En un mundo hiperconectado y dominado por la inmediatez solo se mantienen fronteras físicas. En el ámbito de lo digital no existen tales fronteras y para bien o para mal, toda ventaja y todo problema se hacen globales.

El desarrollo de las tecnologías de la información y la comunicación que forman parte inexcusable de nuestra vida cotidiana, ha generado un nuevo espacio de relación donde la rapidez y facilidad de los intercambios de datos e ideas han eliminado las barreras de distancia y tiempo.

El ciberespacio ha eliminado esas fronteras y ha ampliado mercados, convirtiendo en realidad la idea de globalización, generando nuevas oportunidades, pero también riesgos y amenazas.

El pasado viernes 12 mayo "ciberataque" se convirtió durante horas y casi durante días, en la palabra más pronunciada y escrita, mientas la idea de catástrofe global se extendía para que, finalmente, en realidad se redujese a la categoría de alarma.

El ciberataque empezó a percibirse como masivo a partir de media mañana y en poco tiempo estaban afectados más de 200.000 usuarios en 170 países en los cinco continentes. El virus WannaCry (ransomware) secuestraba los archivos informativos y pedía un rescate en bitcoins a cambio de liberarlos.

El ciberataque tuvo unas dimensiones nunca antes conocidas y finalmente, de un modo casual y sin contribución inicial de especialistas se descubrió la solución, que pudo pararse, tras la aplicación de protocolos de seguridad, con mínimos daños frente a lo que cupo esperar en un principio.

Sin embargo, el ataque ha servido para poner más de relieve, si cabe, la importancia de ciberseguridad en todos los ámbitos y muy especialmente en las empresas cuyo núcleo de actividad depende cada vez en mayor medida, sino ya totalmente, de lo digital. Porque sucesos de este tipo van a volver a repetirse y la dimensión de sus efectos dependerá de la protección que se consiga frente a ellos.

El coste anual de los ataques informáticos supera anualmente en más de 400.000 millones de euros entodo el mundo y la inversión global en ciberseguridad deberá crecera un ritmo mínimo del 7 por ciento anual para al menos mantener el nivel de seguridad actual.

Probablemente, la ciberseguridad está ya en podio de los grandes desafíos de las empresas para las próximas décadas, junto con la energía, la robótica o la protección medioambiental.

La transformación digital plantea mayores retos y amenazas a medida que se acrecienta la interconexión de personas, el flujo de información y el número de dispositivos interconectados, que alcanza cada vez a más ámbitos con el Internet de las Cosas. (IoT), aplicaciones globales y extensísimas redes de información y colaboración.

Ese reto, a la vez básico y crítico, de la ciberseguridad se centra en la prevención, en el desarrollo protocolos y políticas, conceptos, directrices, herramientas y sistemas de gestión que permitan proteger los activos de una organización, y los de sus clientes y proveedores en el ámbito digital.

La amenaza es múltiple. Datos personales sensibles, redes de relaciones, información bancaria, claves de acceso, operaciones online...Todos generan una ingente información sensible, en circulación por una red global cuyos agujeros de seguridad pueden convertirse en un negocio muy lucrativo e, incluso, en brechas abiertas para las amenazas al propio sistema y a la seguridad física de los ciudadanos.

Los riesgos no se circunscriben a la red, porque la red es sólo el entramado sobre el que se sustenta el transporte, la industria, el comercio, la educación o la propia defensa de

los países. El "ciberentorno" incluye cada vez más ámbitos y garantizar su seguridad es garantizar no solo la actividad en la red, sino todas las actividades que de ella dependen.

A todos esos retos comunes de ciberseguridad se unen, en el caso de las empresas, los de la protección de la propiedad intelectual y de su propio saber hacer, y el cumplimiento de una normativa, profusa y compleja en ocasiones.

En España, el "Consejo Nacional de Seguridad" incluyó la ciberseguridad entre las doce prioridades de la "Estrategia de Seguridad Nacional" que tiene entre sus objetivos esenciales conocer y valorar las amenazas del ciberespacio, gestionar sus riesgos y articular una adecuada capacidad de prevención, defensa, detección, análisis, investigación y respuesta.

Esa Estrategia de Seguridad Nacional, persigue lograr la seguridad del ciberespacio a través del desarrollo y aplicación de una política nacional que proporcione una mayor confianza en el uso de las tecnologías de la información y la comunicación.

Ello exige la implantación de un marco nacional de políticas públicas, procedimientos y normas técnicas, pero también necesita una actualización continua del ordenamiento jurídico en una materia cuyos avances se miden progresivamente en unidades tiempo menores.

Pero para un problema que no es nunca local, tan importante como desarrollar la legislación es armonizarla a nivel global, desarrollando e implantado una regulación eficaz que no deje espacio a la creación de "paraísos para el ciberdelito".

En 2006, el Consejo de Ministros autorizó la creación y puesta en marcha del Instituto Nacional de Tecnologías de la Comunicación (Inteco) para contribuir a la convergencia de España con Europa en el ámbito de la sociedad de la información desarrollando proyectos innovadores en el área de las tecnologías de la información y de la comunicación.

En 2013, el Instituto se transforma en un centro de referencia en ciberseguridad para la Economía y la Sociedad Digital y en 2014, tras aprobarse la Estrategia de Ciberseguridad Nacional pasó a llamarse Instituto Nacional de Ciberseguridad de España, Incibe.

Su actividad, basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, se centra en afianzar la confianza digital, elevar el nivel de ciberseguridad y contribuir al desarrollo mercado digital de manera que se impulse el uso seguro del ciberespacio en España.

El Instituto es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.

Pero tanto o más importante que la normativa o las herramientas, en esta cuestión, es decisivo desarrollar una conciencia social de los riesgos derivados del ciberespacio sobre la que poder edificar una sólida cultura de ciberseguridad.

Para ello son necesarias sensibilización sobre las amenazas, sobre la importancia de los intangibles a proteger y sobre la necesidad real de protección de los sistemas y redes, y de la información que en ellos reside y circula.

La ciberseguridad es hoy materia imprescindible para lograr una adecuada protección que permita el desarrollo de instituciones, empresas y ciudadanos.