Contrato de Ofertas de Servicios en la Nube

Anexo de Medidas de Seguridad de la Información

Dell ha implementado y mantendrá las siguientes medidas de seguridad corporativas. Estas medidas, que deben tomarse junto con las medidas de seguridad descritas en la correspondiente Descripción de la oferta del servicio, constituyen la única responsabilidad de Dell con respecto a la seguridad de la Oferta del servicio. A menos que se defina lo contrario en el presente documento, todos los términos con inicial en mayúscula que aparezcan en este documento tendrán el significado que se les ha atribuido en el Contrato de ofertas de servicios en la nube.

Descripción	Medidas
Programa de seguridad de la información	Dell ha implementado y mantendrá un programa de seguridad de la información (que incluye la adopción de políticas y normas internas) diseñado para: (a) identificar los riesgos de seguridad razonablemente previsibles relativos a los componentes de los centros de datos corporativos de Dell, en su caso, así como a sus servidores, equipos de red, cortafuegos y sistemas de software host que se encuentran bajo el control exclusivo de Dell y que se utilizan para prestar la Oferta del servicio ("**Red de Dell**"); y (b) mitigar los riesgos de seguridad identificados, cuando lo estime oportuno, incluso mediante evaluaciones y pruebas de riesgos periódicas. Dell ha designado a uno o más responsables de seguridad para coordinar, supervisar y hacer cumplir el programa de seguridad de la información. Dell mantendrá un programa de gestión de amenazas y vulnerabilidades a fin de supervisar las vulnerabilidades de la Red de Dell de forma continua. Las vulnerabilidades se identifican mediante una serie de fuentes o métodos, entre los que se incluyen proveedores, investigadores de seguridad, análisis de vulnerabilidades, ejercicios de simulación de ataques, o Red Team, pruebas de penetración e informes de empleados. Las vulnerabilidades de terceras partes que hayan sido dadas a conocer públicamente son revisadas para determinada 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 normativo y los requisitos normativos de Dell.
Ciclo de vida de desarrollo seguro y respuesta a vulnerabilidades	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 definido ciclo de vida de desarrollo seguro. 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 de la Oferta del servicio. Dell sigue un riguroso proceso para evaluar y mejorar continuamente sus prácticas de desarrollo

	seguro y respuesta a vulnerabilidades; asimismo, las compara periódicamente con las prácticas estándar del sector. Tras investigar y validar una vulnerabilidad notificada en la Oferta del servicio, 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: Política de respuesta ante vulnerabilidades de Dell | Dell España 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.
Administración de activos	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 controles que puede aplicar se incluyen: (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 comunicación; y (c) activos de información, como bases de datos, planes de recuperación ante desastres, planes de continuidad empresarial, clasificación de datos o información archivada. Dell clasifica los activos en función de la criticidad empresarial o de la sensibilidad de la clasificación de datos. Dicha clasificación permite restringir adecuadamente el acceso a un activo.
Seguridad relativa a los Recursos Humanos	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 la seguridad del personal a su entera discreción, en virtud de la política actual y de conformidad con la legislación y disponibilidad locales, 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 Seguridad Social, verificación de antecedentes penales, verificación de formación académica y empleo, además de una verificación de idoneidad para ser contratado. Dell intenta cumplir los estándares actuales del sector para empresas similares del mismo sector, pero no puede adaptar la seguridad de su personal ni su proceso de selección para cumplir las expectativas específicas de un Cliente en particular. Los terceros o contratistas externos son, o bien verificados por Dell como condición del contrato respectivo, o bien verificados por el contratista a partir de un proceso de verificación aprobado por Dell. Dell dispone de un proceso disciplinario para tomar medidas frente al personal que no cumpla los requisitos de su programa de seguridad de la información, incluidos, entre otros, los establecidos para cumplir con sus compromisos y requisitos relativos a la seguridad, la disponibilidad y la confidencialidad.

	Dell imparte una formación anual de concienciación sobre seguridad a todo el personal aplicable y exige a los correspondientes subcontratistas que impartan dicha formación a su personal.
Seguridad física	Dell dispone de políticas y controles que tienen como objetivo limitar la entrada a las instalaciones donde se encuentran los componentes físicos de la Red de Dell al personal autorizado; estas políticas y controles tienen como objetivo evitar un acceso no autorizado. Se han implementado controles basados en riesgos en las instalaciones que alojan 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, medidas de vigilancia, alarmas, acceso limitado a zonas protegidas, protección de las vías de acceso, cámaras de videovigilancia, tarjetas llave o autenticación de dos factores. Esta disposición se aplica a los Centros de Housing gestionados por Dell.
Seguridad de la red	La Red de Dell se hará accesible de forma electrónica al personal de Dell en la medida en que sea necesario para prestar la Oferta del servicio. 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. Dell se 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 su 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. 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 protocolos de cifrado y otros protocolos adecuados (por ejemplo, TLS) cuando accede de forma remota al sistema de un cliente o cuando transmite información personal a través de redes abiertas. Cuando no están en uso, Dell almacena sus claves de cifrado en soluciones aprobadas que han sido diseñadas para proporcionar unas prácticas de gestión de claves aceptadas por el sector.
Controles de acceso	Dell implementa controles de acceso adecuados diseñados para protegerse contra el acceso no autorizado a la Red de Dell. Para reducir el riesgo de uso indebido, intencionado o de otro tipo de riesgos, el acceso se controla según los principios de "privilegios mínimos" 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 nivel de sistema para el acceso, así como generación de informes relacionados con el acceso.

	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, anotar, 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. Dell utiliza prácticas estándar del sector para mejorar los controles de acceso, incluyendo: (a) la desconexión automática de las sesiones de usuario en caso de inactividad; (b) el requisito de introducir el identificador y la contraseña para volver a acceder; (c) la protección contra el acceso externo mediante uno o varios cortafuegos aceptados por el sector cuya conexión a Internet, en su caso, esté protegida por una conexión VPN; (d) el enmascaramiento de contraseñas cuando se muestran o se introducen, según proceda; y (e) un cifrado de contraseñas adecuado y estándar del sector cuando se transmiten.
Gestión de incidentes	Dell utiliza un marco de respuesta ante 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: (a) un equipo interno de respuesta ante incidentes con un jefe de respuesta; (b) un equipo de investigación para realizar un análisis de causa origen e identificar 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; y (e) una revisión de los acontecimientos tras el incidente.
Gestión de la continuidad empresarial	Dell cuenta con planes de continuidad empresarial ("**BCP**", por sus siglas en inglés) para recuperarse de una interrupción de su actividad y reanudar las operaciones empresariales normales tan pronto como sea razonablemente posible. Según las circunstancias, Dell tomará las medidas razonables y oportunas para ponerse en contacto con Usted en caso de que la interrupción de su actividad empresarial afecte materialmente a los clientes de Dell.