

## »Empresas &amp; sectores.



Enrique Salem, consejero delegado de Symantec. /EDU BAYER

## ENRIQUE SALEM

Consejero delegado de Symantec

## “El fraude corporativo interno es imposible de eliminar”

## MANUEL ÁNGEL-MÉNDEZ

“Con un poco de ambición y mucho sudor de la frente”. Así resume Enrique Salem, mitad en inglés, mitad en castellano, el salto desde su ciudad natal caribeña, Barranquilla (Colombia), a lo más alto del sector tecnológico en Silicon Valley (California). A sus 44 años, es el único directivo hispano al frente de una de las grandes corporaciones americanas, Symantec, el mayor fabricante mundial de *software* de seguridad por facturación y capitalización bursátil. Más de cien millones de consumidores y miles de empresas utilizan su programa Norton para protegerse de virus, *spam* y estafas informáticas. Aun así, las amenazas virtuales crecen desorbitadamente año tras año, un 165% en 2008. El cibercrimen es un negocio redondo, pero también combatirlo. Por eso muchos reprochan a las compañías de antivirus su escasa efectividad. “Invertimos lo que sea necesario para eliminar el problema”, dice Salem. En el año fiscal 2009, Symantec aumentó un 5% sus ingresos, hasta los 6.200 millones de dólares, y un 17% el beneficio.

**Pregunta.** España es el cuarto país del mundo con más ordenadores infectados (62%), tras Taiwan, Rusia y China. ¿Cómo es posible?

**Respuesta.** Depende de la in-

fraestructura tecnológica, de la penetración de la banda ancha y de si operan grandes proveedores de acceso a Internet. Telefónica domina en España. No es que tengan la culpa, pero los *hackers* optan por países con grandes operadoras. Son un objetivo más fácil.

**P.** ¿Echa en falta mayor colaboración de gobiernos y proveedores de acceso a Internet para atacar problemas como el *spam*?

**R.** Los gobiernos tendrían que

“Mantenemos el gasto en I+D siempre en el entorno del 14% de los ingresos”

“Microsoft no ha tenido éxito con su programa gratuito de seguridad”

colaborar más entre sí. Quien lanza un ataque, lo puede hacer simultáneamente en varios países. Las operadoras lo tienen más difícil. Es muy complejo técnicamente saber quién envía *e-mails* infectados e instalar sistemas de filtros en la Red.

**P.** ¿De qué forma se están sofisticando los ataques informáticos?

**R.** Son mucho más selectivos. Antes se enviaban en masa, ahora se dirigen a personas y compañías concretas. Por ejemplo, si una empresa compra a otra, los cibercriminales enviarán un *e-mail* con algún enlace, haciéndose pasar por un organismo del Gobierno para preguntar por la operación de compra. Ese *e-mail* acaba circulando internamente, alguien hace clic en el enlace y se descarga un programa infectado.

**P.** Directivos de su sector reconocen que las empresas de seguridad deberían ser más efectivas, ir por delante del cibercrimen y no a remolque. ¿Falta voluntad?

**R.** No, en absoluto. Invertimos cualquier cantidad necesaria para eliminar el problema. Hasta ahora veíamos un ataque y luego ofrecíamos la solución. Ese modelo no funciona. Por eso hemos creado un nuevo concepto, analizar programas basándose en su reputación: cuándo fueron creados, número de personas que los utilizan... Si la reputación no es satisfactoria, se bloquea.

**P.** Sin embargo, han reducido en dos años su gasto en I+D del 17% al 14% de los ingresos, cuando éstos han subido un 18%. ¿No les debilita este recorte?

**R.** Siempre mantenemos el gasto en I+D alrededor del 14%. Si a veces sube o baja es por el impacto de las adquisiciones de compañías. No queremos estar ni más

altos ni más bajos del 14% de los ingresos.

**P.** ¿Cómo ha aumentado la crisis económica el riesgo de amenazas informáticas?

**R.** El riesgo es que muchos trabajadores han sido despedidos. Cuando la gente se va, el 59% se lleva información confidencial. En realidad es un robo. Menos del 10% de firmas controlan dónde se guarda esa información y quién tiene acceso a ella.

“Actualmente, el 59% de los despedidos se lleva información confidencial”

“El 90% de las firmas no controla dónde guarda información ni el acceso a ella”

**P.** ¿Se puede evitar este tipo de fraude interno, como el que le costó 4.900 millones de euros a Société Générale el año pasado cometido por un empleado?

**R.** Es inevitable. El fraude corporativo interno se puede reducir y gestionar, pero es imposible de eliminar. Se necesitan regulaciones, tecnología y concienciación

por parte de los directivos. Es muy difícil que se cumplan estas tres condiciones a la vez.

**P.** ¿Les beneficia entonces la actual recesión? Sus ingresos y beneficios aumentaron en 2009.

**R.** La seguridad informática es anticíclica. Es como ir al médico, no es opcional ni prescindible. Tenemos más de 2.000 millones de dólares en caja y el nivel de deuda es bajo. Además, entre un 60% y un 70% de nuestros ingresos anuales son recurrentes. Estamos bien preparados.

**P.** ¿Se ha tocado fondo, ve una recuperación del gasto tecnológico de consumidores y empresas?

**R.** Creo que sí. Aunque es complicado predecir qué ocurrirá en 2010. Las grandes corporaciones han reducido un 9% su presupuesto de tecnología en 2009. El año que viene tal vez veremos crecimientos planos inferiores al 1%.

**P.** Los analistas han mostrado cierta inquietud por su cuota de mercado en el segmento corporativo. Sólo tienen el 22% del mercado mundial, frente al 11% de McAfee, que gana terreno.

**R.** Éste es un objetivo estratégico. McAfee ha crecido un poco más, pero el 51% del mercado está en manos de pequeños proveedores. Queremos evolucionar al mismo ritmo, o mejor, que el mercado, no importa si ganamos cuota a expensas de unos u otros.

**P.** Han adquirido más de treinta organizaciones desde 1999, seis en 2008 y sólo una este año. ¿Seguirán comprando en 2010?

**R.** No tenemos prisa. Ahora estamos centrados en integrar las adquisiciones. Nos podemos permitir ser pacientes, especialmente ahora que las valoraciones aún no se han ajustado. Nos interesan áreas como movilidad y *software* como servicio.

**P.** En el segmento de consumidores tienen más del 50% de cuota. Hace poco describió la situación como: “Symantec y los siete enanitos”, en referencia a sus competidores. ¿Sigue pensando igual?

**R.** Sí, claro que sí [risas]. Pero más importante incluso que la cuota son los análisis que hacen de nuestros productos, especialmente Norton. Obtenemos críticas muy positivas.

**P.** ¿No le preocupa que cada vez más personas se descarguen antivirus gratuitos de Internet? Incluso Microsoft acaba de estrenar su propio programa gratis (Microsoft Security Essentials).

**R.** Microsoft no ha tenido éxito en seguridad. El mercado no le ha aceptado. Y la gente sabe que un programa gratuito probablemente no le va a poder proteger por completo. Menos del 25% de personas utiliza estos productos.

**P.** Cada vez compartimos más información personal en redes sociales y *blogs*, pero la seguridad no parece mejorar. Facebook y Hotmail perdieron miles de contraseñas recientemente. ¿Qué aconseja?

**R.** Pedagogía, conocer cuáles son las amenazas y ser cuidadoso. Hay un problema de confianza en las aplicaciones de Internet. La gente no quiere depender de Facebook o Hotmail para proveerles seguridad. No confía en que sean capaces de hacerlo. Ése es nuestro trabajo. No importa el canal, Gmail, Hotmail... Importa el programa de protección. ■