centro nacional de inteligencia
centro criptológico nacional

La Estrategia Española de Ciberseguridad, un esfuerzo oportuno y necesario

Es un lugar común afirmar que los países desarrollados dependen, hoy más que nunca, de sus infraestructuras TIC, tanto para el desarrollo y mantenimiento de sus servicios gubernamentales y administrativos como para la realización y avance de sus transacciones comerciales, financieras o personales. Sin embargo, la evolución de este nuevo espacio, el **ciberespacio**, constituido por los sistemas de información, las redes, las informaciones y los servicios, comporta nuevos **riesgos, retos y amenazas** a los que es preciso hacer frente, aquí y ahora.

No es de extrañar, por tanto, que durante el año 2011 numerosos países de nuestro entorno publicaran o actualizaran sus Estrategias Nacionales de Ciberseguridad como el mejor camino para desarrollar coherentemente todas las acciones de prevención, detección y respuesta que requieren las amenazas en el ciberespacio. La filosofía convergente en buena parte de ellas es la de aunar la libertad de acceso a las redes de comunicaciones abiertas con la necesaria seguridad que debe presidir su uso. En esta línea se enmarca, también, la **Estrategia Española de Ciberseguridad** (EECS), en la que se está trabajando en estos momentos y que parte de una premisa clara: el desarrollo y la prosperidad de España pasan por disponer de un ciberespacio accesible, seguro y confiable.

La ciberseguridad, por lo tanto, no debe considerarse como un mero aspecto de la seguridad; es más bien un condicionante de nuestra sociedad y de nuestro sistema económico. Máxime, si tenemos en cuenta que el ciberespacio puede verse comprometido por causas técnicas, fenómenos naturales o agresiones deliberadas, producidas desde cualquier parte del mundo y, en ocasiones, con escasas posibilidades de descubrir su origen e, incluso, su presencia.

La rentabilidad económica, política o de otro tipo que se obtiene; la facilidad y bajo coste en el empleo de las herramientas utilizadas, así como el bajo riesgo para el atacante, que lo puede hacer de forma anónima, han posibilitado el incremento constante de las amenazas. Ciberdelincuentes, crimen organizado, terroristas, *hacktivistas* e, incluso, los propios estados, capaces de explotar las vulnerabilidades tecnológicas con el objeto de recabar o destruir información, sustraer activos de valor y amenazar los servicios básicos, incluyendo los proporcionados por las llamadas infraestructuras críticas, son algunos de los actores que conforman las ciberamenazas.

GOBIERNO DE ESPAÑA · MINISTERIO DE LA PRESIDENCIA

CCN-CERT

El desarrollo y la prosperidad de España pasan por disponer de un ciberespacio accesible, seguro y confiable

Integración y coordinación

Ante esta situación compleja y cambiante, el espíritu de la EECS es el de promover la realización de un **esfuerzo coordinado**, y adecuadamente dirigido, de todas las partes implicadas en la ciberseguridad (Administraciones Públicas, sector privado y los propios ciudadanos) para contrarrestar la rápida evolución de las ciberamenazas.

De igual modo, y dado que la ciberseguridad no es algo que un país pueda lograr aisladamente, y teniendo en cuenta el carácter trasnacional de las amenazas y la dificultad de atribución de su autoría, la EECS apuesta por una **respuesta global**, coordinada y coherente con los socios y aliados de España.

Así pues, se busca un **Modelo de Ciberseguridad Integrado** que, dirigido por el Gobierno, garantice a nuestro país su seguridad y progreso, a través de la adecuada coordinación de todas las Administraciones Públicas entre sí, con el sector privado y con los ciudadanos, canalizando las iniciativas y esfuerzos internacionales en defensa del ciberespacio.

Para conseguir este uso seguro, confiable y con resiliencia de las Redes y Sistemas de Información, públicos y privados (particularmente los operadores de infraestructuras críticas), la Estrategia debe señalar la **necesidad de emplear herramientas adecuadas para la prevención, detección y respuesta a los ciberataques**.

Todo ello, sin olvidar una evidencia: no se podrá lograr ninguno de estos objetivos si todas aquellas personas que están involucradas en la seguridad de las organizaciones, de manera activa o pasiva, no son conscientes o no están adecuadamente formadas sobre su responsabilidad en el propósito común.

Por ello, la EECS mantendrá como objetivo la **sensibilización de los ciudadanos, profesionales, empresas y Administraciones Públicas** sobre los riesgos derivados del ciberespacio; al tiempo que se profundiza en el aprendizaje, habilidades, experiencia y capacidades que necesita nuestro país para sustentar un ciberespacio seguro. ■

Centro Criptológico Nacional
Centro Nacional de Inteligencia
Gobierno de España-Ministerio de la Presidencia