

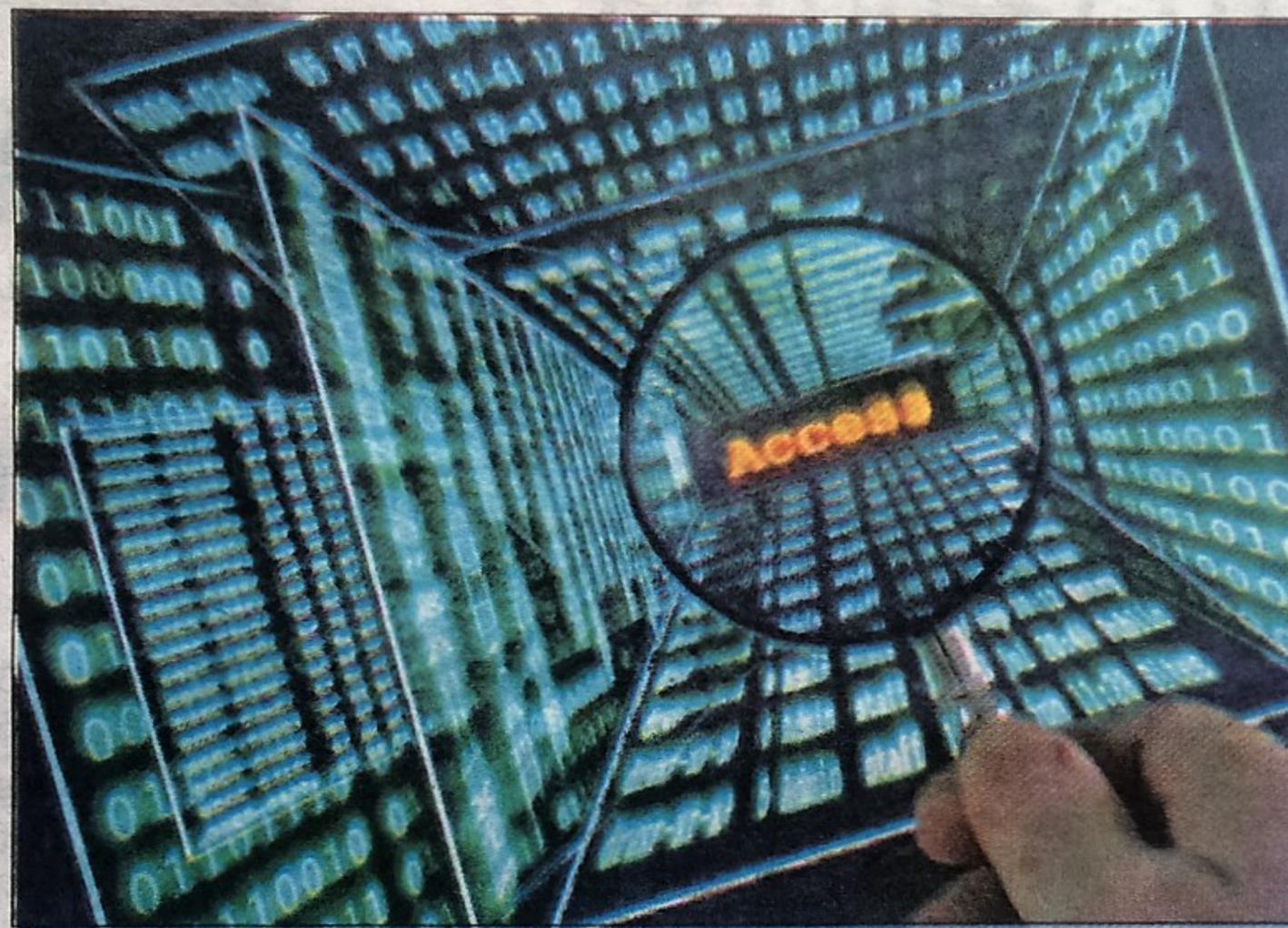
# Top cuatro de las ciberamenazas del año

CON MOTIVO del Encuentro de expertos en ciberseguridad inteligente, que se realizará el 14 de este mes en Bogotá y que está dirigido a los directivos de las grandes compañías del país para que aprendan a blindarse frente a los delitos cibernéticos, Entelgy, consultora IT española, ha realizado un análisis de las tendencias en ciberataques para este 2016.

**1 La nube:** El almacenamiento de datos e información en la nube (cloud computing) es una tendencia en auge y por ello los ciberdelincuentes están mejorando las técnicas para conseguir información de las víctimas a través de malware.

**Consejo:** Establezca contraseñas con números, caracteres y letras y no olvide cerrar siempre la sesión cada vez que accedas a servicios en la nube.

**2 Ramsonware:** El atacante restringe el acceso a archi-



vos y partes del sistema, que son desbloqueados a cambio de una cantidad económica.

**Consejo:** Mantenga siempre el software de tu equipo y el antivirus actualizado. Evite la descarga y apertura de archivos o correos electrónicos sospechosos y activa la extensión de los

mismos para identificarlos que, de forma engañosa, acaban con el clásico ejecutable ".exe".

**3 Dispositivos móviles:** Cada vez pasamos más tiempo con el móvil en Internet y lo utilizamos para más cosas. El concepto BYOD hace referencia

a la expansión del uso del móvil personal en el entorno de la empresa. El foco de los ciberataques se está centrando cada vez más en móviles y tablets.

**Consejo:** Piense en lo que puede suceder si pierdes el móvil y no tienes habilitada ninguna clave de entrada. Cualquiera tendrá acceso a todo lo que guardas en él: redes sociales, mensajería, documentos, WhatsApp.

**4 Waterhole:** es un ataque que redirige a la víctima a una web que imita a otra lícita (de un banco, operador de telefonía móvil y policía, con el objetivo de extraer información con la que realizar operaciones fraudulentas).

**Consejo:** Adoptar soluciones antispam, ya que muchos ataques de Spear-Phishing se inician a través de la recepción de un correo electrónico fraudulento. Analice bien cada correo que llegue y descarte abrirlo si detecta algo anómalo.