datos aleatorios que se utilizan como entrada para una función unidireccional que transforma los datos, una contraseña o una frase de contraseña en valores hash. La función principal de las sales es defenderse de los ataques de diccionario o de su equivalente en valores hash, un ataque de tabla arcoíris previamente calculada.

Todas las claves de cifrado se generan mediante generadores de números aleatorios seguros. Los datos en tránsito se protegen mediante TLS a través de HTTPS (Hypertext Transfer Protocol Secure). Todos los algoritmos de cifrado son estándares de la industria y los datos en reposo están cifrados.

HTTPS se utiliza en las comunicaciones externas para las transmisiones de comentarios proporcionados por el usuario, eventos de telemetría de diagnóstico y la consulta de una API en Dell.com o Microsoft Azure IoT Hub con el fin de obtener información del sistema que se utiliza en el proceso de restauración. Se utiliza un MQTT seguro para el enfoque de pub-sub.

El protocolo HTTPS estándar se utiliza para proteger la comunicación entre el cliente y la infraestructura de back-end cuando se transmite contenido al dispositivo del usuario final o se descarga de este. HTTPS o MQTT seguro se utiliza para proteger la transmisión de datos de telemetría, la comunicación con una API de back-end en Dell.com o Microsoft Azure IoT Hub, y la descarga de contenido recuperado de Dell.com.

Todos los componentes de red se encuentran protegidos por un firewall y un equipo de seguridad de red se encarga de administrarlos. El tráfico de red se controla estrictamente. Todo el tráfico entrante se transmite a través de puertos específicos y solo se envía a las direcciones de red de destino adecuadas. SupportAssist utiliza el ancho de banda de red para diversos eventos que requieren conectividad con la infraestructura de Dell Technologies Services. El ancho de banda utilizado puede variar según la cantidad de sistemas de destino que monitorea SupportAssist. Consulte el documento Datos recopilados de PC conectadas para obtener más información sobre el consumo promedio de datos.

¿Qué hace SupportAssist con los datos?

SupportAssist utiliza los datos recopilados para brindar soporte automatizado, proactivo y predictivo a los clientes. Si hay problemas con un sistema, SupportAssist generará una alerta para que un agente de soporte técnico lo solucione.

SupportAssist también utiliza los datos recopilados para predecir cuándo un componente está a punto de fallar mediante el uso de software de inteligencia artificial basado en datos recopilados de decenas de millones de sistemas Dell en el campo. Esta alerta predictiva se puede utilizar para enviar una pieza antes de que falle, lo que da como resultado un nivel optimo de tiempo de actividad y protección de datos.

Por último, SupportAssist utiliza los datos para detectar y eliminar virus y malware de los sistemas de los usuarios, optimizar el rendimiento del sistema operativo y brindar recomendaciones sobre actualizaciones de BIOS, controladores y firmware.

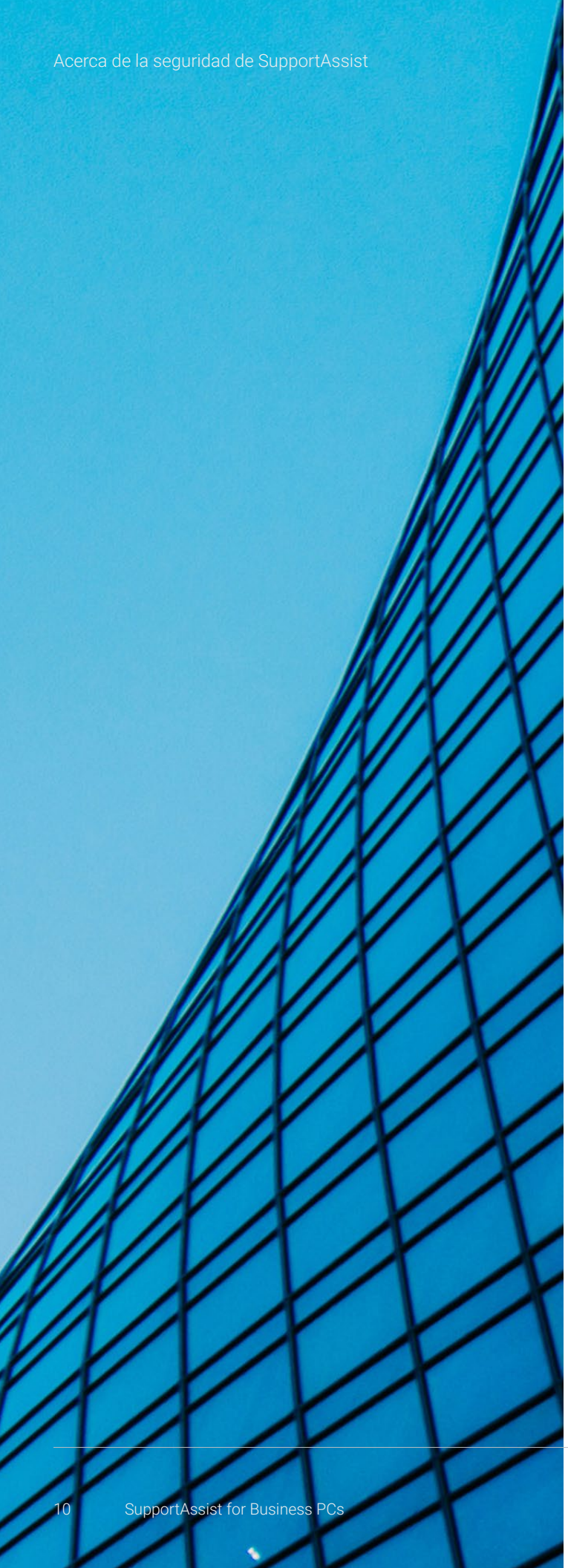
El uso de aplicaciones del sistema proporciona información valiosa sobre el uso del sistema con el componente de información valiosa.

Seguridad física

Dell Technologies Services aloja los datos de SupportAssist, que incluyen los componentes de seguridad, redes, sistemas y aplicaciones, en un centro de datos en Estados Unidos diseñado para mantener altos niveles de disponibilidad y seguridad. Los datos de SupportAssist están protegidos mediante una amplia variedad de medidas.

El acceso a los centros de datos donde reside la infraestructura está restringido al personal autorizado. El acceso se controla con tarjetas inteligentes.

Las medidas de seguridad físicas y lógicas garantizan la seguridad de los datos almacenados.



Seguridad lógica

Los datos que genera SupportAssist se almacenan en 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.) se encuentra restringido a través de herramientas internas que se auditan y evalúan según las pautas de Dell Digital (TI).

- **Auditoría:** se mantienen registros de dispositivos monitoreados, a los que solo la infraestructura o las aplicaciones de Dell Technologies Services pueden acceder. Estos registros recopilan todos los intentos de inicio sesión o acceso al sistema operativo o a la consola del servidor web de SupportAssist.

Las compilaciones administradas por TI se refuerzan mediante los controles recomendados por las prácticas recomendadas de seguridad del Centro para la seguridad de Internet (CIS).

Por último, el ecosistema de SupportAssist emplea alta disponibilidad local dentro de su centro de datos e infraestructura idéntica en un centro de datos independiente. Las únicas excepciones son las tecnologías que son intrínsecamente de alta disponibilidad, como los clústeres de big data y las nubes privadas.

Para la analítica de datos, Dell Technologies Services aprovecha los entornos de nube que controlamos y administramos por completo, incluidas las nubes privadas, híbridas y públicas. Las bases de datos relacionales, los servicios de almacenamiento simples y los almacenes de datos están cifrados y utilizan privilegios mínimos. Ninguna base de datos relacional está orientada al público. Los almacenes de datos están protegidos mediante HTTPS.

¿Cuáles son las políticas y prácticas de seguridad de Dell Technologies?

Desarrollo

Nuestro estándar interno de Secure Development Lifecycle (SDL) sirve como referencia fundamental para las organizaciones de productos de Dell Technologies, ya que proporciona parámetros de referencia esenciales para el desarrollo seguro de productos y aplicaciones. Dell proporciona un catálogo de control de SDL definido basado en ISO/IEC 27034 y un estándar basado en la infraestructura de desarrollo de software seguro (SSDF) de NIST. Estas herramientas ayudan a los equipos de Dell a crear productos seguros para los clientes y a evitar que se introduzcan vulnerabilidades y debilidades de seguridad en el software y el hardware compatible con Dell o desarrollado por este. Los equipos de ingeniería deben adoptar estos controles durante el desarrollo de nuevas características y funcionalidades. Estos controles abarcan actividades de análisis, así como medidas proactivas y prescriptivas centradas en áreas de riesgo clave.

Las actividades de análisis, incluido el modelado de amenazas, el análisis de código estático, el escaneo y las pruebas de seguridad, son componentes integrales destinados a identificar y mitigar los fallos de seguridad durante todo el ciclo de vida útil del desarrollo. Además, SDL incluye controles prescriptivos para ayudar a garantizar que los equipos de desarrollo aborden proactivamente problemas de seguridad específicos, incluidos los descritos en los estándares de la industria, como Open Web Application Security Project (OWASP) Top 10 y SANS Top 25.

SupportAssist for Business PCs se alinea con esta sólida infraestructura de SDL y emplea el modelo de madurez de SDL de Dell para implementar controles de seguridad de acuerdo con los estándares de la industria. El programa DevSecOps protege los procesos modernos de desarrollo e implementación de software de Dell mediante la automatización de los controles de SDL y la aplicación de políticas de seguridad en un entorno de integración continua e implementación continua (CI/CD). Estas herramientas de CI/CD automatizan los procesos de compilación, prueba e implementación, lo que garantiza que los cambios de código se integren y prueben continuamente como parte del flujo de trabajo de desarrollo.

Los ingenieros de SDL realizan evaluaciones de seguridad de SDL para identificar problemas y vulnerabilidades de seguridad en el software y proporcionan recomendaciones a los equipos de desarrollo para corregir estos hallazgos de seguridad. Esta garantía proporciona visibilidad de la madurez de nuestras prácticas de seguridad y la postura de seguridad de nuestro software y hardware.

Esta evaluación incluye lo siguiente:

- Evaluación de vulnerabilidades mediante pruebas de penetración.
- Pruebas de seguridad de otros fabricantes realizadas por proveedores respetados como SecureWorks.
- Evaluación de las soluciones de administración de identidad, autenticación y autorización.
- Escaneo exhaustivo de todas las bibliotecas y componentes de otros fabricantes mediante herramientas de análisis de composición de software líderes en la industria.
- Comunicación de asesorías de seguridad de Dell para mejoras de seguridad específicas.
- Clasificación rigurosa de datos en colaboración con nuestra organización de seguridad global, que alinea los esfuerzos de privacidad y seguridad para proteger los datos electrónicos.
- Someter las aplicaciones a auditorías de seguridad y procedimientos de gobierno corporativo.

Reglamento General de Protección de Datos (RGPD)

Dell ha implementado medidas diseñadas para garantizar que tengamos los procesos y procedimientos necesarios para cumplir con nuestras obligaciones en virtud del RGPD. Dell rastrea los desarrollos en las leyes de privacidad en todo el mundo y garantiza el cumplimiento de sus obligaciones aplicables en virtud de la legislación de privacidad pertinente. En los casos donde Dell actúa como un procesador, lo hace según un formulario de mutuo acuerdo o un formulario de acuerdo de procesamiento de datos estándar. Para obtener más información, visite los siguientes enlaces:

- Resumen de los controles y la declaración corporativa de seguridad de la información del RGPD de Dell
- El compromiso de Dell con el cumplimiento del RGPD
- Preguntas frecuentes sobre el cumplimiento de Dell para los clientes de Dell Technologies

Los procesos seguros y las prácticas comprobadas de la industria garantizan la seguridad de SupportAssist.

Prueba de validación de seguridad

Con regularidad, se llevan a cabo evaluaciones de seguridad de otros fabricantes en la aplicación de SupportAssist y su infraestructura de soporte.

Las evaluaciones de aplicaciones incluyen el transporte de datos y la seguridad de la API, el análisis de código fuente estático y dinámico, las evaluaciones cruzadas del Proyecto abierto de seguridad de aplicaciones web (OWASP) y las bibliotecas de otros fabricantes.

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

Administración de cambios

El proceso de administración de cambios de Dell Technologies sigue las prácticas recomendadas de ITIL Foundation, según lo dictado por la junta corporativa de administración de cambios. Todos los cambios se administran mediante vales de solicitud de cambios. Aquellos que accedan al sistema para iniciar cambios deben recibir la capacitación de ITIL, así como familiarizarse con SDL. Todas las actualizaciones y mejoras aplicadas a la infraestructura de back-end se someten a un control de versión para garantizar un seguimiento y una trazabilidad adecuados. El equipo emplea un proceso de compilación automatizado para aplicar nuevas compilaciones o revocar cualquier compilación o corrección que se haya implementado.

Cada versión publicada en Dell.com/support contiene información sobre los cambios introducidos con limitaciones conocidas.

Nuestro equipo de administración de productos prepara todos los cambios y las características nuevas, que se priorizan mediante un proceso de administración de cambios y plan de registro.

Autenticación

SupportAssist utiliza MyAccount de Dell para la autenticación de la infraestructura de Dell Technologies Services, la clave simétrica aleatoria de la aplicación, JWT y los grupos de inicio de sesión del sistema operativo para garantizar una autenticación inmediata.

A los grupos, como el equipo de administración de bases de datos y el equipo de soporte operativo, que tienen acceso a los componentes de SupportAssist, se les asignan deberes y derechos de acceso separados. Todas las actualizaciones realizadas en el entorno de producción atraviesan un proceso de control de cambios definido que incorpora verificaciones.

Comunidad consciente de la seguridad

Dell ofrece un plan de estudios de capacitación en seguridad basada en funciones para enseñarles a los empleados nuevos y actuales las prácticas recomendadas de seguridad específicas del trabajo y a utilizar los recursos pertinentes. Dell Technologies se esfuerza por crear una cultura consciente de la seguridad en toda su comunidad. Además, la comunidad de desarrolladores forma parte del programa Security Champion de Dell, diseñado para fomentar la seguridad en una etapa temprana de la producción en las prácticas de desarrollo de software.

Generación de informes de incidentes

En Dell Technologies, todos deben informar oportunamente cualquier actividad sospechosa, problema de ciberseguridad o amenaza a nuestro Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) por correo electrónico a security@dell.com.

Respuesta ante vulnerabilidades

Dell Technologies se compromete a minimizar los riesgos asociados con las vulnerabilidades de seguridad de los productos, las aplicaciones y los servicios de nube. Para lograr prácticas oportunas de respuesta ante vulnerabilidades, Dell sigue las pautas descritas en el Estándar de Respuesta ante Vulnerabilidades (VRT) de Dell Technologies. Dell participa activamente en varias iniciativas de la comunidad, como el Foro de Equipos de Respuesta ante Incidentes y Respuesta (FIRST) y el Foro de Garantía de Software para la Excelencia en el Código (SAFECode). Los procesos y procedimientos de Dell se alinean con la Infraestructura de Servicios FIRST PSIRT, así como con otros estándares, incluidos ISO/IEC 29147:2018 e ISO/IEC 30111:2019.

Dell Technologies se esfuerza por abordar las vulnerabilidades de los productos, las aplicaciones y los servicios de nube en el menor tiempo comercialmente razonable. Los plazos exactos pueden variar según la vulnerabilidad específica y su impacto, como la complejidad del esfuerzo/impacto de la vulnerabilidad para corregirla. El Equipo de Respuesta ante Incidentes de Seguridad de Productos (PSIRT) coordina la respuesta y la divulgación de todas las vulnerabilidades de productos que se nos informan. Todas las divulgaciones de vulnerabilidades de productos de Dell Technologies están disponibles en línea en la página Asesorías, avisos y recursos de seguridad de Dell. Para obtener más detalles sobre las prácticas de respuesta ante vulnerabilidades de Dell, consulte la Política de respuesta ante vulnerabilidades de Dell.

Asociaciones de la industria

Dell Technologies participa en varios grupos de toda la industria para colaborar con otros proveedores líderes para definir, desarrollar y compartir las prácticas recomendadas en seguridad de los productos, y para mejorar aún más el desarrollo seguro. Algunos ejemplos de colaboración en la industria incluyen:

- Dell Technologies, cofundó y actualmente preside la junta directiva del Foro de garantía de software para la excelencia en el código (SAFECode). Otros miembros de la junta incluyen representantes de Microsoft, Adobe, SAP, Intel, Siemens, CA y Symantec. Los miembros de SAFECode comparten y publican prácticas y capacitaciones sobre garantía de software.

Un líder de la industria en la definición de las prácticas recomendadas de seguridad de los productos y la mejora del desarrollo seguro.

Asociaciones de la industria (continuación)

- Dell Technologies es miembro activo del Foro de Equipos de Respuesta ante Incidentes y Seguridad (FIRST). FIRST es una organización de primer nivel y un líder mundial reconocido en respuesta ante incidentes y vulnerabilidades.
- Dell participa activamente en el foro Open Group Trusted Technology Forum (OTTF). OTTF lidera el desarrollo de un programa y una infraestructura de integridad de la cadena de suministro global.
- Algunos empleados de Dell fueron miembros fundadores del Centro de diseño seguro del IEEE, que se lanzó bajo la iniciativa de ciberseguridad del IEEE con el fin de ayudar a los arquitectos de software a comprender y abordar las fallas de diseño de seguridad frecuentes.

Estándares de seguridad de la industria

- Los empleados de Dell participan activamente en los organismos de estándares y en los consorcios de la industria, que se centran en el desarrollo de estándares de seguridad y en la definición de prácticas de seguridad para toda la industria, que incluyen:
- Cloud Security Alliance (CSA)
- Foro de equipos de respuesta ante incidentes y seguridad (FIRST)
- The Open Group
- Foro de garantía de software para la excelencia en el código (SAFECode)
- Asociación de la industria de redes de almacenamiento (SNIA)

Dell Technologies cuenta con la certificación ISO 9001. Dell lleva a cabo auditorías trimestrales periódicas y revisiones de cumplimiento para todos sus centros de desarrollo y fabricación.

V. Conclusión

La tecnología de conectividad SupportAssist ofrece funcionalidades inteligentes de automatización y corrección para permitir el máximo tiempo de actividad para el equipamiento de computadoras de escritorio y laptops Dell de una organización. Dell Technologies Services puede proporcionar esta tecnología de vanguardia con una seguridad óptima centrándose en procesos seguros, transmisión segura de datos y almacenamiento seguro de datos.

Si tiene preguntas y desea obtener más información, visite **Dell.com/SupportAssist**

[1] Para conocer los requisitos y los sistemas compatibles, consulte nuestra Guía del usuario (versión de SupportAssist for Home PCs para uso personal) o la Guía del administrador (versión de SupportAssist for Business PCs para la administración de equipamientos de PC) y haga clic en "PC compatibles". Las funcionalidades proactivas y predictivas dependen del plan de servicio activo y de las reglas comerciales de Dell Technologies. Para conocer las funcionalidades de ProSupport Suite for PCs, consulte nuestra Guía del administrador y haga clic en "Funcionalidades de conexión y administración y planes de servicio de Dell". Para conocer las funcionalidades de Dell Care Suite, Premium Support Suite o Alienware Care Suite for PCs, consulte la Guía del usuario y haga clic en "Funcionalidades de SupportAssist y planes de servicio de Dell".

[2] Información basada en un análisis de Dell realizado en diciembre de 2023.