

Anexo de medidas de seguridad de la información de Dell APEX

Los Servicios Dell APEX utilizan un modelo de responsabilidad de seguridad compartida en el que tanto Usted como Dell tienen una serie de responsabilidades, ya que están alojados en Sus instalaciones o en un Centro de Housing y, por lo general, no implican el alojamiento de Contenidos de Cliente en servidores ubicados en centros de datos gestionados por Dell. Sus responsabilidades se describen en la Descripción de la Oferta del Servicio correspondiente.

Dell ha implementado y mantendrá las siguientes medidas de seguridad corporativas para los Servicios Dell APEX. Estas medidas, junto con las medidas de seguridad descritas en la Descripción de la Oferta del Servicio, constituyen la única responsabilidad de Dell con respecto a la seguridad de los Servicios Dell APEX. A menos que se defina lo contrario en el presente documento, todos los términos en mayúscula que se utilizan en este documento tendrán el significado que se les ha adscrito en el Contrato Dell APEX.

Descripción	Medidas
<p>Programa de seguridad de la información</p>	<p>Dell ha implementado y mantendrá un programa de seguridad de la información (incluyendo la adopción de políticas y normas internas) diseñado para:</p> <ul style="list-style-type: none"> (a) Identificar los riesgos de seguridad razonablemente previsibles para las partes, en su caso, de los centros de datos corporativos de Dell, servidores, equipos de red, cortafuegos y sistemas de software host que se utilizan para prestar los Servicios Dell APEX ("Red de Dell"). (b) Realizar esfuerzos comercialmente razonables para mitigar los riesgos de seguridad identificados en la Red de Dell, de la forma y manera que Dell considere adecuada, incluso mediante evaluaciones y pruebas de riesgo periódicas. <p>Dell ha designado a uno o más responsables de seguridad para coordinar, supervisar y hacer cumplir el programa de seguridad de la información.</p> <p>Dell mantendrá un programa de gestión de amenazas y vulnerabilidades que supervise las vulnerabilidades de la Red de Dell de forma continua. Las vulnerabilidades se identifican mediante una serie de fuentes/métodos que pueden incluir proveedores, investigadores de seguridad, análisis de vulnerabilidades, ejercicios de simulación de ataques, o Red Team , pruebas de penetración y reportes de empleados. Las vulnerabilidades de terceras partes que hayan sido dadas a conocer públicamente son revisadas para determinar la aplicabilidad de las mismas al entorno de Dell. Los análisis y las evaluaciones de vulnerabilidades se realizan de forma rutinaria y periódica en la infraestructura de aplicaciones de Dell. Estos procesos se han concebido para permitir la identificación proactiva y la corrección de vulnerabilidades, así como para respaldar el cumplimiento de los requisitos corporativos y normativos de Dell.</p>
<p>Ciclo de vida de desarrollo seguro y respuesta a vulnerabilidades</p>	<p>Dell ha implementado y mantiene un programa de ciclo de vida de desarrollo seguro para definir los pasos que se deben seguir para asegurar que sus ofertas se han evaluado, desarrollado y empaquetado adecuadamente bajo la estructura de un programa de gobernanza formal con un ciclo de vida de desarrollo seguro definido. Este programa, junto con el programa de seguridad de la información de Dell, ayuda a abordar la seguridad en todo el ciclo de vida de desarrollo y mantenimiento del Sistema Dell APEX. Dell utiliza un proceso riguroso para evaluar y mejorar continuamente sus prácticas de desarrollo</p>

	<p>seguro y respuesta a vulnerabilidades, y Dell las compara periódicamente con las prácticas estándar del sector.</p> <p>Tras investigar y validar una vulnerabilidad notificada en el Sistema Dell APEX, Dell intentará identificar, desarrollar y habilitar una solución adecuada de acuerdo con la política de respuesta ante vulnerabilidades publicada por Dell, que actualmente se encuentra en https://www.dell.com/support/contents/article/product-support/self-support-knowledgebase/security-antivirus/alerts-vulnerabilities/dell-vulnerability-response-policy.</p> <p>Dell comunica las soluciones a sus Clientes a través de avisos de seguridad cuando procede. Dell hace todo lo posible por proporcionar soluciones en un plazo comercialmente razonable, cuando procede. Los plazos de respuesta dependerán de muchos factores, como la gravedad, la complejidad de la solución o el componente afectado.</p>
<p>Administración de activos</p>	<p>Dell rastrea y gestiona los activos físicos y lógicos de la Red de Dell. Entre los ejemplos de los activos que Dell puede rastrear, y los controles que puede aplicar, se incluyen:</p> <ul style="list-style-type: none"> (a) Activos de software, como aplicaciones y programas de software del sistema. (b) Activos físicos, como servidores, equipos portátiles o de escritorio, cintas de archivado o copia de seguridad, impresoras y equipos de comunicaciones. (c) Activos de información, como bases de datos, planes de recuperación ante desastres, planes de continuidad empresarial, clasificación de datos o información archivada. <p>Dell clasifica los activos en función de la criticidad empresarial y/o la sensibilidad de la clasificación de datos. Dicha clasificación permite restringir adecuadamente el acceso a dicho activo.</p>
<p>Seguridad en Recursos Humanos</p>	<p>Como parte del proceso de contratación, los empleados de Dell deben firmar un acuerdo de confidencialidad en el momento de la contratación y someterse a un proceso de verificación sujeto a la legislación aplicable. Aunque Dell se reserva el derecho de revisar sus políticas e implementar las medidas que considere necesarias para velar por la seguridad en cuanto a los recursos humanos, bajo la política actual y sujeto a la legislación local y disponibilidad, Dell lleva a cabo una o más de las siguientes revisiones para contratar a un nuevo empleado: pruebas toxicológicas, verificación de la información relacionada con la seguridad social, búsqueda de antecedentes penales, verificación de educación y empleo, y verificación de elegibilidad laboral. Dell intenta cumplir con los estándares actuales del sector para empresas similares del mismo sector, pero Dell no puede adaptar la seguridad de su personal ni el proceso de selección para cumplir con las expectativas específicas de un Cliente en particular.</p> <p>Los terceros o contratistas externos son, o bien verificados por Dell como condición del contrato respectivo, o bien verificados por el contratista siguiendo un proceso de verificación aprobado por Dell.</p>

	<p>Dell mantiene un proceso disciplinario para tomar medidas frente el personal que no cumpla con los requisitos de su programa de seguridad de la información, incluidos, entre otros, los establecidos para cumplir con sus compromisos y requisitos de seguridad, disponibilidad y confidencialidad.</p> <p>Dell proporciona entrenamientos anuales de concienciación sobre seguridad a todo el personal aplicable y exige a los subcontratistas aplicables que impartan dicho entrenamiento a su personal.</p>
Seguridad física	<p>Dell dispone de políticas y controles que tienen como objetivo evitar la entrada no autorizada a las instalaciones y restringen el acceso físico a las instalaciones, donde se encuentran los componentes físicos de la Red de Dell, al personal autorizado.</p> <p>Existen controles basados en riesgos en las instalaciones que albergan componentes físicos de la Red de Dell (por ejemplo, centros de datos). Entre los controles de acceso pueden figurar guardias de seguridad, registros de seguridad, vigilancia, alarmas, acceso limitado a zonas seguras, protección de las vías de acceso, videovigilancia, tarjetas llave o autenticación de dos factores.</p> <p>Esta disposición se aplica a los Centros de Housing gestionados por Dell.</p>
Seguridad de la red	<p>Dell puede acceder electrónicamente a la Red de Dell según sea necesario para prestar los Servicios Dell APEX. Dell mantendrá políticas y controles de acceso para gestionar el acceso permitido a la Red de Dell desde cada conexión, incluido el uso de cortafuegos y controles de autenticación.</p> <p>Dell protege contra el uso malicioso de activos y software malicioso en la Red de Dell, a través de la implementación de controles basados en el riesgo. Esos controles pueden ser, entre otros: políticas de seguridad; controles de acceso restrictivos; entornos para desarrollo y pruebas separados; detección de malware en servidores, equipos de escritorio y equipos portátiles; análisis de archivos adjuntos de correo electrónico en busca de malware; análisis de cumplimiento normativo del sistema; monitorización para impedir intrusiones y respuesta a estas; registro de eventos sospechosos clave y envío de alertas al respecto; procedimientos de manejo de la información según el tipo de datos, aplicación de comercio electrónico y seguridad de la red; uso de activos externos y análisis del sistema y las aplicaciones en busca de vulnerabilidades.</p> <p>Dell exige el cifrado de los datos en tránsito y en reposo cuando sea necesario y de conformidad con su programa de seguridad de la información. Dell utiliza cifrado y protocolos adecuados (por ejemplo, TLS) cuando accede de forma remota al sistema de un cliente a través de redes abiertas. Dell almacena sus claves de cifrado, cuando no están en uso, en soluciones aprobadas diseñadas para proporcionar prácticas de gestión de claves aceptadas por el sector.</p>
Controles de acceso	<p>Dell implementa controles de acceso adecuados diseñados para proteger contra el acceso no autorizado a la Red de Dell. Para reducir el riesgo de uso indebido, intencionado o no, el acceso se controla según los principios de "mínimo privilegio" y "necesidad de saber". Dell puede utilizar diversos controles de acceso, tales como revisiones de acceso, mantenimiento de cuentas de servicio y acceso privilegiado a las aplicaciones, configuraciones a</p>

	<p>nivel de sistema para el acceso y la generación de informes relacionados con el acceso.</p> <p>Dell utiliza prácticas estándar del sector, incluida, cuando procede, la autenticación de dos factores, para identificar y autenticar a los usuarios de la Red de Dell. Dell exige el uso de contraseñas seguras en toda la Red de Dell. Dell (a) prohíbe a los usuarios de la Red de Dell compartir, escribir, enviar por correo electrónico, enviar por mensajería instantánea o almacenar contraseñas sin cifrar en cualquier sistema; y (b) bloquea las cuentas tras una serie de intentos fallidos de introducir la contraseña.</p> <p>Dell utiliza prácticas estándar del sector para mejorar los controles de acceso, incluyendo:</p> <ul style="list-style-type: none"> (a) La desconexión automática de las sesiones de usuario en caso de inactividad. (b) El requisito de introducir la identificación y la contraseña para volver a acceder. (c) La protección contra el acceso externo mediante uno o varios firewalls aceptados por el sector cuya conexión a Internet, en su caso, esté salvaguardada por una conexión VPN. (d) El enmascaramiento de las contraseñas cuando se muestran o se introducen, según proceda. (e) Un cifrado de contraseñas adecuado y estándar del sector cuando se transmiten.
<p>Administración de incidentes</p>	<p>Dell utiliza un marco de respuesta a incidentes para preparar, responder, gestionar y minimizar los efectos de los eventos de seguridad. El marco incluye procedimientos que deben seguirse en caso de incidente de seguridad, entre ellos:</p> <ul style="list-style-type: none"> (a) Un equipo interno de respuesta a incidentes con un jefe de respuesta. (b) Un equipo de investigación que realice un análisis de causa raíz e identifique a las partes afectadas. (c) Procesos internos de información y notificación. (d) Un proceso de documentación de las medidas de respuesta y los planes de corrección. (e) Una revisión de los acontecimientos tras el incidente.
<p>Gestión de la continuidad empresarial</p>	<p>Dell cuenta con planes de continuidad empresarial ("BCP"), por sus siglas en inglés) para recuperarse de una interrupción empresarial y reanudar las operaciones empresariales normales tan pronto como sea razonablemente posible. Dell hará intentos razonables y oportunos, según las circunstancias, para ponerse en contacto con Usted en caso de una interrupción de la actividad empresarial que afecte materialmente a Sus Servicios Dell APEX.</p>