DOCUMENTO
DE CONCLUSIONES

Ciberseguridad en el Sector Público

Fecha de publicación 13/03/2017
Informática El Corte Inglés

OBSERVATORIO
SECTOR PÚBLICO
INFORMÁTICA El Corte Inglés

OSPI

Presentación

El Observatorio del Sector Público (OSPI) es una iniciativa de Informática El Corte Inglés que vio la luz a mediados del pasado 2015, y que lleva a cabo tareas de identificación, ordenación, valoración y difusión de políticas públicas, planes de acción, proyectos y servicios exitosos para la transformación digital, a partir de los cuales se puedan efectuar propuestas aplicables al sector público español. Más información aquí.

El presente documento es el resultado de un coloquio entre diferentes expertos en el ámbito de la ciberseguridad, procedentes tanto de la Administración Pública como de la empresa privada. A lo largo del Encuentro, los expertos abordaron la ciberseguridad con un enfoque multinivel: desde las estrategias supranacionales y nacionales a las necesidades operacionales que puedan tener los Centros de TI de las AAPP o las infraestructuras críticas. Y también con un enfoque integral: amenazas, vulnerabilidades, herramientas, ciberdelito, respuesta a incidentes, impacto económico, etc.

Introducción

Moderado por Víctor M. Izquierdo Loyola, Presidente del Observatorio del Sector Público (OSPI), el debate se articuló alrededor de tres grandes bloques temáticos. El primero de estos bloques estuvo dedicado a analizar las estrategias, políticas y planes en materia de ciberseguridad, tanto a nivel nacional como internacional, tomando como referencia en el caso español la Estrategia de Ciberseguridad Nacional, integrada en la Estrategia de Seguridad Nacional (http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional). En el ámbito internacional las intervenciones se centraron en los recientes cambios legales, con la aprobación de la Directiva NIS y del Reglamento General de Protección de Datos, poniendo de manifiesto las nuevas obligaciones de notificación de incidentes.

En el segundo bloque del debate se abordó la problemática relacionada con las ciberamenazas. Y se pusieron sobre la mesa aspectos tan relevantes como los factores y tipos de amenazas más frecuentes, la prevención y el impacto económico que acarrean.

Ya en el tercer bloque, los especialistas convocados por el OSPI debatieron sobre las posibles respuestas a los incidentes. En particular, acerca de las soluciones organizativas y tecnológicas más eficaces, sobre cómo abordar la ciberseguridad en los nuevos entornos y en las prioridades de inversión para mejorar la capacidad de respuesta de las Administraciones Públicas.

Conclusiones generales

- La ciberseguridad en las Administraciones Públicas dispone de un nivel aceptable gracias al Esquema Nacional de Seguridad (ENS. http://www.boe.es/buscar/pdf/2010/BOE-A-2010-1330-consolidado.pdf). En la situación actual lo que toca es potenciar su implementación, así como desplegar los servicios compartidos que le deberían acompañar.
- Sensibilización y formación a la sociedad, a las empresas y, por supuesto, a la Administración son aspectos esenciales de las políticas públicas en este campo, especialmente en la fase de prevención de incidentes.
- Vivimos en un espacio en el que confluyen la vida real y el entorno virtual, por ello, hay que abordar la seguridad en los dos ámbitos de forma paralela.
- Por supuesto que las Administraciones Públicas deben invertir de manera permanente en ciberseguridad, mediante la adquisición de productos avanzados (bienes o servicios) para la protección de sus sistemas. Pero ello no es suficiente, sino que es necesario contemplar aspectos de formación de especialistas, de regulación, de estandarización, de gobernanza, etc., con una visión de 360º.
- El software juega un papel determinante en la protección de los entornos operativos. Y dentro de él, conviene tener en cuenta las alternativas que ofrece el software abierto, al ofrecer amplias posibilidades de configuración y personalización, evitando así la dependencia tecnológica de productos propietarios.
- Hay tres aspectos clave que deben ser tenidos en cuenta por las Administraciones:
  - Reducción del perímetro, gracias al empleo de servicios compartidos y de la implementación de un punto de acceso único a la red.
  - Retención del talento: selección y gestión de los profesionales con formación especializada en seguridad dentro de la Administración;
  - Trabajar en futuros escenarios forenses reglados.
- La Estrategia de Ciberseguridad Nacional (http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional) ofrece un enfoque integral, involucrando a todos los actores afectados. Está bien concebida y es similar a las de otros países de nuestro entorno. El momento actual es el del desarrollo de los planes derivados de la Estrategia. Sin embargo, nos enfrentamos a un problema enorme, debido a la dificultad de seguir el vertiginoso avance tecnológico.
- Hay acontecimientos que nos permiten ser optimistas en relación con el problema que nos ocupa: disponemos de un potente acervo normativo, de carácter obligatorio para las Administraciones Públicas. Además, hay asuntos que son de general conocimiento de la sociedad, como los que afectan a la protección de datos personales.
- Finalmente, entre las áreas de actividad que pueden marcar la evolución de la ciberseguridad en los próximos tiempos se encuentran las siguientes:
  - Proactividad e inteligencia predictiva.
  - Análisis de riesgos a partir de escenarios.
  - Idear mecanismos de seguridad sin necesidad de que existan elementos conectados.

Estrategias, Políticas y Planes

El caso español, la estrategia de la UE, legislación, organización y colaboración con el sector privado

Para analizar las estrategias, políticas y planes en materia de ciberseguridad, los expertos han tomado como referencia para el caso español la Ley de Seguridad Nacional (http://www.boe.es/boe/dias/2015/09/29/pdfs/BOE-A-2015-10389.pdf), cuya aprobación supuso la creación de un marco legal para enfrentar los nuevos retos de la seguridad, más transversales, garantizando una arquitectura de gobernanza adecuada a esta situación. La creación previa del Consejo de Seguridad Nacional, que preside el propio Presidente del Gobierno, reflejaba ya la necesidad manifiesta de que la responsabilidad sobre las políticas en materia de seguridad y ciberseguridad se situara al máximo nivel de responsabilidad del Gobierno.

Los expertos convocados han destacado también el relevante papel del Esquema Nacional de Seguridad (ENS) y la necesidad de que realmente se aplique esta norma vigente en nuestro país. El ENS surge de la Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos y es de aplicación a todos los sistemas de las Administraciones Públicas (general del Estado, autonómica y local). Pero, al tratarse de una norma de consenso, a veces ha resultado difícil materializar e impulsar su implantación en las Administraciones Públicas, especialmente en la Administración Local. Por ello constituye una prioridad la generación de una red de confianza entre las Administraciones, que permita compartir información, crear estructuras para la cooperación interadministrativa y un modelo de gobernanza para la ciberseguridad.

En cuanto a los riesgos, los expertos llaman la atención sobre la escasez de profesionales entrenados, lo que conduce a que, en ocasiones, los equipos operativos estén poco poblados. Por lo que los expertos han recomendado poner en marcha iniciativas de formación avanzada, a fin de repoblar dichos equipos.

A nivel de la UE hay que tener en cuenta la Directiva 2013/40, relativa a los ataques contra los sistemas de información (https://www.boe.es/doue/2013/218/L00008-00014.pdf), cuyos objetivos son aproximar las normas de Derecho penal de los Estados miembros en materia de ataques contra los sistemas de información, mediante el establecimiento de normas mínimas relativas a la definición de las infracciones penales y las sanciones aplicables, y mejorar la cooperación entre las autoridades competentes. Esta Directiva, que ya ha sido traspuesta al derecho español a través de una modificación del Código Penal, constituye una excelente herramienta para la lucha contra el ciberdelito, si bien deja algunos aspectos que requerirían una mayor concreción, como el concepto de “adecuado nivel de protección”. En este sentido, también es necesario subrayar la necesidad de que jueces y fiscales dispongan de más información y formación en la materia a fin de lograr una aplicación efectiva de la norma.

Más recientemente se han incorporado al derecho europeo dos nuevas normas que afectan al tema del debate. Se trata de la Directiva 2016/1148, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (https://www.boe.es/doue/2016/194/L00001-00030.pdf), más conocida como Directiva NIS, y el Reglamento General de Protección de Datos (https://www.boe.es/doue/2016/119/L00001-00088.pdf), relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que entró en vigor el pasado mes de mayo, si bien será aplicable a partir del 25 de mayo de 2018.

Estrategias, Políticas y Planes

Conclusiones y recomendaciones

- Una estrategia de ciberseguridad adecuada debe tener en cuenta las tres capas del ciberespacio: la física, la lógica y la social.
- Hacen falta muchos más recursos con las competencias adecuadas que los actualmente disponibles. Se necesita una masa crítica de, al menos, 5.000 o 6.000 agentes con competencias básicas en escenarios de ciberdelito. El ritmo al que se vienen formando nuevos agentes es claramente insuficiente.
- En relación con el Esquema Nacional de Seguridad (ENS), hay que conseguir que su implantación sea completa, ya que actualmente su implantación apenas llega al 50%.
- Las empresas privadas tienen un papel relevante para lograr la aplicación completa del ENS en la Administración Pública. La publicación de la Guía CCN-STIC-809, relativa a la Declaración y certificación de conformidad con el ENS y distintivos de cumplimiento (https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/1279-ccn-stic-809-declaracion-de-conformidad-con-el-ens/file.html), permite habilitar a empresas para hacer auditorías de seguridad y expedir certificados. Hay que impulsar a las Administraciones Públicas para que lleven a cabo estas auditorías, teniendo en cuenta que el ENS, al igual que ocurre con el Esquema Nacional de Interoperabilidad, es obligatorio, pero su incumplimiento no acarrea sanciones.
- En el área de la ciberseguridad es necesario generar estructuras de gobernanza y redes de confianza que incorporen a todas las Administraciones Públicas y que se extiendan también a nivel supranacional, especialmente en el ámbito de la Unión Europea.
- Las ciberamenazas van más allá de lo que se conoce comúnmente como ciberdelito. Hay otras amenazas, como pueden ser ataques desde otro Estado. Ante este tipo de riesgos lo aconsejable es adoptar medidas preventivas.
- Las Administraciones Públicas deben trabajar a conciencia en la protección de las infraestructuras críticas y los servicios esenciales. Hay que tener en cuenta que éste es un campo con amplia presencia del sector privado, por lo que existe una mayor dificultad a la hora de imponer obligaciones.
- Dos nuevas normas cambiarán el panorama sustancialmente dentro de la Unión Europea: la Directiva NIS (Network Information Security) y el Reglamento General de Protección de Datos. Ambos obligan a la notificación de incidentes, eso sí, a distintos puntos de contacto. En el caso de la Directiva NIS deben notificarse los incidentes que afecten a operadores de servicios esenciales (que, dicho sea de paso, no coinciden con los operadores de Infraestructuras Críticas). Estas notificaciones deben dirigirse a la autoridad competente en materia de NIS, o a los equipos de respuesta a incidentes de seguridad informática (CSIRTs). Por su parte, el nuevo Reglamento General de Protección de Datos de la UE promueve la creación de mecanismos de certificación, con carácter voluntario, lo que constituye un avance muy importante. Pero, en este caso, las notificaciones se dirigen a las Autoridades de control en materia de protección de datos. Quizás fuera razonable establecer un único punto para las notificaciones que afectan a estas dos normas de la UE.
- Los atentados de Nueva York (11-S) supusieron un punto de inflexión para incentivar las políticas y estrategias de ciberseguridad. Hoy, la mayor amenaza que puede esperar cualquier país de nuestro entorno, incluyendo España, proviene de entornos yihadistas. Es necesario aplicar medidas adecuadas a fin de reducir nuestra vulnerabilidad, teniendo en cuenta que los que nos pueden atacar cuentan con muchos recursos procedentes de los mercados de droga, armas, petróleo, etc.

Ciberamenazas

Factores de las amenazas: Tipos, prevención e impacto económico.
Agentes y objetivos que persiguen. El ciberterrorismo.
¿Cómo afectan en particular a las infraestructuras críticas?

La revolución que supone la digitalización de la economía y de la sociedad implica una transformación global en la que la información y los datos juegan un papel determinante. La eclosión de la economía digital también ha traído aparejado el crecimiento exponencial de los riesgos de seguridad. Aunque personas y organizaciones públicas y privadas han ido tomando conciencia de estos riesgos, agudizando su preocupación por la necesidad de impulsar un entorno (tanto físico como virtual) seguro, sigue habiendo multitud de amenazas que frecuentemente pasan desapercibidas.

Los expertos han señalado que en España hay que prestar atención prioritaria a las cuestiones relacionadas con el ciberespionaje (supone pérdidas de competitividad y empleo), el ciberdelito (según fuentes del Reino Unido, el 42% de las amenazas de *ransomware* terminan con el pago de rescates), y el *hacktivismo*, cuyos ataques pueden provenir no solo de España, sino de otras zonas geográficas. Hay que estar muy atentos también al ciberterrorismo, en ocasiones financiado por la delincuencia organizada. Así arrancaba el segundo bloque del Encuentro sobre ciberseguridad en las Administraciones Públicas.

Entre las principales reflexiones que compartieron los expertos destaca el hecho de que hasta el momento presente las políticas y estrategias de seguridad ponían el foco en las personas. Ahora, sin menospreciar el factor humano como principal fuente de riesgo, hay que asumir que estamos adentrándonos en un nuevo territorio, como consecuencia de la digitalización de la economía y la sociedad. Asistimos a la presencia creciente de los algoritmos en la vida ordinaria y a la eclosión de la Internet de las cosas (IoT), lo que implica el salto a un modelo con una pluralidad de identidades digitales.

Las respuestas de los expertos para mitigar las posibles consecuencias que implica este nuevo escenario pasan por:

- La necesidad de contar con un régimen sancionador eficaz.
- Desarrollar capacidades de vigilancia avanzadas.
- Aumentar las inversiones con una tendencia clara hacia el equilibrio entre la seguridad lógica y la seguridad física. Ahora gastamos mucho en seguridad física y muy poco en seguridad lógica.

Antes de las conclusiones a las que se llegó en esta parte del Encuentro, los expertos dejaron una frase para la reflexión: “la inseguridad informática está siendo el motor de la propia seguridad informática”.

Ciberamenazas

Conclusiones y recomendaciones

- Cualquier estrategia de seguridad, en sentido amplio, debe tener en cuenta las amenazas que provienen del ciberespacio.
- Siendo importantes las personas como factor de riesgo, ya no se sitúan en el centro de las políticas de seguridad. La era del IoT y la presencia de algoritmos y la multiplicidad de identidades digitales, acentúan los riesgos.
- Nos estamos adentrando en un territorio nuevo, en el que somos gobernados por algoritmos. En este contexto, los tiempos de respuesta no se ajustan al modelo humano, incapaz de operar en microsegundos. Ello supone un salto cualitativo, con la aparición de nuevas amenazas.
- Es necesario equilibrar las inversiones en seguridad física y en seguridad lógica, lo que permitirá minimizar la vulnerabilidad de personas y organizaciones. Incluso desde el punto de vista tecnológico, estamos asistiendo a una convergencia entre los mundos físico y lógico.
- Hay que analizar el coste de la eficacia de las medidas de seguridad. En este análisis, se debe tener en cuenta la valoración de los intangibles para medir a largo plazo los efectos de la falta de seguridad.
- Las principales amenazas que se ciernen sobre España son el ciberespionaje, el ciberdelito, el hackivismo y el ciberterrorismo. El crimen organizado dista de ser un hecho romántico: hay empresas organizadas del crimen que ofrecen sus capacidades, desarrollando herramientas, haciendo uso de la ingeniería social y explotando vulnerabilidades
- Para hacer frente a las amenazas, en España disponemos de una normativa desarrollada, en la que se establecen las obligaciones No obstante, sigue habiendo cierto desconcierto sobre cómo ponerla en práctica. A título de ejemplo, podemos decir que menos del 5% de los órganos administrativos y organismos públicos efectúan las auditorías obligatorias del ENS.
- Para avanzar en este terreno de la realización de auditorías es clave la colaboración del sector privado. En este ámbito, hay que motivar a las empresas privadas para que se acrediten ante ENAC, de conformidad con la norma UNE-EN ISO/IEC 17025:2005. Criterios generales para la acreditación de laboratorios de ensayo y calibración.

Respuesta ante incidentes (o preparación ante posibles incidentes)

¿Qué soluciones organizativas, tecnológicas, etc. resultan más eficaces?

¿Cómo abordar la ciberseguridad en nuevos entornos: la ciudad inteligente, el IoT, ...?

¿Qué inversiones resulta necesario priorizar para mejorar nuestra capacidad de respuesta?

Ya en el tercer bloque, los especialistas convocados por el OSPI debatieron sobre las posibles respuestas a los incidentes. En particular, acerca de las soluciones organizativas y tecnológicas más eficaces, sobre cómo abordar la ciberseguridad en los nuevos entornos y en las prioridades de inversión para mejorar la capacidad de respuesta de las Administraciones Públicas.

Tras constatar el importante número de incidentes que afectan a las Administraciones Públicas: se estima que pueden llegar a 21.000 en 2016, los expertos señalaron que es necesario establecer mecanismos de notificación y métricas para determinar el origen de los ataques, los recursos afectados y el tiempo de resolución, entre otras cuestiones. Por otra parte, hacen falta equipos dedicados a tiempo completo, al mando de un responsable, que trabajen siguiendo procedimientos adecuados. Sólo así cabe esperar una respuesta eficiente y que permita efectuar la trazabilidad de los incidentes en un escenario de evidencia forense.

Además, las Administraciones Públicas deberían crear equipos de seguridad activa que les permitan anticiparse a los ataques y pasar de la resolución de incidentes a disponer de una respuesta preventiva ante situaciones de crisis. En este sentido, se muestra la necesidad de conectar el mundo de la ciberseguridad con otros ámbitos de la seguridad nacional.

Los expertos señalaron también la necesidad de que la contratación pública tenga en cuenta los estándares básicos de ciberseguridad, para cuya efectividad hacen falta certificaciones de seguridad y productos confiables. Finalmente, mencionaron tres propuestas para reforzar la ciberseguridad en las Administraciones Públicas: salida única a Internet, prestación centralizada de servicios horizontales y liderazgo que cuente con el apoyo de toda la organización.

Respuesta ante incidentes (o preparación ante posibles incidentes)

Conclusiones y recomendaciones

- Es importante subrayar que, sin lugar a dudas, las Administraciones Públicas son vulnerables. Una vez, asumido esto, para resolver las incidencias se necesitan equipos dedicados. No es suficiente con que las Administraciones Públicas cuenten -como especifica el ENS- con un responsable de seguridad, sino que éste deberá estar acompañado de un equipo que le ayude a proporcionar respuestas eficientes y procedimentales.
- Hay que facilitar el intercambio de información sobre incidentes para evitar que éstos se repitan en Administraciones diferentes. Aunque las Administraciones Públicas no compiten, hay un cierto recelo para intercambiar información sobre los ataques que se reciben. El modelo a seguir podría ser la creación de grupos pequeños para generar confianza, porque por mandato imperativo no se consigue la misma eficacia.
- Es importante establecer sistemas de trazabilidad de los incidentes, aunque ello es muy difícil de instrumentar. La inteligencia debe estar preparada para la maldad, ya que hoy se ofrece el delito como servicio (CaaS).
- La creación de equipos de seguridad ofensiva o seguridad activa permitirá adelantarse a los ataques. O bien nos anticipamos al ataque antes de que se produzca, o aumentamos la resiliencia.
- Hay que conectar el mundo de la ciberseguridad con otros ámbitos de la Seguridad Nacional (diplomacia, inteligencia, economía ...)
- Es necesario tomar conciencia de todos los elementos inteligentes que tienen IP y que no están protegidos: IoT, sistemas industriales inteligentes, redes SCADAs, cámaras de CCTV, etc. La presencia de estos dispositivos hace que el perímetro se haga prácticamente ilimitado.
- La obsolescencia de los equipos físicos y lógicos en las Administraciones Públicas constituye un problema que deberá resolverse a través de un plan de inversión que permita actualizar la infraestructura.
- Las Administraciones Públicas deberían incluir requisitos de cumplimiento de estándares básicos de ciberseguridad en los pliegos de condiciones de los contratos. Apoyándonos en el ENS y sus certificaciones, se deben incorporar productos confiables al parque de recursos TIC de la Administración.
- Las políticas públicas tienen que estar en evaluación permanente, a fin de ajustarlas en función de los resultados que logran en la mejora de la ciberseguridad.
- Por sus efectos positivos sobre la ciberseguridad, hay que apostar por la prestación centralizada de servicios compartidos y la salida única a la Red, apoyando a quien lidere su implementación dentro de la Administración.

El debate sobre "Ciberseguridad en el Sector Público" es el quinto de una serie (los anteriores han estado dedicados a Smart Cities, Big Data, Factor Humano y Gobierno Abierto), y en esta ocasión, han participado los siguientes expertos: Enrique Ávila Gómez, director del Centro Nacional de Excelencia en Ciberseguridad; Javier Candau Romero, Jefe del Departamento de Ciberseguridad del Centro Criptológico Nacional (CCN); Joaquín Castellón Moreno, Director Operativo del Departamento de Seguridad Nacional. Presidencia del Gobierno; Ángel García Collantes, Criminólogo. Profesor de la Universidad a Distancia de Madrid (UDIMA); Pablo L. Gómez Sierra, Experto en Ciberterrorismo; Javier Valdés Quirós, Director de Proyectos Especiales en Logtrust; y Manuel Barrios Paredes, Responsable de Seguridad Corporativa – CISO en Informática El Corte Inglés.

Sobre el Observatorio del Sector Público (OSPI)

Con el foco puesto en la transformación digital de las Administraciones Públicas y tomando como marco de referencia la iniciativa puesta en marcha por Informática El Corte Inglés, Administración Digital 2020, el Observatorio del Sector Público lleva a cabo tareas de identificación, ordenación, valoración y difusión de políticas públicas, planes de acción, proyectos y servicios exitosos para la transformación digital, provenientes principalmente del ámbito internacional, a partir de los cuales se pueden efectuar propuestas aplicables al sector público español, dando lugar a un verdadero centro de conocimiento de la Administración Digital.

OTRAS PUBLICACIONES:

www.administraciondigital2020.com/observatorio.html

OBSERVATORIO
SECTOR PÚBLICO
INFORMÁTICA El Corte Inglés
OSPI

OBSERVATORIO
SECTOR PÚBLICO
INFORMÁTICA El Corte Inglés

OSPI