

M

Microsoft Windows 2000 Professional se considera como el sistema operativo ideal para computadoras móviles y de escritorio, diseñado para sustituir a Windows 95 como el estándar de las empresas. Pues al agregarle el poder y la seguridad de Windows NT Workstation, así como la interfaz de Windows 98, se obtiene como resultado el más sencillo y eficiente sistema operativo de escritorio hasta ahora.

Las funciones mejoradas de Windows 2000 Professional, ayudan a los usuarios a aprovechar completamente sus capacidades. Este Windows constituye hasta ahora el más sencillo sistema operativo para configurar o trabajar en una computadora o navegar en Internet. Fue desarrollado con base en el poder de Windows NT Workstation, por lo que ofrece estándares de seguridad, confiabilidad industrial y un mejor desempeño. Proporciona las mejores características de Windows 98, para estar al día en apoyo móvil y asegurarle que podrá aprovechar la nueva generación de equipos y provee un escritorio más manejable y más sencillo de implementar, administrar y dar soporte, lo que traduce en una disminución del costo total de propiedad (TCO).

A continuación una visión detallada de las nuevas características y mejoras que nos trae el Windows 2000 Professional.

INSTALACIÓN MÁS FACIL

Una de las mejoras que se experimenta al utilizar Windows 2000 es que su sistema de instalación es más confiable y simplificado, soporta scripts de instalación que requieren una participación mínima. Los administradores pueden hacer un script completo del proceso de instalación, de manera que no se necesita contestar más preguntas que el nombre y contraseña; aun las instalaciones para las que no se ha preparado un script son más simples y más confiables. Su instalación es sumamente fácil. Además, Windows 2000 Professional cuenta con soporte para la creación de redes pequeñas.

A continuación detallamos varios ejemplos de lo que hace Windows 2000 Profesional durante una instalación sin script:

SIMPLIFICA EL PROCESO DE INSTALACION

Las pantallas y las preguntas que se presentan durante el proceso de instalación poseen un lenguaje sencillo y no técnico.

AUTOMATIZA MAS TAREAS

Windows 2000 Professional tiene más supuestos acerca de la manera en que se deberían instalar las computadoras. Además, proporciona detección de hardware y soporta Plug and Play, lo que automatiza la instalación y la configuración de los dispositivos de hardware.

HACE EL PROCESO DE INSTALACION MÁS CONFIABLE

Windows 2000 Professional rastrea los problemas durante la instalación, y en caso de que surja algún problema que no sea crítico (lo que no evitará que la computadora arranque), la instalación continuará. Cuando ésta se haya completado, el sistema operativo genera un reporte de registro de problemas, para que un administrador lo resuelva.

PARA CONECTARSE

Utilizar CTR+ALT+DEL antes de conectarse, es la manera más segura para que el usuario se conecte a Windows 2000 Professional; ayuda a proteger el sistema operativo de algún acceso no autorizado. Para conectarse, primero se ve una pantalla de conexión simplificada que oculta los nombres de dominio. No es frecuente que necesiten cambiar su dominio; por lo tanto, ocultar esta opción puede reducir los costos del escritorio de ayuda, al disminuir las posibilidades de que cambien el dominio en forma inadvertida.

CONFIGURACION DE REDES PEQUEÑAS

Con Windows 2000 Professional es posible configurar redes pequeñas al sólo conectar las computadoras configuradas con Windows 2000 Professional en un hub. La primera vez que Windows 2000 Professional inicia, se ajusta a una predeterminación que busca un servidor DHCP (Protocolos de configuración de host dinámico).

UN ESCRITORIO WINDOWS MÁS PODEROSO Y PERSONALIZABLE

Windows 2000 Professional introduce varias mejoras en el área de escritorio, ofrece más opciones para personalizar el escritorio e integrar la automatización, a fin de adaptarse a la manera en que uno interactúa con el sistema operativo. El menú personalizado reduce el desorden del escritorio, al adaptar dinámicamente el menú Inicio para así ofrecer un acceso inmediato a los recursos de la computadora que utiliza más a menudo.

PERSONALIZACION DEL ESCRITORIO

El escritorio de Windows 2000 Professional está más ordenado y es más fácil personalizar. Se pueden establecer más preferencias para adaptar la computadora a nuestras necesidades y el sistema operativo mismo tiene mejores capacidades de aprender los hábitos de una persona específica, para ayudarlo a completar las tareas de manera más rápida.

MENU PERSONALIZADOS

La función Menús personalizado de Windows 2000 Professional, monitorea en forma continua y resalta sólo los elementos del menú que se emplean más; para presentar otros elementos del menú, se utilizan las flechas dobles.

LISTAS UTILIZADAS CON MAYOR FRECUENCIA

La lista Usado con mayor frecuencia en Windows 2000 Professional rastrea dónde ha estado el usuario y mantiene una lista de estos recursos en el lugar adecuado. Las listas Usado con mayor frecuencia se mantienen en varios lugares a través de la interfaz Windows 2000 Professional, incluso en los Cuadros de diálogo Búsqueda y Abrir/Guardar.

AUTOCOMPLETAR

Windows 2000 Professional mejora de manera significativa la función autocompletar y amplía su uso a través del escritorio, no sólo para escribir URL. Primero, cuando Autocompletar reconoce una correspondencia, en lugar de escribir sobre una entrada, presenta una lista de opciones, y uno selecciona la opción correcta. Segundo, Autocompletar puede buscar para dar una lista de posibilidades. Windows 2000 Professional utiliza Autocompletar a través del sistema operativo, incluidos los cuadros de diálogo, Ejecución, Formas, Correlación de los controladores de red y Windows Explorer.

ACCESO MEJORADO A DOCUMENTOS Y RECURSOS

Windows 2000 Professional almacena todos los archivos en una ubicación central, la carpeta Mis

Documentos, para facilitar que éste encuentre y respalde información en su propia computadora. Además, cuenta con una mejor función de búsqueda y, debido a que soporta documentos basados en la red, facilita la localización de documentos y recursos que necesita y que no están almacenados en la propia computadora. Windows 2000 Professional puede trabajar con documentos basados en la red, aunque ésta no está trabajando de manera adecuada. El sistema operativo se puede configurar para sincronizar de modo automático los recursos cuando la red vuelve a estar en línea.

CARPETA MIS DOCUMENTOS

Esta Carpeta fue mejorada de manera significativa, ya que ahora tenemos una ubicación consistente para guardar y encontrar información. A menos que una aplicación se deba guardar explícitamente en una carpeta diferente, Windows 2000 Professional intercepta la ruta Guardar y la redirecciona a la carpeta Mis Documentos. El contenido de Mis Documentos se almacena en una base por usuarios; aunque éste comparta una computadora, no puede visualizar los documentos de otro.

ENCONTRAR INFORMACION Y RECURSOS

Windows 2000 Professional incluye varias mejoras que facilitarán encontrar la información; así, ubicar archivos y carpetas de manera local en la red corporativa, en intranet corporativo o en Internet es ahora más fácil y más rápido. Un botón de búsqueda más poderoso y consistente disponible en el menú de Inicio, en Mi PC y en el Explorador de Windows, facilita buscar la información en forma local y en Internet; y los lugares de la red visitados recientemente también son más fáciles de buscar. Además, Búsqueda contiene la funcionalidad Autocompletar que ayuda a encontrar elementos de trabajo cuyas direcciones o nombres de archivo son difíciles de recordar.

BUSQUEDA DE IMPRESORAS

Los usuarios de Windows 2000 Professional pueden buscar impresoras que tengan los atributos que necesiten, como tamaño de papel, impresión por los dos lados, resolución y color. También pueden crear propiedades de impresoras personalizadas.

BUSQUEDA EN INTERNET

En Windows 2000 Professional, el panel mejorado Búsqueda presenta opciones de búsqueda por temas, en lugar de por motor de búsqueda, como sitios Web, personas empresas o mapas. Se pueden personalizar los motores de búsqueda utilizados para cada una de las búsquedas por tema, incluso la adición de motores de búsqueda personalizados. Si no se está satisfecho con los resultados de una búsqueda, se puede redirigirla a otro motor de búsqueda, al hacer clic en el botón Siguiente en la ventana de Búsqueda.

TRABAJAR CUANDO LA RED ESTA INACTIVA

Cuando una persona hace clic en un documento o carpeta y después selecciona Hacer disponible fuera de línea, dicho documento o carpeta se almacena en la computadora de escritorio así como en el servidor de la red. El administrador de sincronización permite al usuario configurar el sistema para sincronizar elementos mientras éste está libre, cuando la persona se conecta o desconecta de la computadora.

OTRAS MEJORAS FUNDAMENTALES

Una de estas mejoras es el cuadro de diálogo Abrir/Guardar, con la que se encuentran documentos. Su barra de herramientas estilo Outlook incluye una lista de los documentos e historial utilizados con mayor frecuencia. Los que utilizan Windows 2000 Professional, pueden imprimir por Internet. Mediante el Protocolo de impresión por Internet (IPP) basado en estándares, las personas con conexiones a Internet pueden enviar

documentos a cualquier impresora conectada a Internet en un ambiente Windows 2000 Server.

CONFIABILIDAD Y SOPORTE MEJORADOS PARA CAMBIOS DE LA CONFIGURACION

Windows 2000 Professional soporta aplicaciones autorreparables, Plug and Play y manejo de potencia, que permiten instalar el hardware y las aplicaciones sin comprometer el sistema ni incurrir en pausas significativas. El soporte para Plug and Play, la administración de potencia y el bus serial universal (USB) facilitan trabajar con hardware. Un Panel de control mejorado organiza las herramientas de manera más lógica.

TRABAJAR CON APLICACIONES

El cuadro de diálogo Agregar/Eliminar Programas de Windows 2000 Professional proporciona mayor información acerca de las aplicaciones, como espacio de disco utilizado, versión, frecuencia de uso y si está disponible el soporte técnico en línea.

TRABAJAR CON HARDWARE

Windows 2000 Professional ha sido mejorado para trabajar con una mayor variedad de componentes hardware, y específicamente da soporte a Plug and Play, administración de energía, y bus serial universal (USB). USB es un tipo de bus que facilita aún más la instalación de diferentes tipos de periféricos compatibles, incluidos teclados, cámaras, escáner y otros dispositivos de imagen.

El asistente Agregar/Quitar Hardware ayuda a resolver problemas de hardware; así cuando Windows 2000 detecta un hardware nuevo, verifica las configuraciones para el dispositivo e instala el controlador correcto.

PANEL DE CONTROL REORGANIZADO

Este panel se ha reorganizado con el objeto de que resulte más fácil realizar las tareas de mantenimiento regulares y la resolución de problemas. De igual forma, estos cambios protegen también, contra cualquier cambio que pudiera provocar que los sistemas no trabajen de manera adecuada.

Algunos puntos fundamentales del Panel de Control incluyen:

Organización más lógica

Se puede ir directamente a configuraciones del Módem, seleccionar el separador Hardware y elegir Resolución de Problemas.

Sistema

Combina varios applets (pequeñas aplicaciones) para facilitar la forma en que se establecen las configuraciones de la máquina: Identificación de red, Hardware, Perfiles del usuario y Avanzado.

Usuarios y Contraseñas

Esta utilería se utiliza para agregar usuarios y grupos. Sin un usuario no administrativo desea cambiar esta información, la aplicación le permite hacerlo sin que sea necesario desconectarse y luego volver a conectarse.

AGREGAR/QUITAR HARDWARE

Cuando Windows 2000 Professional detecta un hardware nuevo, verifica las configuraciones actuales para el

dispositivo e instala el controlador correcto; además el asistente, muestra una lista del hardware instalado y ayuda a verificar para que esté seguro de que cada dispositivo está trabajando de manera adecuada.

HERRAMIENTAS ADMINISTRATIVAS

En el Panel de Control mejorado, las herramientas avanzadas están en el mismo cuadro de diálogo. Estas herramientas incluyen:

- **Servicios de Componentes.** La cual se utiliza para instalar y administrar programas COM+ de una interfaz gráfica, o para automatizar tareas administrativas utilizando un lenguaje de programación o script.
- **Administración de Sistema.** La administración de la computadora combina varias herramientas administrativas de Windows 2000 (Herramientas de Sistema, Almacenamiento, y Servicios y Aplicaciones) en un solo árbol de consola, que ofrece fácil acceso a propiedades administrativas de la computadora específica.

VISUALIZADOR DE EVENTOS

Al utilizar los registros de eventos del Visualizador de Eventos, se puede compilar información acerca del hardware, software y problemas con el sistema, además de monitorizar eventos de seguridad de Windows 2000.

INTERFAZ DEL USUARIO SIMPLIFICADA

Con Windows 2000 Professional el escritorio está menos desordenado, se han consolidado varios componentes de la interfaz en áreas comunes, como mover la Barra de Canales a Mis Favoritos.

La función Historial rastrea los documentos que se han abierto y permite recuperar con rapidez los archivos en los que se ha trabajado en el pasado. Se desarrolló un asistente fácil de un paso para ayudar a conectarse a unidades de red: ahora se puede conectar con facilidad a una red eligiendo únicamente Herramientas, Conectar a unidad de red y escribiendo el nombre del servidor y el del componente compartido.

MENUS PERSONALIZADOS

Estos menús traen a la parte superior de la lista, las aplicaciones que se utilizan con mayor frecuencia, y ocultan de manera automática las aplicaciones que no se utilizan. Cuando se hace clic en el menú Inicio/Programas, se puede ver que Windows 2000 Professional sólo muestra las aplicaciones que se han utilizado más recientemente; el menú de Inicio no está sobrecargado con todos los demás programas que casi nunca se usan. También se ha hecho el menú de Inicio más fácil de configurar o personalizar. Localizar documentos se ha facilitado más en el Cuadro de diálogo Archivo/Abrir.

LA EVOLUCION DE PLUG AND PLAY

Plug and Play es una combinación de soporte de hardware y software que permite al sistema de la computadora reconocer y adaptar cambios en la configuración de hardware con poca o nula intervención del usuario. En Windows 2000, el soporte para Plug and Play fue optimizado para laptops, estaciones de trabajo y computadoras de servicios que incluyen tarjetas de sistema ACPI. Plug and Play permite cambiar la configuración de una computadora con la seguridad de que todos los dispositivos trabajarán juntos y de que la máquina iniciará correctamente después de hacer los cambios.

EL PODER DE WINDOWS NT

Microsoft Windows 2000 Professional se basa en la fuerza de Windows NT para proporcionar confianza, una mayor seguridad, la habilidad de operar de manera integrada con su red actual, así como un nivel de desempeño bastante efectivo.

MAYOR GRADO DE CONFIABILIDAD

Windows 2000 Professional, se hizo con el objeto de aumentar la confiabilidad de Windows NT Workstation, mejorando su protección a los archivos del sistema, la eliminación de los 45 escenarios más comunes de Reinicio, y la resolución y recuperación más sencillas de problemas. El nuevo Instalador de Windows contribuye a la estabilidad de Windows 2000 Professional, ya que tiene la capacidad de autorreparar aplicaciones que han sido dañadas.

WINDOWS INSTALLER

Es un nuevo servicio de instalación que consiste en un servicio de instalación residente en el sistema operativo, un formato estándar para administración de componentes y una API de administración para herramientas y aplicaciones.

COMPONENTES DE WINDOWS INSTALLER

Un componente de Windows Installer es el fundamental y más pequeño de los tres contenedores lógicos. El mismo, es una colección de archivos, llaves de registro y otros recursos que se instalan o remueven en conjunto.

Ruta Clave

La ruta clave representa el camino a un componente dado. Cuando una aplicación solicita una ruta para un componente, el servicio Windows Installer regresa la ruta al recurso de ruta clave (típicamente la ruta al archivo clave).

Código de Componente

El Código de Componente globalmente único, evita colisiones entre componentes que son distintos. Asimismo, los componentes de Windows Installer vencen una limitación tradicional del sistema operativo, el habilitar la administración efectiva de recursos además de los archivos.

FUNCIONES DE WINDOWS INSTALLER

Las funciones de Windows Installer son piezas granulares de una aplicación que una persona puede instalar y, por lo general, representan las funciones de la aplicación misma. En esencia, las funciones son grupos de componentes. Es instructivo ver una función como una forma meramente conveniente para seleccionar un grupo de componentes para la instalación.

PRODUCTOS DE WINDOWS INSTALLER

Consisten en una o más funciones de Windows Installer. Cada producto se describe en el servicio Windows Installer en la forma de un solo archivo de paquete (archivo *.msi). Los productos no poseen en forma directa alguno de los recursos, pero sí tienen identificadores únicos globalmente conocidos como Códigos de producto.

ARCHIVO DE PAQUETE DE WINDOWS INSTALLER

Este archivo es un formato de la base de datos que ha sido optimizado para el rendimiento de instalación y describe, entre otras cosas, las relaciones entre funciones, componentes y recursos para un producto dado.

INSTALACION A SOLICITUD: NIVEL DE FUNCIÓN

Las aplicaciones que utilizan la API de administración del servicio Windows Installer no requieren que la persona ejecute la instalación nuevamente, si decide más tarde que requiere funcionalidad adicional. Si mientras usa tal aplicación se solicita alguna funcionalidad que no fue previamente instalada, la aplicación puede llamar al servicio Windows Installer para instalar la función o funciones necesarias para la persona.

INSTALACION TERMINADA (VOLVER LA INSTALACION ORIGINAL)

El servicio Windows Installer mantiene una operación de deshacer para cada operación que ejecute durante una instalación, remoción o cualquier otro cambio de configuración. Si algo falla durante una sesión de instalación, el servicio Windows Installer puede regresar la computadora al estado preciso en el que estaba; esto incluye la restauración de archivos escritos o borrados, llaves de registro y otros recursos.

ELASTICIDAD DE LA FUENTE

Siempre que el servicio de Windows Installer necesite acceso a los medios fuente para realizar una instalación a solicitud, reinstalación, u otra operación de configuración, tiene la habilidad de buscar fuentes de respaldo si la fuente adicional no está disponible debido a una avería de la red u otro problema temporal.

ACTUALIZACIONES Y PARCHES

Además del soporte de actualización nativo, el servicio Windows Installer proporciona tecnología incorporada de parches. De la misma forma en que el paquete Windows Installer se somete al servicio de Windows Installer para ser instalado, un parche basado en Windows Installer puede aplicarse a un producto existente instalado por Windows Installer para actualizarlo o repararlo. Después de aplicado el parche de Windows Installer, permanece en la computadora y se usa con los medios de la fuente original para proporcionar los bits para instalación a solicitud y la elasticidad.

TRANSFORMACIONES DE PERSONALIZACIÓN

Las transformaciones de personalización del servicio Windows Installer modifican el archivo de paquete de Windows Installer en el momento de la instalación y puede, por tanto, afectar dinámicamente el comportamiento de la instalación. Las modificaciones genéricas pueden construirse en una simple transformación y aplicarse a muchos paquetes diferentes, siempre que tales modificaciones sean legales para los archivos de paquete en cuestión.

De forma similar a los parches, las transformaciones de personalización permanecen almacenadas en la memoria caché de la computadora.

OPERACIÓN EN AMBIENTES ASEGURADOS

En un ambiente Windows 2000, usando el cambio basado en la Política de Grupo y Administración de Configuración, el administrador puede aprobar ciertas aplicaciones, al especificar que todas las operaciones de configuración en tales aplicaciones (instalación, remoción y reparación) se ejecuten como cuenta del sistema local. De esta forma, los administradores pueden asegurar el registro y los sistemas de archivo, el servicio Windows Installer puede todavía realizar instalaciones para la persona. Sólo las aplicaciones aprobadas por el administrador se ejecutan con privilegios elevados.

En un ambiente Windows NT 4.0, los administradores pueden especificar que todas las operaciones de Windows Installer se ejecuten con privilegios del sistema local, pero ciertos productos no pueden aprobarse en forma granular.

SERVICIOS WINDOWS INSTALLER DENTRO DE AMBIENTES ADMINISTRADOS

Windows Installer está disponible en Windows 95, Windows 98 y Windows NT 4.0 y está incorporado a Windows 2000. Puede usarse para efectuar instalaciones en forma local o puede utilizarse con Systems Management Server 2.0 para el control centralizado de instalación y distribución de software.

Windows Installer es una parte importante de IntelliMirror, un componente clave de la Administración de Configuración y cambios basados en políticas de Windows 2000.

El servicio Windows Installer proporciona ciertas funciones de elasticidad mejorada en escritorios Windows 2000, sin importar si el escritorio existe en un ambiente administrado por Windows Server 2000. La información a nivel de producto, requiere soporte del sistema operativo, pero éste también habilita la elasticidad del recurso cuando se activa un producto usando un acceso rápido habilitado por Windows Installer, registro de asociación de archivos, servidor OLE u otro punto de entrada.

SEGURIDAD BASADA EN ELEVADOS ESTANDARES DE DESEMPEÑO

Windows 2000 Professional ofrece una infraestructura segura que permite seleccionar los niveles de protección para la información y las aplicaciones que se necesitan. Para las computadoras que requieran estar conectadas a UNIX, Microsoft ofrece un complemento llamado Windows NT Servicios para UNIX que incluye un cliente y servidor NES, un cliente y servidor Telnet, herramientas de Scripting y sincronización de password.

Algunas de las características que se pueden encontrar en Windows 2000 Professional son:

SISTEMA DE ENCRYPTADO DE ARCHIVOS

Este nuevo sistema de encriptación EFS permite codificar archivos en el disco duro, a los que únicamente se puede tener acceso vía autorización de Windows NT. Esta característica protege archivos en caso de pérdida o robo de laptops, así como en sistemas de cómputo de oficinas.

EFS ofrece la tecnología principal de encriptación de archivos para almacenar los archivos NTFS encriptados en disco. EFS se dirige particularmente a los problemas de seguridad que surgen por las herramientas disponibles en otros sistemas operativos, que permiten acceder archivos desde un volumen NTFS sin una verificación de acceso.

Una medida de seguridad estándar en un sistema de computadora personal es hacer el intento de iniciar desde un disco flexible antes de intentarlo desde el disco duro; esto protege a los usuarios contra fallas en el disco duro y particiones de inicio dañadas. Lamentablemente, también agrega la conveniencia de iniciar diferentes sistemas operativos. Esto podría significar que alguien con acceso físico a un sistema pudiera desviar las funciones de seguridad integradas del control de acceso al sistema de archivos Microsoft® Windows NT®, utilizando una herramienta para leer las estructuras en disco Windows NTFS.

TECNOLOGÍA DE ENCRYPTACIÓN EFS

EFS se basa en la encriptación de clave pública, que aprovecha la arquitectura CryptoAPI en Windows. Cada archivo se encripta utilizando una clave generada de manera aleatoria, que es independiente del par de clave privada/pública de la persona que lo utiliza, con lo que se evita varias formas de ataque con base en

criptoanálisis. La encriptación de archivos puede utilizar cualquier algoritmo de encriptación simétrico.

La primera versión del EFS expone DES como el algoritmo de encriptación, pero las versiones futuras permitirán esquemas de encriptación alternos.

DÓNDE RESIDE EL EFS

El EFS está integrado firmemente con el NTFS. Cuando se crean archivos temporales, los atributos del archivo original se copian a los archivos temporales, siempre que los archivos estén en el volumen NTFS. Si encripta un archivo, el EFS también encripta sus copias temporales.

El EFS reside en el kernel del sistema operativo y utiliza una agrupación de no búsqueda para almacenar las claves de encriptación de archivo, lo que asegura que nunca estén en el archivo de búsqueda.

INTERACCIÓN DEL USUARIO

La configuración predeterminada del EFS permite que los usuarios inicien la encriptación de archivos sin esfuerzo administrativo. El EFS genera de manera automática un par de clave pública para la encriptación de archivos de un usuario, en caso de que no exista. La encriptación y desencriptación de archivos se soporta sobre una base de directorio completo o por archivos; la encriptación de directorios se refuerza de manera transparente. Todos los archivos (y subdirectorios) creados en un directorio marcado para encriptación se encriptan en forma automática.

Cada archivo tiene una clave de encriptación única, lo que lo hace seguro para volver a nombrarlo; si renombra un archivo desde un directorio encriptado a un directorio no encriptado en el mismo volumen, el archivo permanece encriptado. Los servicios de encriptación y desencriptación están disponibles en Windows Explorer.

SISTEMA DE AUTENTICACIÓN KERBEROS

La implementación del protocolo Kerberos versión 5 en Windows 2000 se basa en RFC 1510, que ha pasado a través de una amplia revisión de la industria y es bien conocido en la comunidad de seguridad. La autenticación Kerberos proporciona varias funciones que soportan los objetivos de rendimiento y seguridad para las redes empresariales.

Windows 2000 integra el protocolo Kerberos en el modelo de seguridad distribuida de Windows 2000 existente, y utiliza las funciones de ampliación del protocolo, como lo han hecho otras arquitecturas de seguridad, como DCE y SESAME. El protocolo Kerberos es sólo uno de los protocolos de seguridad soportados en Windows 2000; otros incluyen NTLM para compatibilidad con versiones anteriores SSL y la Seguridad de nivel de transporte (TLS) estándar de IETF para autenticación de clave pública, Negociación protegida individual (SPNEGO) de mecanismos de seguridad y la seguridad IP (IPsec) para la seguridad a nivel de la red utilizando la autenticación de clave compartida o clave pública.

El Kernel de Windows 2000 realiza una verificación de acceso en cada intento para abrir un controlador de objetos. El control de acceso y la auditoría se administran al configurar las propiedades de seguridad del objeto para otorgar permisos al usuario, o preferencia a un grupo. La autorización se administra de manera central, al agregar usuarios a los grupos de Windows 2000 a los que se otorgan los derechos de acceso correspondiente.

Windows 2000 utiliza la autenticación Kerberos para realizar una conexión interactiva del usuario hacia una cuenta de dominio Windows 2000.

Windows 2000 implementa un Centro de distribución de clave Kerberos (KDC) y Active Directory como servicios en el Controlador de dominio. Cualquier duplicación del DC Windows 2000 tiene un servicio KDC a su disposición; KDC se ejecuta como un proceso privilegiado junto con Active Directory. Ambos servicios administran la información sensible, incluidas contraseñas para las cuentas de usuarios.

AUTENTICACION TARJETA INTELIGENTE

Las tarjetas inteligentes son un componente clave de la infraestructura de clave pública que Microsoft está integrando en la plataforma de Windows, debido a que las tarjetas inteligentes mejoran las soluciones únicamente de software como autenticación, conexión y correo electrónico seguro. Las tarjetas inteligentes son esencialmente un punto de convergencia para certificados de clave pública y claves asociadas ya que proporcionan almacenamiento resistente a intromisiones para proteger las claves privadas y otras formas de información personal; aíslan cómputos críticos de seguridad que impliquen autenticación, firmas digitales e intercambio de claves de otras partes del sistema que no tengan una necesidad de saber; y permiten la portabilidad de credenciales y de otra información privada entre computadoras en el trabajo, el hogar o el camino.

AUTENTICACIÓN DEL CLIENTE

La autenticación del cliente implica la identificación y la validación del mismo a un servidor para establecer un canal seguro de comunicaciones. Un protocolo seguro como el nivel de Socket seguro (SSL) o Seguridad en el nivel de transporte (TLS) se utiliza generalmente junto con un certificado de clave pública confiable, proporcionado por el cliente que identifica a éste con el servidor. El cliente podría ser Internet Explorer ejecutándose en Windows o Windows NT, y el servidor podría ser Internet Information Server (o algún otro servidor del Web que soporte SSL/TLS).

CONEXIÓN INTERACTIVA DE CLAVE

Windows 2000 soportará la conexión interactiva de clave pública usando un certificado X.509v3 que está almacenado en una tarjeta inteligente junto con la clave privada. En lugar de una contraseña, la persona registra un número de identificación personal (NIP) en la identificación gráfica y autenticación (GINA), que se usa posteriormente para autenticar a la persona con la tarjeta.

El certificado de clave pública de la persona se recupera de la tarjeta a través de un proceso seguro; se verifica su validez y que sea de un emisor confiable. Durante el proceso de autenticación se emite un challenge, basado en la clave pública contenida en el certificado; se debe verificar que la tarjeta en realidad posea la clave privada correspondiente y pueda utilizarla con éxito. Después de una verificación minuciosa del par de claves privada y pública, la identidad de la persona contenida en el certificado se utiliza para hacer referencia al objeto de la persona almacenado en Active Directory, para construir una contraseña y regresar al cliente Ticket Granting Ticket (TGT).

CORREO ELECTRÓNICO SEGURO

Esta es una de las aplicaciones más emocionantes y habilitadas por la clave pública, debido a que permite compartir información de manera confidencial y se puede confiar en que la integridad de la información se mantuvo durante el tránsito. Al utilizar Microsoft OutlookTM Express o el cliente de colaboración y mensajes de Outlook 98, la persona puede seleccionar un certificado de clave pública emitido por una autoridad de certificados de confianza que se use para firmar en forma digital y descifrar mensajes seguros. Al publicar el certificado de la persona en un directorio público en la empresa o en Internet, otras personas dentro de una compañía o en la Red de redes pueden enviar correo electrónico encriptado al usuario, y viceversa.

AUTENTICACION DE CLAVES PÚBLICAS

Windows 2000 Professional soporta certificados estándar X.509 v3.0. El sistema operativo Microsoft Windows 2000 introduce una infraestructura de claves públicas (PKI) completa para la plataforma Windows. Esta infraestructura amplía los servicios criptográficos de claves públicas (PK) basados en Windows que fueron introducidos durante los últimos años, por lo que proporciona un conjunto integrado de servicios y herramientas administrativas a fin de crear, instalar y administrar aplicaciones basadas en PK. Esto permite a los desarrolladores aprovechar los mecanismos de seguridad de confidencialidad compartida o el mecanismo de seguridad basado en PK, según sea necesario.

CRIPTOGRAFÍA DE CLAVES PÚBLICAS

La criptografía es la ciencia de proteger datos. Los algoritmos criptográficos combinan matemáticamente datos de texto simple de entrada y una clave de encriptación para generar datos encriptados (texto cifrado). Con un buen algoritmo criptográfico, no es posible, desde el punto de vista computacional, invertir el proceso de encriptación y derivar los datos de texto simple, empezando sólo con el texto cifrado; algunos datos adicionales, como una clave de desencriptación, son necesarios para efectuar la transformación.

FUNCIONALIDAD DE CLAVES PÚBLICAS

La separación entre claves públicas y privadas en la criptografía PK ha permitido la creación de varias nuevas tecnologías. Las más importantes de éstas son las firmas digitales, la autenticación distribuida, convenio de claves secretas a través de claves públicas y sin claves secretas compartidas anteriores.

Las siguientes líneas describen los usos principales de la criptografía PK.

Firmas Digitales

Crear y validar firmas digitales se basa en una transformación matemática que combina la clave privada con los datos que se van a firmar, de tal forma que: 1) sólo la persona que posee la clave privada pudo haber creado la firma digital; 2) quien tenga acceso a la clave pública correspondiente puede verificar la firma digital; 3) cualquier modificación de los datos firmados invalida la firma digital.

Autenticación

La autenticación de entidades garantiza que el transmisor sea la entidad que el receptor piensa que es. Si una persona recibe datos de otra, y después le envía un intercambio de señales encriptado con la clave pública de la segunda persona, ésta decodifica el intercambio de señales y lo envía de nuevo a la primera persona, probando que tiene acceso a la clave privada asociada con la clave pública que esa persona utilizó para emitir el intercambio de señales.

Convenio de claves secretas a través de clave pública

Otra función de la criptografía PK es que permite que dos partes acuerden una clave secreta compartida, utilizando redes de comunicaciones públicas y no seguras.

Encriptación de datos masivos sin claves secretas compartidas anteriores

La cuarta tecnología principal habilitada por la criptografía PK es la capacidad de encriptar datos masivos, sin establecer claves secretas compartidas anteriores. Los algoritmos PK existentes tienen un alto nivel computacional con relación a los algoritmos de claves secretas; esto los hace adecuados para la encriptación de grandes cantidades de datos. Para obtener las ventajas de la criptografía PK junto con la encriptación eficaz masiva, normalmente se combinan las tecnologías PK y de claves secretas.

PROTEGER Y CONFIAR CLAVES CRIPTOGRÁFICAS

En la criptografía de claves secretas, los dos usuarios confían en su clave secreta compartida porque la acordaron mutuamente o la intercambiaron en una manera segura, y cada uno convino guardarla para evitar el acceso de una tercera parte mal intencionada. En contraste, al utilizar la criptografía PK, la primera persona sólo necesita proteger su clave privada y la segunda persona la suya.

Confianza y validación

Microsoft Certificate Services, que se incluyen con Windows 2000, proporcionan un medio para que una empresa establezca CA con facilidad a fin de soportar requerimientos empresariales. Los Servicios de certificación incluyen un módulo de políticas predeterminadas que es adecuado para emitir certificados destinados a entidades empresariales. Esto incluye identificación de la entidad solicitante y validación de que el certificado solicitado está permitido bajo la política de seguridad PK de dominio; puede modificarse fácilmente o mejorarse para cubrir otras consideraciones de políticas o ampliar el soporte CA para varios escenarios de extranet o internet.

JERARQUÍAS DE CERTIFICACION

Windows 2000 PKI supone un modelo CA jerárquico. Éste fue elegido por su capacidad de escalabilidad, facilidad de administración y consistencia con un creciente número de productos CA comerciales y de terceros. En su forma más simple, una jerarquía CA consta de una sola CA, a pesar de que en general una jerarquía contiene múltiples CA con relaciones principales y secundarias claramente definidas. De hecho puede haber varias jerarquías de interés sin conectar; no existe un requerimiento de que todas las CA compartan una CA principal común de nivel superior (o raíz).

En este modelo, los componentes secundarios son avalados por certificados emitidos por una CA principal, que une una clave pública de CA a su identidad y a otros atributos manejados por políticas. La CA en la parte superior de una jerarquía se conoce generalmente como una raíz CA. Las CA subordinadas se conocen a menudo como CAs intermedias o emisoras.

En un mundo ideal, PKI sería una infraestructura. Las CA emitirían un paquete de certificados completamente interoperables basados en un protocolo estándar de solicitud de certificados: Entonces, las aplicaciones los evaluarían en una manera consistente (incluso si han sido revocados), y no habría ambigüedad en la interpretación de sintaxis o gramática en ninguna parte del proceso.

REDES PRIVADAS VIRTUALES

Una de las funciones de una plataforma de comunicaciones basada en Windows es el soporte de Red Privada Virtual o VPN. Las VPN se han hecho populares debido a que ofrecen ahorros operacionales, a la vez que mantienen la seguridad relacionada con la infraestructura de red privada. Al utilizar una VPN, un trabajador que se traslada de un lado al otro o una sucursal, puede conectarse a la red corporativa con una llamada local, proporcionando ahorros importantes en el uso de larga distancia, número 800 o líneas contratadas.

La seguridad se mantiene debido a que VPN utiliza un túnel seguro, con lo que permite que sólo los usuarios autenticados accedan a la Intranet corporativa. Las soluciones VPN de Microsoft ofrecen encriptación de 128 bits dentro de Estados Unidos, con encriptación de 40 bits soportada en el extranjero donde la ley lo permita. Una red privada virtual se puede describir como la capacidad de conectarse por túnel a través de Internet u otra red pública, de manera que proporcione la misma seguridad y otras funciones que antes estaban disponibles únicamente en las redes privadas. Con el túnel se encapsula un paquete de mensajes dentro de un paquete IP para su transmisión a través de la red pública, y la encapsulación de información se abre al llegar a la red objetivo, como puede ser la red de área local corporativa (LAN).

Windows 2000 Professional incluye soporte para las Redes a fin de permitir al sistema comunicarse en forma privada en redes pública. Se puede crear una Red Privada Virtual que proporcione acceso seguro a la red de la empresa usando un proveedor de servicios Internet local (ISP) y una de las tres diferentes tecnologías que Windows 2000 Professional soporta: Protocolo Point to Point Tunneling (PPTP), Protocolo Layer 2 Tunneling (L2TP), o Protocolo de Seguridad IP (IPSec).

LO MEJOR DE WINDOWS 98

Windows 2000 Professional incluye y mejora las funciones clave de Windows 98, con lo que perfecciona el apoyo a sistemas móviles y agrega soporte para los últimos modelos de equipos. Está diseñado para que las personas que trabajan fuera de línea (desconectados de una red), tengan la misma experiencia que las que trabajan en línea. Administrar los documentos fuera de línea y de las páginas de la Red es mucho más automatizado, ya que las mejoras en el sistema indican y actualizan la administración.

Uno de sus principales objetivos de diseño es crear un ambiente de trabajo consistente para las personas que usan computadoras móviles, ya sea que estén conectadas o desconectadas de la red, lo que les permite trabajar en forma más productiva. Como resultado, las personas pueden trabajar en los mismos archivos, carpetas o sitios Web estando conectados o no, y sincronizar con facilidad esos recursos.

ACCESO FUERA DE LÍNEA

Archivos y carpetas fuera de línea permite a las personas móviles utilizar cualquier combinación de archivos, carpetas o controladores correlacionados fuera línea. En lugar de utilizar una herramienta por separado, como el Portafolio, la persona simplemente hace clic con el botón derecho del mouse en cualesquier archivos o carpetas de la red, y después hace clic en Hacer disponible fuera de línea en el menú. La función de archivos y carpetas fuera de línea funciona con cualquier servidor de archivos de Server Message Block (SMB), incluidos Windows for Workgroups y cualquier versión de Windows NT Server. Las mejoras adicionales para utilizar recursos fuera de línea están disponibles cuando se utiliza Windows 2000 Professional junto con Windows 2000 Server. Con Windows 2000 Server, los administradores pueden establecer propiedades sobre carpetas de red compartidas para definir cómo almacenar esos archivos en las computadoras de cliente.

ACCESO A CONTENIDO WEB FUERA DE LÍNEA

Las personas que utilizan Windows 2000 Professional también pueden acceder a páginas o sitios Web completos fuera de línea, para verlos en la misma forma que los archivos o carpetas fuera de línea; simplemente, hacen clic con el botón derecho del mouse en el sitio Web de una de las barras de Explorer. Un asistente guía a las personas a través del uso de una página Web fuera de línea y sus vínculos relacionados, y las personas pueden programar cuándo se deben realizar las actualizaciones al contenido de la página Web. Windows 2000 proporciona una sola herramienta para sincronizar todos los recursos de la red, lo que permite ahorrar tiempo.

ADMINISTRADOR DE SINCRONIZACIÓN

Con esta nueva herramienta de sincronización de Windows 2000 Professional, las personas pueden sincronizar en una sola ubicación todos los recursos de la red, incluidos archivos, carpetas, correo electrónico y bases de datos. Asimismo, las personas pueden configurar el Administrador de sincronización para que sincronice en forma automática algunos o todos sus recursos; por ejemplo, las personas pueden configurar ciertos archivos y carpetas para que se sincronicen cada vez que se conectan o desconectan de la red. El administrador de sincronización explora el sistema en busca de cambios, y si detecta alguno, los recursos se actualizan en forma automática. Sólo se actualizan los recursos que han cambiado, lo que acelera significativamente la sincronización.

ADMINISTRACIÓN DE ENERGÍA DE LA PC PORTÁTIL

Maximizar la vida de la batería es un reto constante para los usuarios móviles, por lo que Windows 2000 Professional soporta la generación más reciente de tecnología de administración de energía conocida como hardware de Interfaz de energía y Configuración avanzada (ACPI). ACPI define una interfaz de administración de energía de hardware ampliable y flexible. Con ACPI, Windows 2000 Professional puede administrar el estado de energía del usuario, aplicaciones y controladores de dispositivos.

Además, el sistema se puede configurar para entrar en reposo después de cinco minutos, lo que da a la persona la posibilidad de aprovechar todo el día visitando cliente. El desempeño en este caso sería lento, pero la persona decide qué es más importante, si el desempeño o la energía. Una aplicación podría notificar al sistema operativo que está realizando un cálculo grande o reproduciendo una película, y la PC no cambiaría a un estado de baja energía.

ADMINISTRACIÓN DE LOS DISPOSITIVOS PERIFÉRICOS

Las personas que trabajan fuera de línea pueden agregar rápida y confidencialmente dispositivos periféricos a sus computadoras. Windows 2000 Professional detecta en forma automática e instala la mayor parte de los dispositivos periféricos a sus computadoras. Windows 2000 Professional detecta en forma automática e instala la mayor parte de los dispositivos nuevos y antiguos de hardware para un rendimiento Plug and Play verdadero. Plug and Play también ahorra tiempo cuando se anexan dispositivos como proyectores y/o monitores grandes a laptops durante una presentación.

Windows 2000 Professional soporta el estándar Bus Serial Universal (USB), que se puede utilizar para conectar dispositivos USB a las computadoras sin que se requiera reiniciarlas. Estos dispositivos usan un cable de conexión estándar, lo que significa que no hay necesidad de viajar con cables y conectores adicionales.

CONEXIÓN Y DESCONEXIÓN

Los que utilizan Windows 2000 Professional pueden conectar computadoras móviles dentro y fuera de una estación de conexión sin que se requiera reiniciarla. Esto es especialmente útil al trasladarse de un ambiente, como una oficina, a una sala de conferencias para una presentación (las aplicaciones abiertas y los documentos siguen ejecutándose). Si la persona conecta la computadora a una configuración desconocida, se detecta e instala el nuevo hardware.

PERFILES DE HARDWARE

Los que utilizan Windows 2000 Professional pueden moverse con facilidad entre diferentes ambientes de hardware sin que sea necesario reconfigurar el hardware o descifrar mensajes de error sobre dispositivos que no se requieren para un perfil dado.

ONNOW: INICIO Y APAGADO RÁPIDOS

Windows 2000 Professional hace que la computadora se active con el uso de un switch. El soporte para el estándar de hardware ACPI permite a la persona pasar del modo **hibernar** a activado en menos de 30 segundos. El modo **hibernar** interrumpe toda la energía de la computadora durante un tiempo indefinido, a la vez que conserva el estado de los programas abiertos y del hardware conectado cuando la computadora pasó a modo de hibernación.

SOPORTE PARA CAPACIDADES MULTILINGÜES

El objetivo de Windows 2000 Professional es dar soporte a las necesidades multilingües de negocios que trabajan en forma global, incluso la facilidad de que los usuarios trabajen en ambientes de idiomas mixtos y reducir el costo total de propiedad (TCO) para implementar y administrar ambientes multilingües. Microsoft ofrece tres versiones distintas: Windows 2000 Professional, versión en inglés; ediciones de idiomas plenamente localizados (disponible en más de 20 idiomas); y Windows 2000 Professional, version MultiLanguage.

Para un acceso superrápido, Windows 2000 Professional soporta el modo **Suspend**, que coloca al sistema en un reposo profundo, con cierta energía. La activación desde el modo **Suspend** sólo toma algunos segundos y sin embargo agrega horas a la vida de una batería.

CREACIÓN DE CONEXIONES REMOTAS

Windows 2000 Professional facilita de manera significativa la conexión remota a redes, incluidas Redes privadas virtuales (VPN), a través de conexiones por marcación, infrarroja y cable directo.

Un asistente nos guía a través de las conexiones de configuración para diferentes tipos de redes, lo que elimina la necesidad de establecer configuraciones manualmente. El asistente de conexión de red ayuda a crear varios tipos de nuevas conexiones con una sola herramienta. La configuración de la conexión también es automatizada, lo que descarta la necesidad de descargar e instalar servicios adicionales, un paso necesario en Windows 95 para configurar ciertos tipos de redes remotas.

CONEXIONES INALÁMBRICAS

Windows 2000 Professional soporta la serie de protocolos de Asociación de datos infrarrojos (IrDA), que permite transferir información y compartir recursos entre computadoras, como impresoras, sin cables físicos. La mayor parte de las computadoras portátiles más nuevas incluyen soporte de hardware para IrDA.

Windows 2000 Professional también soporta la capacidad de otorgar permisos o limitar a las personas que no sean el propietario de la computadora para enviar archivos utilizando la conexión infrarroja; también se puede especificar la ubicación donde deben recibirse los documentos.

USO DEL MISMO DISPOSITIVO PARA VARIAS CONEXIONES

La función Configuraciones por conexión en Windows 2000 Professional mantiene configuraciones individuales para cada conexión de red, de manera que las personas se puedan conectar a varias redes diferentes sin que se requiera reconfigurar las complejas especificaciones para cada una de ellas.

PERFILES DEL USUARIO

Windows 2000 Professional da soporte utilizando varios perfiles del usuario en la misma computadora, lo que evita que los datos del usuario sean vistos por otro. Los administradores pueden configurar laptops con Windows 2000 Professional para que los usuarios tengan su propio conjunto de datos, aplicaciones y preferencias protegidos.

Muchos componentes específicos, como módems o tarjetas de red, se pueden configurar para trabajar a través de cada uno de los perfiles del usuario. Sólo los usuarios con derechos administrativos pueden ver todos los archivos.

PERMISOS DE ACCESO A ARCHIVOS

Los usuarios de Windows 2000 Professional pueden configurar permisos de acceso a archivos, ya sea a través

de la red o en forma local. Estos permisos se pueden configurar para usuarios individuales o grupos de usuarios.

PROTECCIÓN DE LAPTOPS CON TARJETAS INTELIGENTES

Windows 2000 Professional proporciona la opción de equipar a los usuarios con tarjetas inteligentes, que habilitan un sistema de seguridad de factor múltiple y logran que las computadoras sean más seguras. Los lectores de tarjeta inteligentes de PC están disponibles a través de toda una gama de fabricantes.

SOPORTE PARA LA NUEVA GENERACIÓN DE EQUIPOS

Windows 2000 Professional soporta a más de 7,000 dispositivos, incluso aquellos no apoyados previamente en el programa de Windows NT Workstation 4.0. Destacan cámaras digitales, escáners e impresoras; esto representa un aumento del 60% de compatibilidad sobre el Windows NT Workstation 4.

¿QUE VERSION ES LA MEJOR PARA SU ORGANIZACIÓN?

WINDOWS 2000 PROFESSIONAL, VERSIÓN EN INGLÉS

Está diseñado para compañías que realizan casi todos sus negocios en inglés, pero que cuentan con algunos usuarios que trabajan en otros idiomas. Ésta, como todas las ediciones, dan soporte a las funciones de edición y vista multilingüe que permiten que los usuarios lean y escriban documentos en más de 60 idiomas. La tecnología multilingüe en Windows 2000 Professional da soporte a la vista y entrada del idioma chino, para crear y ver documentos en chino cuando sea necesario.

Algunos usuarios que probablemente sean los principales beneficiados con esta versión son organizaciones con una base de usuario que requiere inglés como el idioma de interfaz (UI) para todo su trabajo; y/o usuarios que necesitan leer y escribir documentos en otros idiomas, pero quieren operar en un ambiente que utilice un UI en inglés.

WINDOWS 2000 PROFESSIONAL, VERSIONES LOCALIZADAS

Las ediciones localizadas de Windows 2000 Professional están diseñadas para organizaciones que realizan la mayor parte de sus negocios en un solo idioma que no sea inglés; por ejemplo, una empresa regional con sede en Japón que ofrece sus servicios principalmente a clientes japoneses.

Debido a que cada versión localizada de Windows 2000 Professional incluye funciones de edición y vista multilingüe, los administradores o usuarios pueden instalar series de caracteres adicionales para otros idiomas, incluidos números y letras, símbolos de divisa local y otras configuraciones.

WINDOWS 2000 PROFESSIONAL MULTILANGUAGE VERSION

Proporciona un nivel adicional de soporte multilingüe, al permitir a los usuarios cambiar el idioma de la interfaz del sistema operativo. Esto significa que la persona se puede conectar a una estación de trabajo y utilizar Windows 2000 Professional en cualquiera de los 24 idiomas que incluyen ediciones totalmente localizadas, sólo si el administrador ha instalado los archivos de idioma apropiados. Además, el usuario podrá editar y ver documentos en más de 60 idiomas.

Con el administrador de instalación Windows 2000 Professional, la herramienta gráfica para crear scripts de instalación automatizada, los administradores pueden establecer una localización para que el sistema asegure los símbolos, teclado, divisas apropiados, etc., que se instalen por predeterminación. Los usuarios de la versión Windows 2000 Professional MultiLanguage que utilizan diferentes idiomas para sus tareas cotidianas

pueden compartir estaciones de trabajo.

Windows 2000 Professional MultiLanguage Version dará soporte a los 24 idiomas totalmente localizados que se incluyen en Windows 2000.

27

1