

Encriptar información.

Por : Capacita TV

Fuente: <http://www.tlmsn.com.mx/tecnologia/tips/capacitativ/art003/>

El increíble crecimiento de Internet ha impulsado la creación de empresas con la promesa del cambio en la forma en que vivimos y trabajamos. Pero una preocupación primordial es acerca de la seguridad en Internet

Especialmente cuando se está manejando información confidencial.

Existe mucha información que no deseamos compartir en la Web tal como:

- **Información de nuestras tarjetas de crédito**
- **Correspondencia privada**
- **Información personal**
- **Información financiera**
- **Información crítica de la empresa**

La seguridad de la información que viaja por la red, se realiza a través de varios métodos. Uno de estos métodos para proteger la información es la de mantener la información importante en dispositivos de almacenamiento removibles. Pero el método más popular de seguridad en el cual todos confían es en el “Encriptamiento o cifrado”

Esto es el proceso de codificar la información de tal forma que sólo la persona o computadora que cuente con “la clave” pueda decodificarlos.

Los sistemas de cifrado, están basado en la ciencia de la “criptografía” que ha sido utilizada a través de la historia. Antes de la era digital, quienes utilizaban esta metodología eran los gobiernos, con propósitos militares principalmente.

La mayoría de los sistemas de cifrado de las computadoras pertenecen a dos categorías.

- **Cifrado de código simétrico**
- **Cifrado de código público**

Código simétrico: cada computadora cuenta con una llave secreta (código) que puede ser utilizada para encriptar – cifrar - un paquete de información antes de que sea enviado a través de la red hacia la otra computadora. Esto requiere conocer cuáles computadoras estarán enviándose información mutuamente y de esta forma instalar la “clave” en ambos equipos.

Código público: Utiliza una combinación de código público y privado, el código privado es conocido solamente por tu computadora, mientras que el código público lo otorga tu computadora a otro equipo que desee comunicarse de manera segura con tu equipo.

Para decodificar un mensaje cifrado, una computadora debe utilizar el código público que provee la computadora que lo originó.

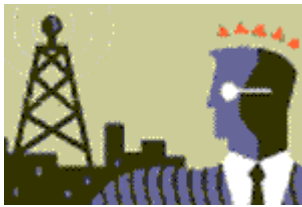
Autenticidad: Es otro proceso que se utiliza para confirmar que cierta información realmente fue originada por una fuente confiable. Para esto existen varias formas de dar autenticidad (algunos autores usan la palabra “autenticar”) a una persona o la información de una computadora. por ejemplo: contraseñas, cifrado digital o firma digital.

Conéctate sin cables

Por José Antonio Ramírez

Fuente: <http://www.tlmsn.com.mx/tecnologia/tips/red/>

Explota la nueva infraestructura en redes para ofrecerla a otros que requieran conectarse a la Web mediante el trabajo en equipo.



La idea es contar con la misma funcionalidad, enlaces y facilidad para compartir acceso a Internet, archivos, documentos, impresora y todo lo que utiliza una red de cómputo local con cables.

La diferencia es que con la tecnología inalámbrica tú puedes habilitar equipos de cómputo personales (conocidos como laptops o notebooks), sin la incomodidad del cableado extendido que exigen las redes tradicionales.

Este nuevo esquema de trabajo puede ser ideal para empresas, quizá como la tuya, que cuentan con cinco o diez empleados y rentan oficinas de manera provisional. Imagínate hacer lo mismo, pero con una red cableada, Olvídate de la incomodidad de trasladar cables, servidores y equipos de un lugar a otro.

La más utilizada

La tecnología inalámbrica que más se utiliza actualmente es conocida como Wi-Fi, la cual designa al estándar 802.11b que permite este tipo de enlaces. Una de sus virtudes es que permite a varios equipos PC compartir una sola conexión a Internet de alta velocidad a una distancia de 92 metros.

De igual manera el uso de redes inalámbricas locales, que los expertos en tecnología denominan Wireless Local Area Network o WLAN, son muy útiles para implementarse en edificios de difícil acceso, construcciones antiguas que en ocasiones se ven limitadas en espacio, al igual que edificios del patrimonio histórico a los que no se les puede hacer modificaciones.

Las redes inalámbrica también aprovechan aplicaciones ideales cuando se complementan con las redes cableadas, situadas en edificios distintos. Mediante enlaces de radio, una red cableada local aumenta su tamaño con la red inalámbrica. De igual manera, las redes inalámbricas son muy útiles cuando se viven situaciones de emergencia, por ejemplo, al dañarse el inmueble de trabajo, o cuando la red cableada se encuentra congestionada.

Cualquier lugar, incluyendo tu hogar, puede ser habilitado para trabajar con este tipo de red. Sólo basta con utilizar los equipos y accesorios necesarios para conectar tus computadoras.

Ventajas

Una de las ventajas de esta infraestructura es que puedes rentársela a hoteles, cafeterías, restaurantes,

plazas comerciales y lugares altamente concurridos. Dependiendo de las necesidades de los usuarios, puedes rentar el equipo por horas o días con tarifas que podrías definir, en principio, tomando como referencia los servicios de acceso a Internet que ofrecen los locales con redes cableadas.

Actualmente, la renta que los distintos cafés-Internet ofrecen en la ciudad de México oscila entre los 20 y 25 pesos por hora. Pero es necesario analizar algunos casos, como el hecho de que un hotel capitalino renta a sus clientes tarjetas PCI, por día, para que se conecten a Internet desde sus laptops, sin límite de minutos.

Si puedes ofrecer en tu negocio algo mejor o lo mismo, existen probabilidades de que el retorno de tu inversión ocurra en el corto plazo.

La facilidad de las redes inalámbricas para acceder a la Web son iguales a las de una red cableada, y las de una conexión individual, en la cual el servicio se contrata con un proveedor de acceso a Internet, con tarifas mensuales accesibles.

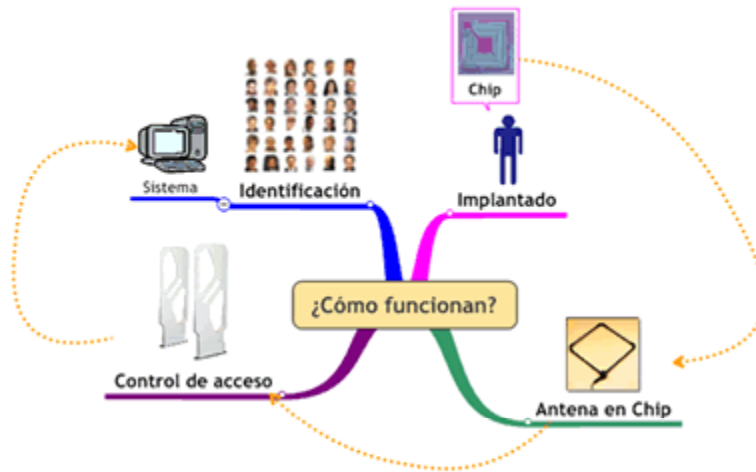
Chips en seres humanos - ¿Un escaparate Orwelliano?



Fuente: <http://www.1msn.com.mx/tecnologia/tips/capacitatetv/art002/>

La tecnología de Chips de Radio Frecuencia insertados en la piel puede salvar vidas. Estos beneficios podrían ser mucho mayores que las preocupaciones de perder la privacidad y vivir en un escaparate Orwelliano. Los promotores de esta tecnología dicen que los Chips de Identificación por Radio Frecuencia (RFID) colocados en la piel pueden reducir drásticamente el robo de identidades, ayudar a identificar víctimas de desastres y mejorar significativamente el cuidado de la salud.

Sus críticos más acérrimos dicen que estas tecnologías permitirían a los gobiernos el seguimiento de cada movimiento de las personas y por lo tanto la invasión de su privacidad y convertir el hábitat de las personas en un gigantesco escaparate Orwelliano. El abuso de la tecnología podría desvirtuarse en otras aplicaciones como la de identificar a potenciales compradores y atiborrarlos de ofertas, o identificar a personas que tengan cierta enfermedad e incurrir en discriminaciones.



El concepto de implantar chips para el seguimiento de seres vivos fue introducido hace más de una década, cuando los dueños de mascotas los comenzaron a utilizar para identificar a sus perros y gatos. Sin embargo su implantación en seres humanos no fue utilizada sino hasta septiembre 11 del 2001, cuando los bomberos marcaron sus brazos con sus nombres, para poder ser identificados en caso de que murieran tratando de rescatar gente.

Hoy en día existen varios tipos de chips para insertarse en seres humanos; algunos dedicados a la identificación y otros que pueden contener información vital de personas enfermas como contraindicaciones, tratamientos de emergencia en caso de infartos, etc. Una de las aplicaciones más valiosas podría ser para combatir secuestros. Aunque la tecnología RFID no permite dar un seguimiento tan estrecho como el GPS (Sistema posicionador por satélite), si permite identificar cuando la persona ha pasado determinado punto de control. **El uso y difusión de esta tecnología a futuro dependerá de la disponibilidad de políticas estrictas en cuanto a la invasión de la privacidad** y de la generación de estándares para cada tipo de aplicación. Hoy en día ya se usan en cárceles para identificar a reos y se sabe que algunos hombres de negocios mexicanos se han mandado implantar los chips en sus brazos como protección potencial en caso de un secuestro.