España fue el tercer país del mundo que más *ciberataques* sufrió en 2014. Para responder al desafío que supone la preservación del ciberespacio ha desarrollado mecanismos como el Esquema Nacional de Seguridad, para crear las condiciones de confianza necesarias en el uso de los medios electrónicos que permitan a ciudadanos y Administraciones el ejercicio de derechos y el cumplimiento de deberes.

LUIS MENÉNDEZ
luis.menendez@yahoo.es

Unidos contra los 'ciberdelitos'

DURANTE 2015 SE registraron en España más de 60.000 *ciberdelitos* de diversa naturaleza, de los cuales casi el 70 por ciento tenían que ver con el fraude y la estafa informática, según el secretario de Estado de Seguridad en funciones, Francisco Martínez. Meses antes era el titular de Asuntos Exteriores en funciones, José Manuel García-Margallo, quien en el curso de una presentación sobre *ciberguerra* señalaba que España fue el tercer país del mundo que más ataques cibernéticos sufrió en 2014, con más de 70.000 *ciberincidentes*, sólo superado por Estados Unidos y Reino Unido. Estos *ciberataques* tuvieron como destinatarios tanto empresas como administraciones públicas.

Los ciberdelitos son ataques que pueden acometerse de forma anónima, desde cualquier parte del mundo

Ataques rentables. Los *ciberdelitos* han proliferado en los últimos años por varias razones. Son rentables en términos económicos o políticos, las herramientas para llevarlos a cabo son de bajo coste y sus autores pueden ocultarse con relativa facilidad, lo que posibilita que los ataques puedan acometerse de forma anónima, desde cualquier parte del mundo y con capacidad para afectar tanto a ciudadanos, como a los sectores público y privado.

Los gobiernos llevan tiempo tratando de prepararse y adaptar sus marcos normativos a este nuevo escenario de confrontación. En nuestro caso, desde 2007, la Ley de acceso de los ciudadanos a los servicios públicos habilitó en su artículo 42 la creación del llamado Esquema Nacional de Seguridad (ENS), el cual tiene por objeto "establecer la política de seguridad en la utilización de medios electrónicos y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información".

Este esquema debe ser aplicado por las Administra-

Otros enfoques, mismo tema

▶ La monografía *El ciberespacio, nuevo espacio de confrontación* del CESEDEN plantea un escenario de conflicto en el que las escaramuzas pueden evolucionar a enfrentamientos mayores que combinados con otras actuaciones constituyan ciberguerra.
▶ http://cort.as/n3eC

▶ La *Estrategia de Ciberseguridad Nacional* contempla entre sus líneas de actuación "garantizar la implantación del Esquema Nacional de Seguridad".
▶ http://cort.as/n3fL

▶ Hipertextual.com recoge en una noticia el día en que el Gobierno de España aprobó su Estrategia de Ciberseguridad Nacional, un plan estratégico enfocado en la seguridad de los sistemas de las Administraciones Públicas, las infraestructuras críticas y las empresas.
▶ http://cort.as/n3gv

▶ El Instituto Español de Estudios Estratégicos publicó en abril un documento de opinión dedicado al concepto de la ciber-resiliencia.
▶ http://cort.as/n3hJ

'No more Ransom'

Uno de los más frecuentes en los últimos tiempos es el *ransomware*, un tipo de *malware* que bloquea el ordenador de la víctima o encripta sus datos, exigiendo un rescate para recuperar el control sobre el dispositivo o los archivos afectados. Para hacer frente a esta amenaza, el 25 de julio surgió No more Ransom, una iniciativa del Centro Europeo de Ciberdelincuencia de Europol, la Unidad Nacional de Delitos de Alta Tecnología de la Policía de los Países Bajos y de Kaspersky Lab e Intel pensada para ayudar a las víctimas de *ransomware* para que puedan recuperar su información cifrada sin tener que pagar a los *ciberdelincuentes*.

Recientemente, 13 países, entre los que se encuentra España, se han unido en la lucha mundial contra el *ransomware*. El llamado *cryptoware* (cifrado de *ransomware*) puede tener como objetivo desde el dispositivo de un usuario individual, a redes dentro de la industria, la salud, e incluso gobiernos, variedad que queda reflejada en la actividad en el portal de "No más de Ransom", que aglutina más de 24,5 millones de visitas desde su lanzamiento.

ciones Públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

Otros propósitos son establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la citada ley; introducir elementos comunes que guíen la actuación de las Administraciones en materia de seguridad de las tecnologías de la información; aportar un

lenguaje común para facilitar la interacción, así como un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios de administración electrónica cuando participan diversas entidades.

Cabría pensar que el grado de adecuación de los sistemas de las Administraciones es pleno, teniendo en cuenta que la disposición transitoria del Real Decreto 3/2010 que regula el Esquema Nacional de Seguridad preveía un mecanismo escalonado para adecuarse al mismo cuyo plazo finalizaba en 2014, pero puede deducirse que esto no es así, puesto que el Real Decreto 951/2015 establece una prórroga hasta el 4 de noviembre de 2017.

Pero el ENS no ha sido el único paso dado en esta dirección. El Consejo de Seguridad Nacional –presidido en la actualidad por Mariano Rajoy– impulsó en 2013 la elaboración de la Estrategia de Ciberseguridad Nacional para dar respuesta al desafío que supone la preservación del ciberespacio. Fue adoptada al amparo y en línea con la Estrategia de Seguridad Nacional, donde la *ciberseguridad* constituye uno de sus 12 ámbitos prioritarios de actuación. Una de las líneas de actuación de la Estrategia de Ciberseguridad Nacional contempla precisamente garantizar la implantación del Esquema Nacional de Seguridad.

El 80% de las empresas europeas han experimentado como mínimo un incidente de ciberseguridad en 2015, según una encuesta de PricewaterhouseCoopers

Actuación coordinada. El *ciberespacio* ofrece un escenario de confrontación único en el que las fronteras se diluyen y se sufre guerra asimétrica –aquella en la que el número de atacantes no se corresponde con el de defensores– por lo que es necesario unir todos los elementos de defensa existentes, afirma José Luis Vázquez-Poletti, profesor del departamento de arquitectura de computadores y automática de la Universidad Complutense de Madrid.

El Esquema Nacional de Seguridad actúa coordinando el trabajo que realizan la Brigada de Investigación Tecnológica de la Policía Nacional, el Grupo de Delitos Telemáticos de la Guardia Civil, redIRIS, el Estado Mayor (Mando Conjunto de Ciberdefensa) y el Centro Nacional de Inteligencia (CNI), "para que cubran su ámbito de actuación, pero no se dupliquen esfuerzos", añade el experto.

Y es que, según una reciente encuesta de PricewaterhouseCoopers, al menos el 80 % de las empresas europeas han experimentado como mínimo un incidente de ciberseguridad en el último año, y el número de incidentes de seguridad registrados en todos los sectores industriales en todo el mundo aumentó un 38 por ciento en 2015.

El ENS está pensado para Administraciones Públicas, pero ¿cómo se lucha desde el ámbito privado? ¿Hay un marco de obligado cumplimiento para empresas? Técnicamente se encuentra la norma ISO 2700, de gestión de seguridad de la información, pero no es de obligado cumplimiento.

Y aquí se abre el debate. Pese a que esta ha adquirido una creciente importancia en materia de certificación, no ha logrado alcanzar el grado de implantación a nivel mundial de otros estándares de gestión, como la ISO 9001, el estándar que establece los requisitos de un sistema de gestión de la calidad. Tal es su importancia que actualmente no se cuestiona si es una norma voluntaria u obligatoria, ya que se considera que quien no goce de certificación puede considerarse excluido del mercado. Váquez-Poletti lo resume en una frase: "En una sociedad de relativamente libre mercado, la confianza en una empresa al final vuelve obligatorias ciertas condiciones".

Los esfuerzos por intensificar la lucha contra las *ciberamenazas* también se encuentran en la agenda de la Comisión Europea. Recientemente ha puesto en marcha la primera asociación público-privada sobre *ciberseguridad* destinada a equipar mejor a Europa contra los *ciberataques* y a reforzar la competitividad del sector, que se espera atraiga una inversión estimada de 1.800 millones de euros hasta 2020. La inversión de la UE será de 450 millones de euros pero se prevé que los agentes de este mercado, representados por la Organización Europea de Ciberseguridad, inviertan tres veces más. La propuesta, según el vicepresidente responsable del Mercado Único Digital, Andrus Ansip, contiene medidas "para reforzar la resiliencia de Europa frente a estos ataques y garantizar la capacidad necesaria para la construcción y expansión de nuestra economía digital". Por su parte, el comisario de Economía y Sociedad Digitales, Günther H. Oettinger, ha hecho un llamamiento a los Estados miembros y a todas las entidades de *ciberseguridad* para que intensifiquen la cooperación y pongan en común sus conocimientos, información y experiencia con el fin de aumentar la ciber-resiliencia de Europa.

Respecto a este concepto, el doctor en informática, Luis de Salvador, considera en un documento de opinión publicado en el Instituto Español de Estudios Estratégicos (IEEE) que la ciber-resiliencia es un conjunto de condiciones dinámicas, el resultado de un largo proceso que implica "la capacidad de analizar críticamente el entorno, tener capacidad de anticipación, incorporar estructuras, actores y funciones flexibles y adaptables". Asimismo, señala que la supuesta resiliencia no ha de ser una excusa para la relajación de la gestión del riesgo ni del cambio, ya que ambos procesos forman parte de los mecanismos para garantizarla. ●

VÍCTOR DOMINGO,
presidente de la Asociación de Internautas
http://www.internautas.org

presidente@internautas.org
https://www.facebook.com/victor.domingo
@victordomingo

Salvemos nuestra privacidad

SI DE UN LADO OBSERVAMOS una evidente falta de cultura de la privacidad por parte de los usuarios y por otro la ausencia de garantías que gobiernos y empresas tienen por la privacidad de ciudadanos y clientes respectivamente, se produce un cóctel perverso que hace de la privacidad una asignatura pendiente que entre todos debemos aprobar urgentemente para establecer las bases que nos aseguren legalmente los derechos fundamentales a nuestra privacidad y el respeto por nuestras comunicaciones electrónicas.

En lo que respecta a los ciudadanos en nuestra calidad de internautas hemos que tener consciencia para dotarnos de claves fuertes y seguras, para lo que es recomendable actuar de la siguiente manera:

Claves largas, complejas y si no tienen sentido, mejor. Las mejores contraseñas, es decir las más difíciles de adivinar y por ende de ser sustraídas, son las largas, que contienen letras, números, signos de puntuación y símbolos. Hay palabras o frases inventadas por el usuario con las que construir contraseñas que pueden ser fáciles de recordar para él mismo e imposibles de descifrar para quien lo intente. Ej: "Tengo1clave+segura." para generar la clave "T1c+s"

Integrar símbolos en tus claves. También se puede tener una clave fácil de recordar y difícil de adivinar utilizando símbolos. Por ejemplo: 'vaca123' (clave fácil de adivinar) quedaría convertida en "vaca!"#".

Contraseñas fáciles, pero difíciles de olvidar y de adivinar. Para muchos, las contraseñas complejas son un riesgo por la posibilidad de olvidarlas. Un truco es usar una palabra o frase fácil, pero cambiando las vocales por números. Por ejemplo: 'Tengoalgoparadecirte' sería "T3ng0alg0parad3c1rt3".

Usar mayúsculas. Utilizando la opción de las mayúsculas se agrega una dificultad más a quienquiera adivinar nuestra clave. La misma puede ir al inicio o en cualquier parte de la clave. Ejemplo: "Elecciones2012" o "eleCciones2012".

No usar la misma clave para todo. Para cada usuario que tenemos (de correo electrónico, red social, banco, etc.) deberíamos contar con una contraseña distinta. Los *ciberdelincuentes* suelen robar contraseñas de sitios web que cuentan con poca seguridad, y luego intentan replicar las mismas en entornos más seguros, como webs de los bancos. Por eso: usar distintas claves en diversos sitios de internet.

¡No compartirlas con nadie! Las claves son personales y no deben ser compartidas con nadie. El usuario es el dueño de la cuenta, pero también es el dueño de la clave. La misma no debe ser conocida más que por su dueño.

Evitar información personal. No incluir en la contraseña nombre, apellido, fecha de nacimiento, número de documento, o información del estilo, ya que son más fáciles de adivinar.

Procurar cambiar la clave luego de un período de tiempo prudencial. Si usamos equipos compartidos o redes públicas en sitios públicos será prudente cambiar las claves de acceso pasado un tiempo.

Preguntas secretas. En el momento del registro en un sitio web, uno de los requisitos que surgen al completar los datos es establecer una pregunta secreta por si alguna vez no recordamos la clave o contraseña de acceso. Por eso debemos elegir la que consideremos más complicada de adivinar, es decir evitando las de respuestas obvias. Ejemplo: Color favorito.

Guardar las claves en un documento de texto. Al elegir contraseñas largas, difíciles de memorizar y tener varias (para los distintos usuarios con los que contamos) puede ser útil tenerlas almacenadas en un documento dentro de nuestro PC. Esto puede ser pesado o tedioso, pero es muy seguro.

También debemos saber que internet dispone de todo lo que insertamos en sus redes; debemos evitar ofrecerle demasiada información sobre nosotros mismos, y ser conscientes de lo fácil que es perder el control sobre ello.

En redes sociales se sugiere no aceptar gente desconocida. Hay que recordar que detrás de un perfil falso puede haber una persona tratando de tomar control del equipo o robar información. En las redes sociales pueden acceder a los perfiles más personas de las que se cree. Una buena práctica consiste en tomarse algunos minutos para configurar la privacidad de la cuenta y así evitar que sea visible para cualquiera.

«Para tener una organización digital segura y protegida tenemos que contar con una clave sólida y eficiente»

Internet permite manejar dinero sin necesidad de tocarlo, las transacciones que realices, que sean con permiso seguro del banco en que confías. Desconfía de los envíos de dinero que no pasan por una entidad bancaria o una administración pública estatal. Por eso es fundamental el uso adecuado de las claves que utilizamos. Todos los sistemas tienen la particularidad de estar protegidos por una contraseña de acceso. Por eso, para tener una organización digital segura y protegida tenemos que contar con una clave sólida y eficiente. Así, evitaremos sufrir incidentes con nuestras cuentas *online*.

Además hay que saber que internet no es ilegal, pero puede ser el escaparate de la comisión de un delito; presta atención a lo que te llega a través de sus redes y desconfía de lo que tenga un origen incierto. Internet es paralela a la vida real, no ajena, lo que pasa suele tener un reflejo directo en el ámbito personal y físico de los implicados.

Existen leyes que castigan las actividades ilícitas en internet, y también hay leyes que protegen a sus usuarios de una mala utilización, especialmente cuando afecta a sus derechos fundamentales (intimidad, secreto de las comunicaciones, datos personales, libertad de expresión, etc.). Si eres víctima, denuncia. Ten a mano información sobre legislación para su consulta rápida o para denunciar.

Internet sin barreras: El derecho de los discapacitados a acceder a la Red