Instituto Nacional
de Tecnologías
de la Comunicación

DIAGNÓSTICO SOBRE EL ESTADO DE LA SEGURIDAD EN LAS PYMES ESPAÑOLAS

Pablo Pérez San-José
Gerente del Observatorio de la Seguridad de la Información
Instituto Nacional de Tecnologías de la Comunicación (INTECO)

En la actualidad hay un consenso casi generalizado en torno a que el desarrollo de cualquier tipo de negocio y el uso de las tecnologías de la información no son hechos aislados y por lo tanto precisan interacción. De hecho, a lo largo de los últimos años el uso de las tecnologías se ha convertido en un importante factor de dinamización del crecimiento económico basado en el aumento de la competitividad y la productividad.

El motor principal de la economía y de la generación de empleo de España está centrado en la pequeña y mediana empresa, cuyo volumen equivale al 99,3% del total del tejido empresarial. Más aún, de los más de tres millones de empresas existentes en España, cerca del 94% son micropymes, es decir, organizaciones con menos de 10 empleados o sin asalariados en plantilla.[1]

Por ello, las iniciativas destinadas a impulsar y facilitar el acceso a las tecnologías de la información por la empresa española necesariamente deben orientarse hacia la PYME, y especialmente, aquellas dirigidas a fomentar un uso seguro de las TIC y la confianza en la Sociedad de la Información.

Situación de tecnológica y de seguridad de la PYME

La pequeña y mediana empresa española se caracteriza por una falta de homogeneidad tecnológica. Claro ejemplo de ello es la implantación de las TIC en estas organizaciones; mientras que más del 98% de las pequeñas y medianas disponen de al menos un ordenador, esta cifra se reduce al 60% en las microempresas. Esta falta de madurez en el uso de las tecnologías de la información se refuerza al observar la brecha existente en el porcentaje de empresas con conexión a Internet (superior al 90% en aquellas y apenas un 45% en las micropymes) o la utilización del correo electrónico (del 93% y 42% respectivamente).[2]

Ahondando en el campo específico de la seguridad informática, podría decirse que en estos momentos no se percibe por la PYME como un aspecto relevante que impida un acercamiento efectivo a la tecnología. Existe, no obstante, un cierto escepticismo sobre

[1] *Directorio Central de Empresas*. Instituto Nacional de Estadística (2006)

[2] Encuesta de Uso de TIC y el Comercio Electrónico. INE (2007)

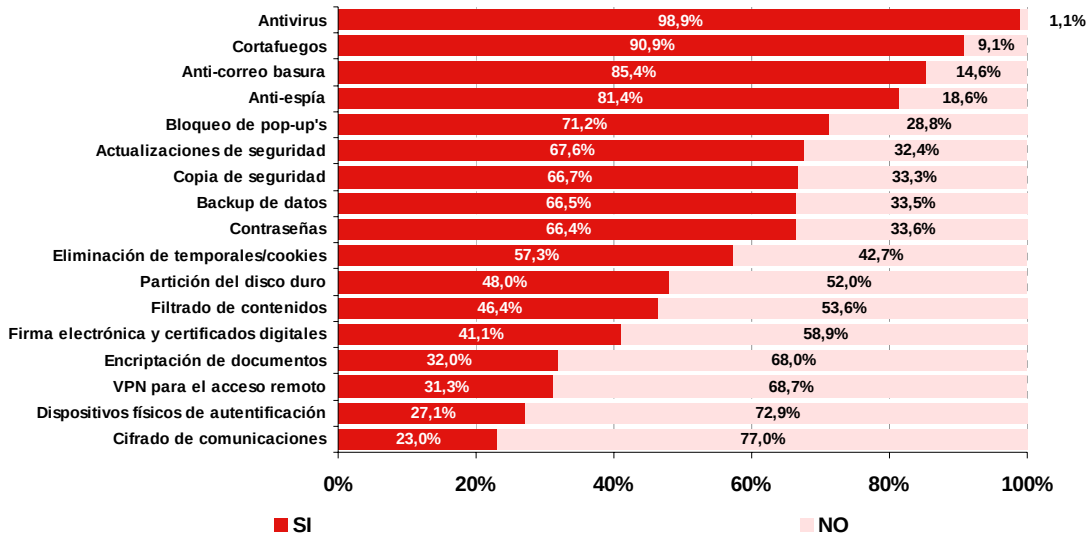
las medidas de protección existentes en la actualidad y se percibe el riesgo tecnológico como algo tangencial y de bajo impacto en el negocio.

Cuando se profundiza en el análisis de las respuestas de las Pymes obtenidas los estudios[3] llevados a cabo por el Observatorio de la Seguridad de la Información, se percibe que existe una carencia de conocimientos específicos de los problemas existentes y de las soluciones disponibles, especialmente en los aspectos más alejados de los conceptos clásicos de protección asociados al uso de Internet. Este hecho provoca una baja demanda de soluciones y servicios de seguridad que tradicionalmente han sido aplicados en la gran empresa, tales como soluciones de *backup*, cifrado o asesoramiento legal para el cumplimiento normativo.

La falta de recursos de las pymes en comparación con las grandes empresas agrava esta situación, lo que pone de manifiesto, cada vez más, la necesidad de iniciativas desde la propia industria como desde la Administración que ayuden a romper las barreras de entrada existentes y que influyan eficazmente en la cultura y el comportamiento de la PYME desde el punto de vista de la seguridad informática.

Si bien a lo largo de los últimos años se ha generado un importante mercado de seguridad de la información con productos y servicios orientados a la gran empresa española, se ha detectado una carencia a este respecto en la pequeña y mediana empresa.[4]

Gráfico 1: Medidas de seguridad empleadas



Fuente: INTECO

[3] Estudio sobre incidencias y necesidades de seguridad en las pequeñas y medianas empresas españolas. INTECO (2008) Disponible en http://observatorio.inteco.es

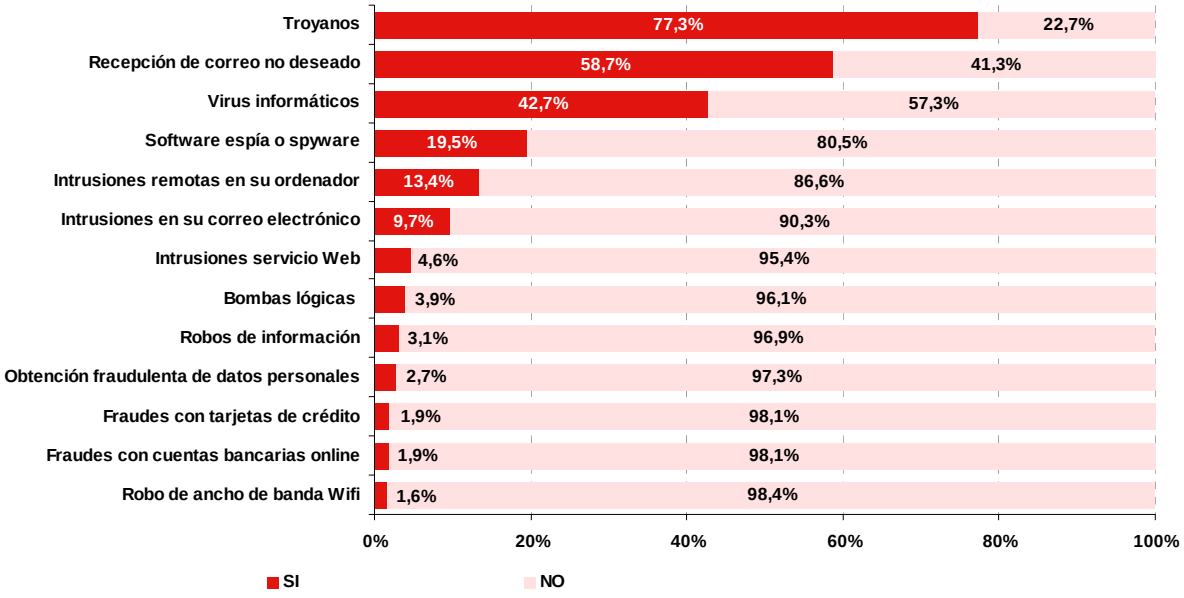
[4] Estudio sobre el Sector de la Seguridad TIC en España. INTECO (2008).Disponible en http://observatorio.inteco.es

En relación con las soluciones técnicas y políticas de seguridad que disponen las pymes españolas, destaca el grado de implantación que tienen las herramientas asociadas a la protección de la navegación en Internet: antivirus (98,9%), cortafuegos (90,9%), *antispam* (85,4%) y antiespías (81,4%). En cambio, las medidas de control en torno al cumplimiento normativo, las copias de seguridad de los datos, la seguridad en el acceso remoto, la continuidad del negocio o el cifrado de las comunicaciones siguen siendo poco conocidas y adoptadas entre las pymes.

¿Qué incidentes de seguridad tienen las pymes?

Aunque tanto las grandes empresas como las pymes están expuestas a un riesgo similar y a pesar de que las pymes tengan implantadas unas herramientas y políticas de seguridad más limitadas, como hemos visto, paradójicamente éstas perciben las incidencias de seguridad que les suceden como menos frecuentes y menos graves. Así, afirman que detectan un menor porcentaje de malware, que reciben menos spam, que sufren menos robos de información, menos intentos de fraude, etc que lo que declaran las grandes empresas.[5].

Gráfico 2: Incidencias de seguridad declaradas por las pymes (%)



Fuente: INTECO

Sin embargo, la auditoría de sus sistemas y el análisis de las incidencias reales (no las que son percibidas) nos conducen a la conclusión opuesta. La explicación es que el desconocimiento, la falta de concienciación y de formación, les impide reconocer o les

[5] Por ejemplo, declaran recibir spam el 80,4% de las grandes empresas, frente al 58,7% de las pymes, y haber sufrido robos de información el 12,8% de las grandes empresas frente al 3,1% de las pymes. Fuente: INTECO en colaboración con el Barómetro de Empresas El País- Deloitte.

hace confundir entre sí las incidencias de seguridad que realmente les suceden y no les permite valorar adecuadamente las consecuencias de las mismas para sus sistemas y para su negocio. Todo ello fomenta una falsa sensación de seguridad y que, por tanto, se genere una menor necesidad de protección.

Las pymes depositan toda su confianza en las herramientas informáticas de protección básica, descuidando otros hábitos y medidas de seguridad. Las herramientas son necesarias pero no son suficientes; además, son necesarias buenas prácticas.

En efecto, la seguridad no es sólo cuestión de tecnologías, sino también de personas. Así, la actitud y los hábitos de los usuarios son fundamentales, pudiéndose mermar la protección alcanzada con las herramientas cuando no se toman otras medidas adecuadas, tales como actualización de las aplicaciones y sistemas operativos para evitar vulnerabilidades, copias de seguridad, uso responsable y prudente del correo electrónico y la descarga de ficheros, etc.[6].

No se debe descuidar la actitud de los propios empleados como fuente de problemas de seguridad – malintencionados o no – para la empresa, ya sea por una falta de concienciación respecto a un uso responsable de los sistemas (política de contraseñas, bloqueo de ordenadores, etc.), o porque la propia falta de conocimiento hace que los trabajadores sean más vulnerables a ataques relacionados con la ingeniería social. Esta situación se constata como uno de los principales riesgos en la PYME.[7]

Posiblemente por esta falta de buenas prácticas, las pymes han puesto de manifiesto una alta frecuencia de incidencias relacionadas con el *malware* (virus, gusanos, troyanos y similares), aún debiendo a priori ser controlables mediante software de seguridad que afirmar tener instalado[8].

Por otro lado, desde el punto de vista de una pyme – que cuenta al menos con ciertos servicios básicos de tecnologías de la información, como el acceso a Internet y el correo electrónico – una amenaza importante es el correo electrónico no deseado (*spam*). Este, además de ser una vía de entrada de amenazas como ataques de malware e intentos de fraude, puede crear incomodidades que lleguen a interrumpir la actividad normal de trabajo y ocasionar con ello pérdidas económicas. Es destacable que las pymes declaren que esta incidencia ha manifestado de manera elevada (58,7%) durante el último año en sus sistemas.

---

[6] 1ª Oleada del Estudio sobre la Seguridad de la Información y e-Confianza de los hogares españoles. INTECO (2007) Disponible en: http://observatorio.inteco.es

[7] Por ejemplo, el 62% de las fugas de información en la empresa se deben a errores de los trabajadores y no a ataques deliberados.

[8] Recordemos que más del 90% declaran tener antivirus y cortafuegos instalados en los sistemas de sus empresas.

Finalmente, es especialmente relevante la falta de cumplimiento normativo en lo relativo a la seguridad de la información por parte de las pequeñas y medianas empresas españolas (LOPD[9], RDLOPD; LSSI[10], etc).

La inmensa mayoría de las pymes afirma conocer la normativa sobre protección de datos (LOPD y RDLOPD) y un 78% de ellas maneja ficheros automatizados con datos de carácter personal. Sin embargo, apenas un 16% de las pymes los han inscrito en el Registro de la Agencia Española de Protección de Datos, lo cual es una obligación que marca la ley para todo fichero con independencia del nivel de los datos que contenga y cuya infracción es sancionable[11].

Por otra parte, el recientemente aprobado RDLOPD – que supone la extensión de las preexistentes obligaciones también a los ficheros no automatizados – se atisba como un auténtico reto para la PYME. Especialmente cuando en el 96% de ellas existen ficheros en soporte papel con datos de carácter personal. En este sentido, en el momento de su entrada en vigor solo un 21% valora internamente procedimientos de tratamiento, almacenamiento, protección y destrucción de los mismos, y apenas el 12% cuenta con mecanismos de control de la copia y reproducción de documentos.[12]

Respecto al cumplimiento de las obligaciones derivadas de la LSSI el panorama no es más halagüeño ya que el 71,4% de las pequeñas y medianas empresas españolas afirma desconocerlas.

Consecuencias de los incidentes de seguridad

En general, las pymes dan poca importancia a las consecuencias que sobre su negocio tienen los incidentes de seguridad que les acontecen y, la mayoría de las veces, no los asocian a pérdidas económicas y no monetizan ni los trastornos sufridos ni su coste de oportunidad[13]. Este hecho se ve agravado por la falta de concienciación de aquellas empresas que no han previsto revertir posibles pérdidas de información mediante una adecuada política de copias de respaldo de los datos sensibles para su negocio – una de cada tres –.

---

[9] Ley Orgánica, 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal. Tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar.

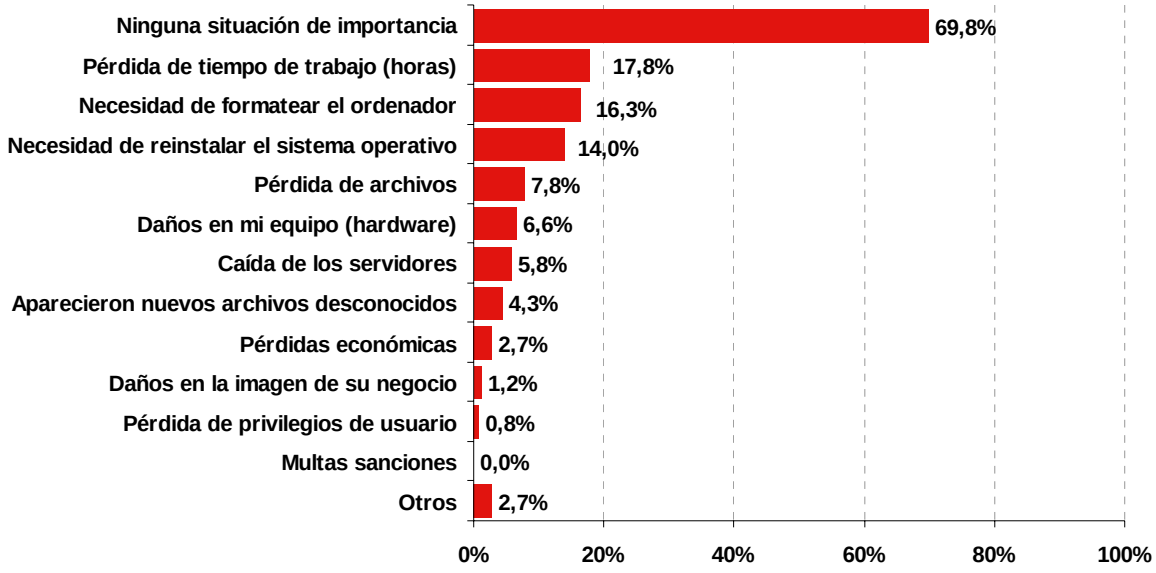
[10] Ley de Servicios de la Sociedad de Información y Comercio Electrónico: La Ley se aplica a todas las actividades que se realicen por medios electrónicos y tengan carácter comercial o persigan un fin económico. La Ley se aplica tanto a las páginas web en las que se realicen actividades de comercio electrónico como a aquéllas que suministren información u ofrezcan servicios de forma gratuita para los usuarios, cuando constituyan una actividad económica para su titular.

[11] Estudio sobre el grado de adaptación de las Pequeñas y Medianas Empresas españolas a la Ley Orgánica de Protección de Datos (LOPD) y el nuevo Reglamento de Desarrollo (RDLOPD). INTECO (2008). Disponible en http://observatorio.inteco.es

[12] Estudio sobre el grado de adaptación de las Pequeñas y Medianas Empresas españolas a la Ley Orgánica de Protección de Datos (LOPD) y el nuevo Reglamento de Desarrollo (RDLOPD). INTECO (2008).

[13] Un 91,3% de las pymes considera no haber sufrido una pérdida económica a causa de una incidencia de seguridad.

Gráfico 3: Consecuencias de las incidencias de seguridad



Fuente: INTECO

Otras consecuencias, como el impacto en la imagen de la empresa, las responsabilidades contractuales o las sanciones legales apenas han sido advertidas por las pymes entrevistadas.

Todo ello hace que, tras verse afectadas por una incidencia, el 85% de las pymes declare que no ha realizado ningún cambio o mejora en sus sistemas de protección ni en sus hábitos de seguridad.

Una oportunidad para la industria, un reto para la Administración

Si existe una característica común a todas las pequeñas y medianas empresas españolas, es precisamente su heterogeneidad, que implica unas necesidades específicas según el tamaño, madurez y sector de actividad de cada de ellas. No obstante, como hemos visto, existen dos carencias comunes a todas ellas que explican su escasa demanda. En primer lugar, el coste de ciertas soluciones existentes en el mercado les resulta poco asequible para sus recursos limitados. La segunda alude a la ausencia de la formación adecuada que en muchos casos les hace acudir al mercado "a ciegas" en busca de soluciones que en ocasiones resultan no concuerdan con sus necesidades.

Con la finalidad de ofrecer una respuesta a estas demandas detectadas, desde el Observatorio de la Seguridad de la Información de INTECO se han identificado una serie de medidas y recomendaciones dirigidas tanto a la industria como a las administraciones públicas.

Por una parte, aquellas destinadas a la **industria** y que implican necesariamente el acercamiento de las soluciones de seguridad a las pequeñas empresas mediante el diseño una política de precios atractivos y poniendo a su disposición profesionales expertos que les asesoren en la implantación de las medidas de protección más adecuadas para su negocio y les ofrezcan un soporte técnico post-venta. Además, es conveniente una adaptación de los productos y servicios ofertados siguiendo criterios de homogeneización, integración y simplificación. Del mismo modo, han de darse a conocer entre las pymes los servicios de seguridad gestionada, que permitan a estas empresas delegar en proveedores tecnológicos de confianza la gestión integral de la seguridad de sus redes y equipos y así obtener importantes ventajas fruto de la especialización, la optimización del servicio y la reducción de costes.

Por otra parte, es un aspecto de común acuerdo que en todo este proceso de adaptación de las empresas al uso seguro de las tecnologías y el fomento de una cultura de seguridad las **administraciones públicas** juegan un papel fundamental. En este sentido, son muchas las iniciativas puestas en marcha por la Administración con el objetivo de mejorar el acceso a las TIC por parte de la pequeña y mediana empresa, especialmente desde la perspectiva de la seguridad y la confianza en las nuevas tecnologías.

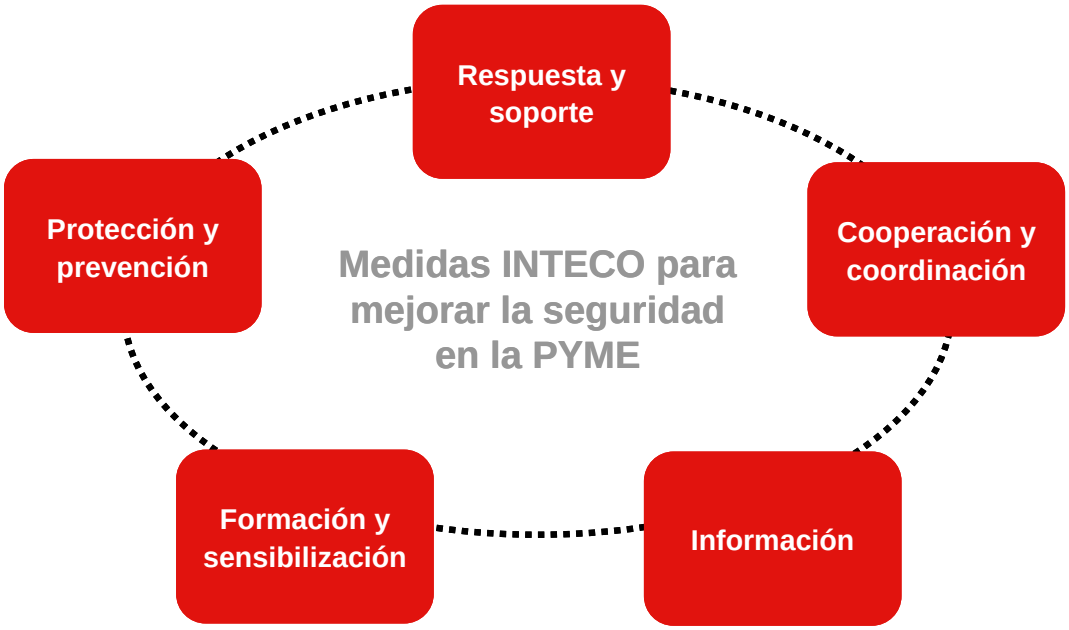
Una de ellas ha sido la puesta en marcha, a través del Instituto Nacional de Tecnologías de la Comunicación (INTECO), de diferentes proyectos enmarcados en la estrategia del Gobierno contenida en el Plan Avanza. Así, actualmente INTECO dentro de su línea estratégica de actuación en materia de *seguridad tecnológica*, ofrece servicios orientados al fomento y uso de soluciones de seguridad, la formación y la difusión de la cultura de la seguridad en las pequeñas y medianas empresas, a través de:

- Centro de Respuesta a Incidentes en Tecnologías Información para Pymes y Ciudadanos: INTECO-CERT
- Centro Demostrador de Seguridad para la PYME
- Observatorio de la Seguridad de la Información

Todos estos pueden agruparse en: servicios de protección y prevención[14], servicios de respuesta y soporte[15], servicios de cooperación y coordinación con otras entidades, servicios de concienciación y formación[16] y servicios de información[17].

[14] Catálogo y desarrollo de herramientas y útiles de seguridad gratuitos y un catálogo de actualizaciones de software para sistemas operativos y aplicaciones. Así como, una eed distribuida de más de 150 sensores (administraciones, empresas, red académica) analizándose diariamente más de 130 millones de correos electrónicos, 35 millones spam y 8 millones de direcciones IP.

[15] Recepción, gestión y soporte ante incidentes de seguridad; recepción, coordinación y respuesta a casos de fraude electrónico; laboratorio de análisis de malware; asesoría legal.



Dentro de estos últimos, se enmarca el *Estudio sobre incidencias y necesidades de seguridad en las pequeñas y medianas empresas españolas*, realizado por el Observatorio y cuyos resultados han permitido llevar a cabo este diagnóstico sobre la situación de la PYME española en materia de e-confianza y seguridad de la información.

[16] Campañas de divulgación y contribuciones en prensa escrita, radio y televisión; jornadas y talleres formativos.

[17] Catálogo de productos, soluciones y servicios ofrecidos por empresas de seguridad; boletines, alertas y avisos de seguridad; estudios, manuales y guías; bases de datos de estadísticas e indicadores; información de actualidad, noticias y eventos de relevancia.; avisos sobre nuevos virus, vulnerabilidades y fraude.