

Seguridad Física de Redes

**Seguridad en Redes de Arriba a Abajo**  
Antes del Firewall, considere el candado.



Índice	
Introducción	3
La meta de la seguridad de redes	3
Seguridad por capas—utilización del modelo OSI como modelo de seguridad	4
Porque el acceso físico a las computadoras es un problema	5
¡Círrrelo con candado!	5
Cámaras de seguridad	8
Asegure sus dispositivos de entrada/salida	9
Utilice Fibra Óptica	10
Proteja sus datos	10
Proteja el equipo de daños accidentales	11
Maneje con cuidado lo inalámbrico	13
No olvide la evidencia en papel	13
El hueco de seguridad más vulnerable—los seres humanos	13
En conclusión	13
Acerca de Black Box	13

Estamos aquí para ayudarle. Si tiene cualquier pregunta acerca de su aplicación, nuestros productos o este documento, contacte a Soporte Técnico Black Box al 55 5420 0100 o 01 800 024 4201 opción 2, o visite [blackbox.com.mx](http://blackbox.com.mx)

## Introducción

*Ley #3: Si un tipo malo tiene acceso físico irrestricto a su computadora, entonces ya no es su computadora.*

*De "10 Reglas Inmutables de Seguridad," Centro de Respuesta de Seguridad Microsoft®*

Se ha dicho que la computadora más segura es una que esté en un cuarto con candado. Y además debe estar apagada.

Obviamente esta no es una situación de sistemas que funciona para la mayoría de las organizaciones, pero la idea general de que aislar las computadoras incrementa la seguridad sigue siendo verdad. El paso más básico que usted puede tomar hacia la protección de redes es proteger su hardware de manera que las personas no autorizadas no puedan tener acceso al mismo.

Proteger el hardware es importante porque si una persona tiene acceso físico a un dispositivo, casi siempre hay una manera de tomar el control y/u obtener datos del mismo.

Es a nivel de hardware, en la parte más baja de la jerarquía de redes, en donde su red es más vulnerable. Una computadora portátil perdida, un puerto USB abierto, una simple toma de red –pueden ser conductos para una pérdida rápida y devastadora de datos que ninguna firewall puede prevenir.

Pero es en el área del Hardware también es donde usted puede configurar la protección de red más efectiva negando el acceso físico a los dispositivos de red. Existen muchas maneras para asegurar la protección física de su red, desde simples candados de puerto hasta sistemas sofisticados de monitoreo remoto. Lo que todos tienen en común es que limitan el acceso al hardware de red para evitar la alteración no autorizada a dispositivos de red o el robo de información.

Este documento explora maneras de mejorar la protección de red mediante seguridad física básica. Independientemente de si está protegiendo secretos gubernamentales, cumpliendo con requerimientos de corporativo o manteniendo información financiera privada, primero tiene que ver quien puede tener acceso físico a su red.

## La meta de la Seguridad de Redes

La Seguridad en las Redes debe asegurar que los usuarios autorizados tengan un acceso cómodo y fácil a la información, previniendo al mismo tiempo el acceso o la manipulación no autorizados. Esto con frecuencia se expresa como Confidencialidad, Integridad y Disponibilidad (CIA, por sus siglas en inglés). La Confidencialidad es evitar que personal no autorizado obtenga información privada; Integridad es evitar que el personal no autorizado altere información; y Disponibilidad es asegurar que la información esté disponible a personal autorizado cuando sea necesario.

La seguridad de redes significa permitir a la gente adecuada tener acceso a la información correspondiente en el momento oportuno. Convirtiéndose en acto de fino equilibrio proteger datos y mantener fuera a usuarios no deseados mientras permite a su personal hacer el trabajo sin molestias innecesarias.

Es importante asegurar que las computadoras y el equipo de redes estén protegidos físicamente a un grado que sea congruente con su valor.

En resumen, la meta de la seguridad de redes es proporcionar máxima Confidencialidad, Integridad y Disponibilidad equilibrando el costo y riesgo.

### Seguridad por capas—utilización del modelo OSI como modelo de seguridad

La seguridad de redes está basada con frecuencia en el conocido modelo OSI, el cual organiza la formación de redes en siete capas. Cuando la información viaja de un nodo de red a otro, el control transferido de una capa a la siguiente, comenzando en la Capa 7 en el nodo de transmisión descendiendo hasta la Capa 1, cruzando al siguiente nodo y luego yendo de la Capa 1 de regreso a la Capa 7 en el nodo de recepción.

Las Capas del modelo OSI son:

Capa 1, Capa Física: Define las características mecánicas y eléctricas de equipo de redes tales como niveles de voltaje, temporización de señales, velocidad de datos, longitud máxima de transmisión, medios de transmisión, topología de red y conectores físicos.

Capa 2, Capa del Enlace de Datos: Aquí se codifican y decodifican paquetes de datos.

Capa 3, Capa de Red: Incluye protocolos de enrutamiento y conmutación.

Capa 4, Capa de Transporte: Proporciona la transferencia transparente de datos entre nodos, así como la recuperación de errores y el control de flujo.

Capa 5, Capa de Sesión: Establece, administra y termina conexiones.

Capa 6, Capa de Presentación: Formatea los datos que se van a enviar a través de una red para asegurar que no haya problemas de compatibilidad.

Capa 7, Capa de la Aplicación: Soporta aplicaciones y procesos del usuario final.

Un plan de seguridad de red completo se encarga de la seguridad en todas las capas OSI, comenzando en la Capa 1 con la protección del hardware y subiendo por todas las capas para incluir protección de contraseña, codificación, Redes Privadas Virtuales (VPNs), escaneo de virus y firewalls.

Una barrera de seguridad en cada Capa protege contra todos los tipos de ataques y proporciona una seguridad de red completa.

La seguridad de la Capa 1 se puede definir a grandes rasgos como la Seguridad Física – mantener a las personas físicamente alejadas del hardware que tiene datos no autorizados para ellas y también proteger el hardware de daño deliberado o accidental.

La seguridad de redes comienza desde la Capa 1. Primero usted debe controlar el acceso físico a una red, después se puede ocupar de la protección de la información. Las soluciones de software costosas y complejas no le hacen ningún bien, si en primer lugar su hardware de red no está protegido adecuadamente. Imagine la situación dónde a la semana siguiente de que usted compre el Firewall más novedoso del mercado, sus datos críticos salgan por la puerta del edificio en el bolsillo de alguien.

## Porque el acceso físico a las computadoras es un problema

El acceso físico irrestricto a una computadora o a una red es su amenaza de seguridad número uno. Si un hacker tiene acceso físico a su red entonces robar información es fácil – la manera más rápida para entrar a una red no es a través del firewall, sino a través de un puerto USB en una computadora que no esté vigilada. El ladrón de información más peligroso puede no ser un hacker que esté lejos sino uno del personal de limpieza dentro de su edificio.

Hay virtualmente un sin número de maneras en que la gente con malas intenciones puede dañar su equipo o robar datos si con tan solo un acceso físico. Por ejemplo, ellos podrían:

- Dañar su equipo usando el método más simple de golpear y patear.
- Utilizar una unidad USB flash para robar datos o introducir un virus dañino.
- Robar o copiar el disco duro y llevárselo para examinarlo en su tiempo de ocio.
- Instalar software no autorizado.
- Inicializar una computadora desde un disco flexible y reformatar el disco duro.
- Cancelar la protección de contraseña en una computadora abriendo el gabinete y reemplazando el chip BIOS.
- Instalar un hardware registrador de teclado para capturar cada golpe de tecla que usted haga.
- Aprenderse contraseñas de notas adheridas dejadas cerca de las computadoras o simplemente al ver a la gente insertar sus contraseñas.
- Recoger papeles que contengan datos privilegiados de la basura.
- Utilizar un dispositivo portátil tal como un iPod®, teléfono celular o cámara digital para extraer datos de su sistema.
- Instalar una toma de red y capturar datos que pasen por su red.
- Ejecutar un programa para conocer las contraseñas o insertar nuevas contraseñas en su sistema.

### ¡Círrrelo con candado!

Antes de instalar ese increíble firewall recuerde que un simple candado físico es su primera línea de defensa contra el acceso no deseado a su red. Cierre con candado gabinetes de cables, oficinas, CPUs de escritorio – cualquier cosa que pudiera proporcionar acceso físico a la red.

### Cerraduras de puerta

Lo primero que usted debería hacer para asegurar su red es poner el equipo tras una puerta cerrada con llave. Los cuartos de servidores, centros de datos y gabinetes de cableado deben estar siempre cerrados con llave. El equipo que se encuentre en áreas de oficinas debe mantenerse en un gabinete bajo llave. Adicionalmente, si es práctico, se debe controlar el acceso a todo el edificio.

Las cerraduras con llave se clasifican principalmente en dos categorías – el candado mecánico pasado de moda y las cerraduras electrónicas.

Aunque los candados mecánicos son simples, fáciles de usar (y con frecuencia, difíciles de seleccionar), generalmente no son la primera opción para las cerraduras de puertas en áreas de equipo. Las llaves se pueden perder o pueden ser robadas y muchas llaves se pueden duplicar fácilmente en la tlapalería local. La combinación de llave y candado está un tanto limitada porque es segura sólo si se puede mantener un control estricto sobre las llaves.

Adicionalmente, a diferencia de los sistemas de cerradura electrónica, las llaves y candados mecánicos, no generan registros de auditoría, de manera que usted no sabe quien tuvo acceso a su equipo ni cuando estuvieron ahí.

Los sistemas de acceso electrónico que utilizan tarjetas, tokens o biometría son los sistemas de cerradura de puerta más populares para proteger áreas de TI. Un sistema de acceso electrónico rastrea a cada usuario individualmente y crea una bitácora que muestra quien tuvo o solicitó acceso al cuarto. Además, estos sistemas le permiten personalizar el acceso, de manera que cada persona pueda entrar a diferentes áreas en su instalación.

Las tarjetas se pueden activar y desactivar rápidamente, de manera que las tarjetas perdidas no son un problema. Sin embargo, una debilidad en el sistema son las tarjetas que se pierden o “se prestaron” y que son usadas antes de que puedan ser descubiertas y desactivadas.

Por mucho, el tipo de cerradura de puerta más seguro es el sistema de acceso biométrico. La biometría es una tecnología que mide las características fisiológicas tales como huellas digitales, iris, voces, caras y manos con fines de autenticación.

La autenticación biométrica se está convirtiendo en una manera popular para identificar a la gente por motivos de seguridad ya que tiene la ventaja de ser más cómoda y más segura que los lectores de tarjeta tradicionales – a nadie se le olvida el dedo en casa ni desliza una retina no autorizada.

Los dispositivos biométricos consisten de:

- Un dispositivo lector o de escaneo
- Software para convertir los datos escaneados en forma digital y compararlos contra una base de datos.
- Una base de datos que guarda datos para comparación

Los datos biométricos son codificados después de ser recopilados. Cuando se escanea una parte del cuerpo, el software identifica puntos de datos específicos y los convierte a un valor numérico usando un algoritmo establecido. Entonces el software compara este valor con un número guardado en la base de datos para aprobar o negar el acceso. Como la base de datos guarda un valor numérico en lugar de una huella digital real o un escaneo del iris, un sistema biométrico no crea dificultades en cuanto a la privacidad.

La autenticación biométrica se puede utilizar sola, pero para incrementar la seguridad se combina frecuentemente con otros métodos de control de acceso tales como lectores de tarjetas, códigos de ingreso o firmas digitales.

Vale la pena recordar que cuando usted planee las cerraduras para sus puertas, un sistema de cerraduras maravilloso no le va a servir de nada si está en una puerta vulnerable. Observe las puertas para asegurarse que no puedan ser abiertas de una pateada o forzadas con una palanca fácilmente. Asegúrese de utilizar una protección de bisagras – una simple placa que cubre el espacio entre la puerta y la articulación – para bloquear el acceso al mecanismo de la bisagra de manera que la cerradura no se pueda botar con un cuchillo, tarjeta de crédito o desatornillador.



*Un ejemplo de un Sistema de Cerradura Biométrica: Control de Acceso Biométrico Black Box Intelli-Pass™ (SAC510NA).*

### Gabinetes con cerradura

Ahora que se ha vuelto una rutina instalar redes en empresas pequeñas y debido a la descentralización de redes, actualmente es común encontrar servidores y otros equipos de red fuera del tradicional ambiente del Centro de Datos.

Cuando el equipo se instala fuera de un centro de datos cerrado con llave, es más vulnerable, no sólo a merced de los hackers sino para cualquier curioso que pase y desee echar un vistazo.

El equipo de red fuera de los centros de datos cerrados con llave debería estar alojado en un gabinete con cerradura. Usualmente los gabinetes tienen rieles estándares de 19" para montaje de equipo en bastidores y están disponibles en tamaños que van desde gabinetes de tamaño completo hasta pequeños gabinetes de montaje en pared. Los gabinetes están disponibles incluso con características de control de clima, de manera que los puede colocar casi en cualquier parte sin tener que preocuparse acerca de temperaturas altas y humedad que dañe su equipo.

Aunque los gabinetes usualmente se cierran con cerraduras de llave estándares con sus consiguientes vulnerabilidades, cada vez hay más disponibles con candados de combinación y biometría.



*Un ejemplo de gabinete para equipo con montaje en pared con control de clima: Gabinete de montaje en pared con aire acondicionado Black Box ClimateCab NEMA 12 (RMW5110AC).*

## Computadoras portátiles

Las computadoras portátiles merecen una consideración especial porque su tamaño reducido y portabilidad las hace extremadamente vulnerables a pérdida y/o robo. Una computadora portátil robada puede no sólo divulgar información privilegiada, sino que también puede proporcionar a un hacker un enlace directo y cómodo a su red.

La mejor manera de evitar un riesgo de seguridad mediante una computadora portátil es, por supuesto, nunca tener datos confidenciales o acceso a la red en una computadora portátil. Pero como esto no siempre es posible, es aconsejable tomar precauciones adicionales con las computadoras portátiles.

Encerrar físicamente una computadora portátil puede hacer mucho para desalentar a un ladrón ocasional. Muchas de las computadoras portátiles actuales tienen una Ranura de Seguridad Universal (*USS, Universal Security Slot*) que les permite asegurarlas a un objeto inamovible con un cable con candado o cerradura.

Muchos de los robos de computadoras portátiles ocurren en la oficina. Utilice su computadora portátil con una estación base que pueda asegurarla en su lugar o encierre su computadora portátil en un escritorio seguro, gabinete o caja especialmente diseñada para computadora portátil con cerradura.

Etiquete su computadora. Si usted rotula o hace un grabado físico en su computadora con su identificación incrementa enormemente las posibilidades de que se le devuelva si se pierde y también la hace un objetivo menos atractivo para los ladrones. También es importante recordar registrar la computadora portátil con el fabricante cuando la compre. Esto permite rastrearla por número de serie.

Utilice la codificación a nivel BIOS para asegurar su computadora portátil. Cuando una computadora portátil está protegida en el nivel BIOS aparece una indicación de proporcionar una contraseña después de que la encienda pero antes de que el sistema se cargue y proporcione acceso a la computadora. Proteger por medio de contraseña una computadora portátil no va a derrotar a un hacker experimentado que puede trabajar con su computadora portátil con toda tranquilidad, pero puede hacer mucho para desalentar a los menos persistentes y hábiles. Asegúrese que la contraseña también proteja el disco duro para que no se pueda extraer fácilmente e instalarse en otra computadora.

Enséñele a su computadora portátil a llamar a casa. Muchas compañías ofrecen software de rastreo que hace que su computadora portátil revise y reporte periódicamente su posición utilizando una combinación de un sistema de posicionamiento global (GPS), puntos de conexión Wi-Fi®, una conexión Ethernet con cable o una red celular. Este servicio puede ayudarle a recuperar rápidamente una computadora portátil perdida o robada. Muchos de estos servicios también le permiten eliminar de manera remota datos en una computadora portátil si desaparece con información confidencial en la misma.

## CPUs, también

Imagínese una sala de espera con una pantalla de video en la pared que proporciona información acerca de inyecciones contra la gripa y el valor de verificar regularmente los valores de colesterol. Una revisión rápida muestra que el video proviene de una computadora personal conectada en red debajo de una mesa lateral – un premio para cualquier hacker experimentado.

Las computadoras en lugares públicos o semi-públicos tales como vestíbulos o salas de espera son blancos fáciles vulnerables para ser pirateadas o sufrir simples actos de vandalismo. Proteja estas computadoras dentro de un gabinete seguro o colóquelas en un área segura y utilice una extensión KVM para conectar un teclado, monitor y ratón colocados en el área pública.



*Un ejemplo de caja con cerradura para computadora portátil: Gabinete para computadora portátil Black Box (RM415A).*

### Cámaras de seguridad

Como no hay sustituto para ver en realidad lo que está pasando, la vigilancia por medio de video es una parte clave del plan de seguridad física de cualquier organización. Con video usted puede ver exactamente lo que le pasó a ese servidor y si la persona que lo hizo concuerda con la tarjeta de acceso que abrió el cuarto del servidor.

Los sistemas actuales de vigilancia por video digital son económicos, de peso ligero y se integran fácilmente en su red. Proporciona un video de calidad mucho mayor que los viejos sistemas que grababan en cinta, y como graban en DVR en lugar de cinta de video, no se tiene la dificultad de cambiar o almacenar cintas. Además, se puede acceder a los sistemas de video integrados en su red desde cualquier parte de la red – incluso a través de Internet.

Los sistemas de video actuales son inteligentes también. Usted los puede configurar para que graben continuamente, graben sólo cuando se abra una puerta, graben en un horario previamente establecido o graben en respuesta a un detector de movimiento. Muchos sistemas pueden enviar alarmas e imágenes a una cuenta de correo electrónico o incluso a su teléfono inteligente.

Para proteger áreas sin conexiones de red convenientes, considere una cámara inalámbrica 802.11g que se puede enlazar con su punto de acceso inalámbrico. Para aplicaciones de rango más largo, una extensión Ethernet inalámbrica de 900-MHz puede ser una manera efectiva de atravesar distancias largas.

Finalmente, recuerde que una cámara de vigilancia no tiene que estar necesariamente conectada o incluso ser real para ser efectiva. Una cámara “falsa” colocada estratégicamente puede reducir los problemas ya que hace pensar a las personas que están siendo observadas.



*Una cámara IP inalámbrica de largo rango: Juego de caja y Cámara de seguridad Black Box LongSpan (LS900-DOME-KIT) con Cámara IP Sony IPELA 340° PITIZ (SNC-RZ50N).*

## Asegure sus dispositivos de entrada/salida

Una computadora personal conectada en red que contenga datos protegidos debe tener todas las entradas y salidas también protegidas. Esto incluye puertos, unidades de disco y dispositivos conectados tales como teclados.

### **Puertos USB**

El puerto USB común es, definitivamente, uno de los portales más fáciles para saltar la red e introducir o extraer datos de una computadora. Los puertos USB son ubicuos – cada computadora portátil y cada computadora personal tiene por lo menos uno – y son fáciles de usar. Las unidades compactas USB flash son económicas, rápidas y pueden contener fácilmente 8 GB o más de datos.

En tan solo unos minutos un hacker puede sacar una unidad flash de su bolsillo, “absorber” todos los datos de su computadora y usted nunca se enterará que pasó. Un iPod® también se puede usar para esto pero eso no es muy común ya que un iPod es más caro, se puede relacionar más fácil al propietario con el aparato y es más difícil de programar. Una manera en que un hacker puede entrar a su sistema, es que cargue sus herramientas de software en una unidad flash y la deje en un área pública (como un área de fumar). La persona que lo encuentre invariablemente insertará la unidad flash en el puerto USB de la computadora para ver que hay en el mismo. Entonces el software de la unidad flash se ejecuta y el hacker está dentro.

Un problema común con los puertos USB es que la gente los utiliza para instalar software no autorizado en una computadora. Este software no reglamentado puede no solo causar problemas al sistema, sino que las empresas están obligadas por ley a comprar licencias de software para cualquier aplicación en sus computadoras – incluso si no lo saben. Afortunadamente, usted puede comprar seguros de puerto efectivos y económicos para evitar que los puertos USB sean utilizados. Estos seguros pueden ser violados pero contribuyen en mucho para hacer más lento el acceso al puerto. Usted también puede desactivar el USB en el nivel BIOS. Esto se puede invertir pero tiene la desventaja de ser una propuesta de todo o nada – elimina todos los puertos USB de manera que no puede usar teclados, ratones o impresoras conectadas por USB.

### **Otros puertos y unidades de entrada/salida**

Aunque los puertos USB son la manera más común de entrar ilegalmente a una computadora, no olvide que se pueden usar otros puertos en serie y en paralelo para entrar a una computadora. No son tan fáciles de usar como un puerto USB así que representan una amenaza menor aunque esto no significa que sean totalmente inocuos. Afortunadamente, tampoco se utilizan mucho actualmente y con frecuencia se pueden desactivar o eliminar por completo de una computadora sin que se les eche de menos.

Unidades de disco flexible, DVD, CD limitado. En estos tiempos donde todo está conectado en red, es fácil olvidar que los datos todavía pueden viajar dentro y fuera de una computadora personal y esto puede ser un medio efectivo para instalar software ilícito. Idealmente, una computadora personal segura no tiene unidades de medios removibles integrados en la misma. Si usted tiene unidades de disco y desea asegurarlos los seguros físicos para unidades de disco CD, DVD y flexible tienden a ser ineficaces así que es preferible utilizar software que requiera una contraseña para que se pueda tener acceso a la unidad de disco.

## Asegure sus dispositivos de entrada/salida

### Registadores de teclado

Un registrador de teclado es un pequeño dispositivo espía muy fácil de obtener (y muy latoso) que se instala entre un teclado y el CPU, este registra cada golpe de tecla hecha en ese teclado hasta dos millones de golpes de tecla – un año de escribir en el teclado para la mayoría de las personas. Un registrador de teclado registra todo lo que usted escriba, incluyendo contraseñas.

Un registrador de teclado no es penetrante y parece una protección común o tal vez un protector contra sobre corriente. No se requieren habilidades especiales para instalarlo y como no utiliza recursos del sistema, no es detectable excepto mediante la observación física del mismo detrás de la computadora. También asegúrese que los teclados utilizados en su organización sean los mismos que los teclados proporcionados porque existen registradores de teclado que se construyen integrados a los teclados.

### Considere prohibir dispositivos electrónicos portátiles

Son populares y su personal le odiará si los prohíbe, pero el hecho es que mucho de los dispositivos electrónicos pequeños actuales tales como reproductores MP3 como iPods, teléfonos celulares, cámaras digitales y PDAs contienen una gran cantidad de memoria y se pueden adaptar para succionar datos de una computadora a través de un puerto USB. Como con frecuencia un iPod se utiliza de esta manera, el nombre general para esta actividad en inglés es “podslurping” (extracción de datos a través de un iPod).

Si tiene datos muy confidenciales en sus computadoras y está extremadamente preocupado acerca de violaciones de seguridad, prohibir estos dispositivos portátiles es definitivamente algo que debe considerar en su plan de seguridad.

## Utilice cable de fibra óptica

Siempre que la seguridad sea un asunto de que preocuparse prefiera cable de fibra en lugar de cobre. La fibra no irradia señales y es extremadamente difícil de infringir. Si el cable es manipulado, es fácil descubrirlo porque el cable tiene fugas de luz y hace que todo el sistema falle. Si se hace un intento para infringir la seguridad de su sistema de fibra usted lo sabrá.

Además la fibra tiene otros beneficios que hacen que su instalación valga la pena. Como es inmune a interferencia EMI/RFI usted lo puede instalar en áreas eléctricamente “ruidosas”. Además, la fibra soporta mayores anchos de banda y distancias más largas que el cobre.

## Proteja datos

### Separe redes seguras de redes inseguras

Actualmente se da por hecho que la red interna de cualquier organización está conectada a la Internet. Sin embargo, incluso con el firewall más capaz una conexión de Internet nunca está totalmente segura.

Si su red contiene información muy confidencial tal como expedientes de pacientes, datos financieros corporativos o los planos más recientes para un bombardero secreto, una de las cosas más efectivas que usted puede hacer para conservar la privacidad es separarla físicamente de la Internet. Por supuesto que sus usuarios probablemente requerirán tener acceso a Internet y usted se lo puede proporcionar pero no en la misma red que contiene los datos confidenciales.

La manera más obvia para una persona accede a una red segura y a una insegura tal como la Internet es tener una computadora separada para cada red. Esta solución tiene a ser costosa pero es finalmente una solución muy segura porque los datos privilegiados nunca se encuentran en la computadora con la que se accede a Internet.

Una manera conveniente de tener dos CPUs separadas en el escritorio sin también tener que tener dos monitores, teclados y ratones por separado es usar un interruptor KVM para cambiar entre las CPUs. Como un interruptor KVM mantiene las CPUs completamente separadas, es imposible que un usuario transfiera información de una a la otra. Para instalaciones particularmente delicada, seleccione un interruptor KVM seguro que está blindado especialmente para que no haya ni la posibilidad más remota de que una señal eléctrica se fugue de una CPU a la otra.



Un ejemplo de un interruptor KVM: Black Box ServSwitch™ Secure (SW4007A).

Otra solución para tener acceso a dos redes separadas es tener un conmutador manual para permitirle a una sola computadora tener acceso a dos redes diferentes por turnos. Usted puede usar un conmutador de fibra o de cobre, pero la fibra se considera generalmente más segura (si usted requiere este nivel de seguridad debe usar fibra de todas maneras).



*Un ejemplo de un interruptor manual de red: Interruptor AB de Fibra Óptica Black Box (SW1002A).*

Esta solución no es tan segura como tener CPUs separadas para cada red, por el peligro de que un usuario deje un archivo delicado en su computadora mientras entra a Internet.

### **Mantenga la información confidencial fuera de las computadoras y otros dispositivos portátiles**

Con frecuencia nos enteramos en las noticias de que una computadora portátil que contenía información confidencial es robada o se pierde, y los datos personales de miles, millones de personas son diseminados. Usted pensaría que con historias como esta que se presentan en las noticias una o dos veces a la semana, las organizaciones pondrían atención y mantendrían los datos confidenciales fuera de las computadoras portátiles.

Sí, usted puede codificar computadoras portátiles y equiparlas con seguros de cadena, pero el hecho es que estos dispositivos portátiles están hechos para viajar y con frecuencia se pierden o son robados. Se olviden en taxis, los roban de los cuartos de hotel y en general desaparecen.

Establezca una política para minimizar los datos confidenciales que esté permitido tener en computadoras portátiles, permitiéndolo únicamente cuando sea absolutamente necesario y limitándolo a la cantidad más reducida de información con la que se pueda realizar el trabajo. Asegúrese que los datos estén bien codificados y elimínelos en cuanto ya no los necesite más.

No olvide que muchos otros dispositivos portátiles tales como teléfonos y PDA también son computadoras y pueden contener datos confidenciales.

#### Respaldo de datos

No importa que precauciones tome contra el daño a su equipo, los accidentes pueden suceder – sobre corrientes de energía, derrames, caídas, etc. Es imposible proteger contra cada escenario posible. El equipo se puede reemplazar pero los datos no. Establezca un plan integral para respaldar y archivar datos.

### **Proteja el equipo de daños accidentales**

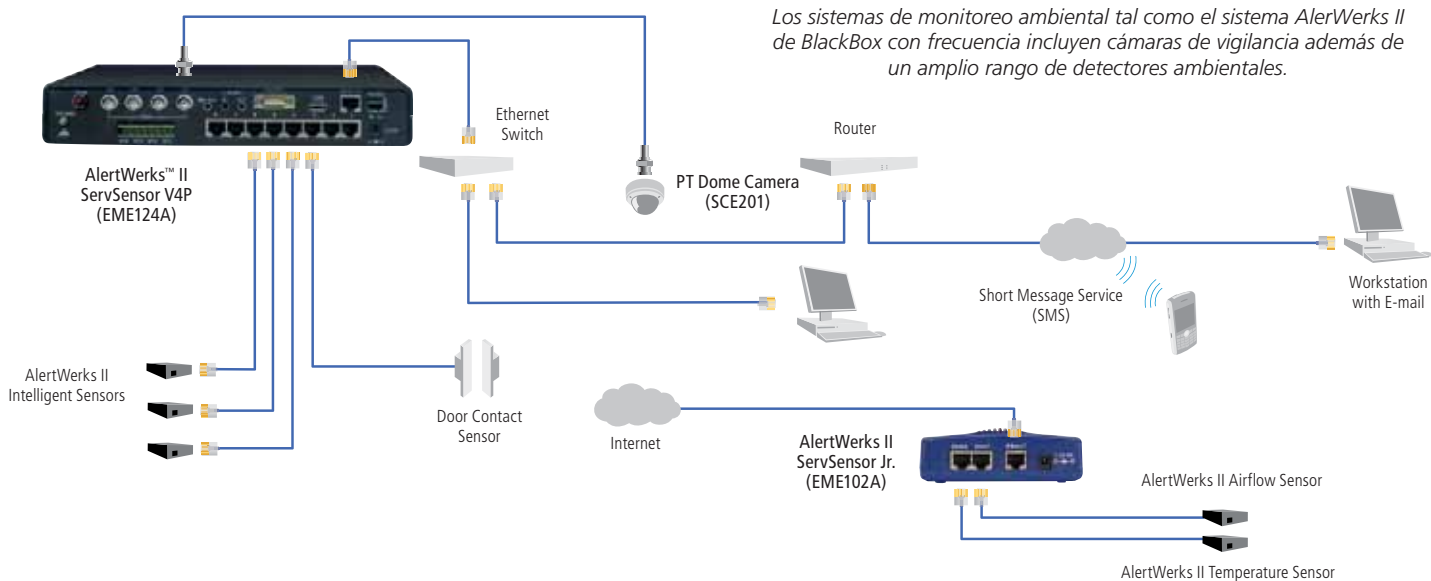
La seguridad de red significa no solo proteger la red contra el daño deliberado y malintencionado sino también protegerlo de daños accidentales por factores ambientales tales como calor, humedad, humo y excesos de corriente.

#### Monitoreo ambiental

Los dispositivos de red se pueden poner fuera de operación tan fácilmente por altas temperaturas como por un hacker. Parte del trabajo de proteger su red física es asegurar que los dispositivos de red se mantengan siempre en un ambiente seguro y bien regulado. Los factores ambientales son especialmente importantes cuando el equipo está instalado en ubicaciones remotas y no supervisadas.

Los productos de monitoreo ambiental le permiten monitorear activamente las condiciones en su bastidor, cuarto de servidores, centros de datos o en cualquier otra parte donde usted necesite proteger bienes especialmente valiosos. Las condiciones monitoreadas incluyen temperaturas extremas, humedad, picos y excesos de corriente, fugas de agua, humo y materiales químicos. Con un monitoreo ambiental adecuado usted está alerta de todas las condiciones que podrían tener un efecto adverso en su equipo esencial para su negocio. Los productos de monitoreo ambiental también le pueden alertar de un daño potencial por error humano, pirateo informático o dedos entrometidos. Muchos sistemas se pueden combinar con monitoreo de video para que pueda tener un ojo en su equipo y monitorear al mismo tiempo sus condiciones.

Los monitores ambientales consisten de tres elementos principales: una unidad base, sondas o detectores, así como conectividad e integración de red. Las unidades base pueden contener uno o más detectores integrados, así como puertos para conectar sondas externas. Adicionalmente, incluyen un puerto Ethernet y tienen software para producción de gráficos y configuración remota. Este software también puede funcionar con software de administración de red existente, tal como los sistemas SNMP.



## Protección contra sobre corriente y energía

Los dispositivos de red generalmente requieren un suministro constante y estable de 120 voltios de corriente alterna (VCA). Esta es la energía estándar proporcionada por las empresas públicas locales de suministro de energía. En general esta electricidad está disponible, limpia y confiable pero está sujeta a fluctuaciones. Demasiado voltaje (sobrecorriente y picos de corriente) o muy poco voltaje (fallas de energía y apagones) puede dañar su equipo o inutilizarlo temporalmente.

Los protectores contra sobrecorriente son dispositivos diseñados para proteger su equipo de sobre-voltajes que puedan dañar su delicado equipo electrónico. Los protectores contra sobrecorriente se deben instalar tanto en las líneas de datos como en las líneas de energía.

Prácticamente hablando, los protectores contra sobrecorriente no absorben ni disminuyen de ninguna otra manera los excesos de corriente dañinos. Su principal función es desviar estas fuerzas destructivas lejos de su delicado circuito. En caso de una sobrecorriente extremadamente grande, un protector contra sobrecorriente romperá el enlace a su hardware. Finalmente, los protectores contra sobrecorriente están diseñados para fallar, sacrificándose ellos mismos para proteger los dispositivos electrónicos.

Un protector contra sobrecorriente protege contra un exceso de energía, pero muchos problemas de energía se presentan como fallas de energía (voltaje bajo) o apagones (interrupción total de la energía) que pueden inutilizar o hacer fallar a su equipo. Un protector de suministro de energía ininterrumpible (UPS) protege sus sistemas contra condiciones de muy poca energía.

El que un servidor no funcione puede detener sus operaciones. Aunque la pérdida de un sólo switch o enrutador puede no detener totalmente a toda una empresa, puede ocasionar una productividad de cero para grupos de trabajo u oficinas remotas enteras.

Por una pequeña fracción del costo de su hardware de red usted puede adquirir un UPS para proteger su red de fallas de energía, apagones y sobrecorriente. Mantiene la energía fluyendo, dándole suficiente tiempo para apagar todo de manera segura durante un apagón. También regula su energía, suavizando sobre-voltajes u sub-voltajes, picos de corriente, sobrecorriente e impulsos peligrosos que generalmente pasan inadvertidos.



Un ejemplo de un protector de sobre-corriente de línea de datos: Protector de Sobre-Corriente Black Box CAT5 100BASE-TX (SP251A-R2).



Un ejemplo de un UPS: APC Smart-UPS XL (SUA3000RMXL3U).

### Maneje con cuidado lo inalámbrico

Lo inalámbrico es por propia naturaleza inseguro. Una red a base de cables requiere acceso a un cable o un puerto para entrar a una red, pero una red inalámbrica extiende su nube por todas partes y para todo aquel que tenga una computadora portátil o una PDA que se pueda conectar a la misma.

Sí, hay normas de codificación pero la verdad es que la codificación básica WEP sólo es marginalmente mejor que no tener ninguna seguridad y ya se tienen disponibles herramientas para infringir las WPA y WPA2 más avanzadas. Utilizar codificación para proteger su red inalámbrica mantendrá alejado al explorador casual, pero no hará mucho para detener a alguien que tenga la determinación para entrar a su red.

La única manera realmente segura de usar inalámbrico es usarlo únicamente en áreas sobre las cuales usted tenga el control físico total. En particular, vigile que su señal inalámbrica no llegue a un área pública o semi-pública tales como una banqueta o el vestíbulo de un edificio.

También tenga cuidado de los puntos de acceso no autorizado que sus usuarios hayan podido conectar a su red Ethernet por su propia comodidad. Los puntos de acceso no autorizado van desde una mera molestia hasta una amenaza de seguridad real en una red grande. Como es tan fácil para los usuarios conectarse en un punto de acceso, usted tiene que protegerse constantemente contra esto. Con únicamente un punto de acceso no protegido se puede tener un punto de entrada vulnerable para toda una red.

### No olvide la evidencia en papel

Las computadoras producen papel. Montones de papel. Esas pilas de impresiones desechadas en el bote de reciclado son el material ideal para un pepenador ambicioso. Si no quiere que lo vean, tritúrelo.

### El hueco de seguridad más vulnerable—los seres humanos

Nada de lo que haga para proteger su red le va a ayudar en algo si la gente en su organización mantiene felizmente las puertas abiertas para perfectos extraños, conecta dispositivos no autorizados como se les dé la gana y escriben sus contraseñas en notas adheribles o en los monitores de sus computadoras.

Un plan de seguridad completo incluye educar a su personal para que esté alerta de asuntos de seguridad física – en este campo usted desea que sean vigilantes y un tanto paranoicos.

### En conclusión

La seguridad física de la red es tan importante o más importante que la seguridad basada en software – una falla en la seguridad física puede nulificar rápidamente todo el trabajo hecho por el lado del software para proteger su red. Sin embargo, este aspecto de la seguridad generalmente no es tomado muy en cuenta o se planea deficientemente. Un plan de seguridad de red sólido incluye una revisión completa de seguridad física, incluyendo control de acceso, vigilancia, monitoreo de centro de datos y respaldo de datos.

### Acerca de Black Box

Black Box Network Services es un proveedor líder de soluciones de red que da servicio a 175,000 clientes en 141 países con 192 oficinas en todo el mundo. El catálogo y el sitio en la Red de Black Box ofrecen más de 118,000 productos que incluyen biometría, soluciones de acceso remoto, gabinetes, cable de fibra óptica y monitoreo ambiental. Su completa solución de monitoreo ambiental, AlertWerks II, protege el equipo de TI esencial para su negocio contra amenazas físicas de temperaturas extremas a daños ocasionados por agua y además ofrece una opción de video. Puede encontrar más información disponible en <http://www.blackbox.com/go/alertwerks> (revisar dónde lo pondremos en el sitio)

Black Box también ofrece un rango completo de productos de red que incluyen interruptores y convertidores, así como gabinetes, bastidores, cables, conectores, y otros productos para la infraestructura de audio, video y datos.

Black Box está reconocida como la compañía de servicios técnicos más grande del mundo dedicada a diseñar, construir y dar mantenimiento a los sistemas de infraestructura de voz y datos complejos de nuestros días.

© Copyright 2009. Derechos reservados. Black Box y el logotipo del Diamante doble "Double Diamond" son marcas registradas, e IntelliPass™, ServSwitch™, y AlertWerks™ son marcas registradas de BB Technologies, Inc. Cualquier marca registrada de terceros en este documento está reconocida como propiedad de sus respectivos propietarios.