MAGAZINE Nº5

#CIBERSEGURIDAD
#PRIVACIDAD

isms forum

DIGITAL [RE] EVOLUTION

El Magazine semestral de ISMS Forum - International Information Security Community

ENTREVISTAS

"La colaboración público-privada y con la sociedad civil se ha convertido en una necesidad real"

MAR LÓPEZ

Jefa de Ciberseguridad, DSN

FIRMA INVITADA

"El futuro de la ciberseguridad"

SOLEDAD ANTELADA

Ingeniera en Ciberseguridad en NERSC, Berkeley Lab, U.S Departamento de Energía. Jefa de seguridad en red de SC20

ARTÍCULO

"¿Qué está haciendo Europa para adaptarse a la nueva era digital?"

REDACCIÓN ISMS FORUM

SEPTIEMBRE 2020
www.ismsforum.es

EDITA
ISMS Forum

DIRECTOR GENERAL
Daniel García Sánchez

CONSEJO EDITORIAL, REDACCIÓN, DISEÑO Y MAQUETACIÓN
Raquel García Robles

EQUIPO DE GESTIÓN
Carmen Granados Ruiz
Cynthia Rica Gómez
Diana Pérez Villa
Leire Ruiz Díaz-Rullo
Raquel García Robles
Virginia Terrasa Bover

PÁGINA WEB
www.ismsforum.es

PRESIDENTE

Gianluca D'Antonio, miembro independiente.

VICEPRESIDENTE

Carlos Alberto Saiz, Ecix Group.

TESORERO

Roberto Baratta, Abanca.

VICESECRETARIO

Francisco Lázaro, RENFE.

SECRETARIO DEL CONSEJO ASESOR

Juan Miguel Velasco.

VOCALES

Xabier Michelena, Accenture Security.
Carles Solé, Banco Santander España.
Gonzalo Asensio, Bankinter.
Virginia Rodríguez, CaixaBank.
Rafael Hernández, CEPSA.
Rubén Frieiro Barros, Deloitte.
Ricardo Sanz, Evolutio.
Edwin Blom, FCC.
Luis Buezo, Hewlett Packard Enterprise.
Eduardo Argüeso, IBM.
Marcos Gómez, INCIBE.
David Barroso, miembro independiente.
Guillermo Llorente, miembro independiente.
Toni García, miembro independiente.
Jesús Sánchez, Naturgy.
José Ramón Monleón, Orange.
Javier Urtiaga, PwC.
Javier García Quintela, REPSOL.
Agustín Muñoz-Grandes, S21sec.
Iván Sánchez, Sanitas.
Alfonso Fernández Jiménez, SIA.
Miguel Ángel Pérez, Telefónica.
Francisco Javier Sevillano, Vodafone.

JUNTA DIRECTIVA

CONTENIDOS

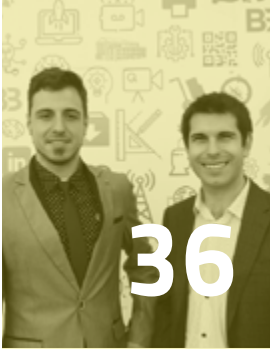
ISMS FORUM MA

FIRMA INVITADA

SOLEDAD ANTELADA

Ingeniera en Ciberseguridad en NERSC, Berkeley Lab, U.S Departamento de Energía. Jefa de seguridad en red de SC20

"El futuro de la ciberseguridad"



PROYECTOS DE INTERÉS

GuardedBox

"Guardedbox, tus secretos a buen recaudo"

IronChip

"IronChip, la startup vasca que ya triunfa en el mercado internacional"

LO QUE NO TE PUEDES PERDER

ISMS Forum

"ISMS lanza la Guía de Buenas Prácticas en Auditorías RGPD"

"Conoce la Guía para la gestión de crisis por ciberincidente en la cadena de suministro"

GAZINE

CARTA DEL PRESIDENTE

Época de cambios, desafíos y reinvención

GIANLUCA D'ANTONIO

Presidente de ISMS Forum

ismsforum.es

Estimados compañeros, socios y colaboradores de ISMS Forum:

Una vez finalizado el periodo estival y con él unas diferentes vacaciones de verano, retomamos el ritmo de trabajo habitual y nos preparamos para este otoño que se anuncia complejo e incierto.

No podemos obviar lo que ha acontecido durante estos últimos meses debido a la crisis sanitaria mundial originada por la Covid-19. Su impacto se ha hecho sentir, como era de esperar, también en la agenda de los equipos de seguridad de la información de las organizaciones. En estos meses, la asociación ha tenido que adaptarse a las circunstancias, reprogramando y, en muchos casos, rediseñando sus eventos. Nuestra dilatada experiencia en la organización de eventos presenciales nos ha servido para buscar nuevas formas de conectar con la comunidad de socios y profesionales de la seguridad de la información. También en nuestro caso, la actual crisis sanitaria ha supuesto un desafío y un elemento de aceleración para la transformación digital que estamos acometiendo.

La Asociación seguirá apostando por una cultura de la seguridad de la información abierta, plural e independiente, comprometida con la comunidad de profesionales que se encargan de gestionar los riesgos tecnológicos generando y fortaleciendo un ámbito de confianza digital. Contamos con la formación y experiencia de nuestros socios, siempre abiertos a participar en todas las iniciativas que apuestan por un libre intercambio de conocimiento, experiencias e información, como el recién constituido Foro Nacional de Ciberseguridad, del cual somos miembros. ISMS Forum es todo esto y más, por lo que solo queda decir:

¡Bienvenidos a bordo!

ACTUALIDAD

ISMS FORUM

La nueva identidad visual de ISMS Forum, en detalle

Redacción ISMS Forum

ISMS Forum ha querido apostar este año por un cambio de imagen que represente las nuevas aspiraciones de la Asociación. Te explicamos en detalle la necesidad de ISMS Forum de renovarse y lucir una nueva identidad ligada a la ambición de expandir sus actividades, ahora sí, a nivel mundial.

Dejamos de ser ISMS Forum Spain

ISMS Forum Spain pasa a ser ISMS Forum. Desaparece 'Spain' porque el deseo de la Asociación es dejar de centrar sus actividades en la capital madrileña y abrir sus fronteras tanto nacional como internacionalmente, apostando por la creación de capítulos que han empezado por ser regionales (Barcelona y Galicia, de reciente apertura), pero con objetivos a largo plazo de ser también internacionales.

Búsqueda de una definición universal

En ese afán de salir del ámbito nacional, creímos obligatorio hacer el ejercicio de redefinirnos en el idioma universal: International Information Security Community. Colocar el concepto de 'comunidad' ha casado a la perfección con nuestro objetivo de seguir ampliando la gran red de empresas y profesionales asociados a ISMS Forum. Un lema que sirve para renovarnos ante los que hoy día nos conocen bien, al tiempo que nos ayuda a causar una primera buena impresión a aquellos que aún no han escuchado hablar de nosotros.

Enlazar nuestra herencia con el presente

Se trata de un cambio de imagen que

Una mirada hacia el futuro que queremos: hacer de ISMS Forum una comunidad internacional

Tan solo es el comienzo de un futuro que esperamos sea próspero en nuestra función de promover el desarrollo, conocimiento y cultura de la Seguridad de la Información tanto en España como fuera de ella. Somos más que una red de empresas y profesionales que comparten experiencias en materia de ciberseguridad y protección de datos. Somos creadores de conciencia en un mundo hiperconectado en el que nuestra seguridad y estabilidad económica dependen de la información, y protegerla es una labor fundamental.

responde a la necesidad de alcanzar nuevos propósitos y seguir creciendo en nuestro ámbito, pero sin dejar atrás nuestra esencia. Por eso, hemos optado por un rebranding que mantiene nuestros signos distintivos, los que tantos años han acompañado nuestra actividad: tipografía minúscula y el azul y rojo corporativos. Además, hemos aprovechado para adaptarnos a los nuevos tiempos, persiguiendo una identidad más jovial y minimalista, facilitando su aplicabilidad técnica y funcional y transmitiendo valores más digitales, abiertos y globales.

Historia y evolución de nuestra marca

El último logotipo ha convivido con nosotros desde 2015, creado para cumplir con los objetivos marcados en la estrategia de ese mismo año a través de un proceso participativo de la Junta Directiva. Las decisiones tomadas respondían al comienzo de una nueva etapa para una organización que dejaba de ser el capítulo español de una organización internacional para convertirse en la matriz y facilitar la aparición de organizaciones regionales y/o nacionales a largo plazo. Se optó por un cambio de tipografía para mayor legibilidad y la desaparición de un símbolo situado en la parte superior izquierda que manifestaba los colores de la bandera española.

ARTÍCULO

¿Qué está haciendo Europa para adaptarse a la nueva era digital?

Redacción ISMS Forum

La digitalización es un proceso que avanza a niveles más rápidos de los que podemos controlar. La regulación europea se modifica periódicamente con la intención de adaptarse a los cambios, y así poder competir a nivel internacional al mismo tiempo que preserva los derechos digitales -en especial los relativos al tratamiento de datos- de forma que se facilite tanto la concienciación y el potencial europeo como la competencia en el entorno internacional. La Estrategia Digital Europea, junto con el Libro Blanco de Inteligencia Artificial, y la revisión de la Directiva NIS, y su consecuente aplicación, van a marcar las bases para la construcción de un ecosistema digital fuerte.

La Estrategia Digital que seguirá Europa en los próximos años

El pasado 20 de febrero la Comisión Europea dio a conocer su Estrategia Digital Europea con el objetivo de presentar una sociedad europea impulsada por soluciones digitales que sitúan en el lugar preferente a las personas, abriendo nuevas oportunidades para las empresas y dando impulso al desarrollo de una tecnología fiable que fomente una sociedad abierta y democrática y una economía dinámica y sostenible.

Estos son los primeros pasos hacia una Europa digitalizada capaz de competir con el gigante estadounidense. La Comisión Europea propone "un enfoque internacional abierto y proactivo", con instrumentos que permitan analizar de forma continua los flujos de datos y el desarrollo económico del sector de procesamiento de datos. Todo ello en colaboración con la normativa impuesta por el Reglamento General de Protección de Datos y los organismos públicos encargados de su cumplimiento.

La Estrategia Digital Europea trata de consolidar los ecosistemas europeos de investigación, desarrollo e innovación por medio de la elaboración de una estrategia industrial, otra de datos y otra de inteligencia artificial. Todas son medidas para digitalizar y dinamizar la UE y movilizar a los Estados miembro para, de esta manera, aumentar su autonomía tecnológica y competitividad industrial.

La Estrategia pretende abordar problemas como los desequilibrios en el poder del mercado o la ciberseguridad a través de la implantación de medidas políticas y financieras, como la creación de un **marco de gobernanza intersectorial para el acceso y la utili-**

zación de los datos, que se encargará de crear un marco legislativo operativo para la gobernanza de los espacios comunes de datos con el objetivo de tomar decisiones en torno a qué datos pueden usarse en según qué situaciones, facilitar la utilización transfronteriza y dar prioridad a los requisitos de interoperabilidad, y es que la cuestión de la transferencia de datos transfronteriza ha dado mucho de qué hablar este año. Recientemente, hemos conocido la sentencia dictada por el Tribunal de Justicia de la Comunidad Europea en el llamado "caso Schrems", que declaró inválida la Decisión 2000/520/CE adoptada por la Comisión Europea acabando con en conocido Acuerdo Safe Harbor o Puerto Seguro, y nos hizo replantearnos en qué punto está Europa digitalmente con respecto al resto de continentes.

Los datos se han convertido en uno de los principales activos de la economía digital, un número muy limitado de agentes controlan, no solo una parte importante de los mercados digitales globales, sino también, los datos que se transmiten por las redes y las tecnologías disruptivas que habilitan la digitalización. Este es uno de los motivos por los que se contempla la implantación de una "Ley de aplicación de los conjuntos de datos de alto valor", con el objetivo de abrir los conjuntos de datos de referencia del sector público, es decir, ponerlos a disposición de los usuarios de forma gratuita en toda la Unión Europea.

Para ello, la Estrategia plantea crear unos **"Habilitadores"**, que consiste en la inversión en datos y el fortalecimiento de infraestructuras tecnológicas de Europa a través de una nueva estrategia industrial y la creación de unos "espacios de datos comunes e interoperables en toda la UE" en sectores estratégicos.

Asimismo, el documento hace referencia al **"empoderamiento de los individuos e inversión en habilidades y en PYMES"** a través de la actualización del Plan de Acción de Educación Digital. Se trata de adoptar medidas para facilitar la competitividad y la innovación de todas las cadenas de valor de las pequeñas y medianas empresas, así como ampliar la reserva de talentos digitales para que puedan desplegar las últimas tecnologías en las empresas de toda la UE. También es importante recalcar en este apartado la necesidad a nivel Europeo de invertir en I+D. Para la construcción de un ecosistema digital fuerte y seguro hay que apostar por tecnologías disruptivas, sin embargo, el nivel de inversión en I+D en Europa es muy inferior a otras regiones. La inversión en TICs en Estados Unidos llega a triplicar la de Europa en el sector, lo que nos demuestra que aún nos queda mucho trabajo por hacer.

La Inteligencia Artificial, clave para el futuro de la tecnología

Una de las claves que contempla la Comisión Europea reside en apostar por la Inteligencia Artificial (IA). El Libro Blanco sobre Inteligencia Artificial busca informar sobre cómo proceder a la implantación de la IA en las organizaciones. Es importante que la Unión Europea cuente con un enfoque común, dando lugar a que cualquier marco regulador de la IA sea el mismo, tanto para los Estados miembros de la UE como para las instituciones, oficinas, órganos y organismos de la UE.

La Inteligencia Artificial conlleva riesgos, por lo tanto, es necesario -como ya manifestó en su día el European Data Protection Supervisor- que seamos prudentes a la hora de su implantación. Una adopción rápida por parte del sector público es esencial, pero debemos valorar los beneficios, costes y riesgos de manejar grandes cantidades de datos con una tecnología tan nueva.

Para la Unión Europea constituye un reto aprovechar las oportunidades que la IA nos ofrece, e implantar su "marca europea" en el desarrollo de las mismas. Desde la UE se muestran a favor de un enfoque orientado a la regulación y la inversión con dos objetivos principales que armonicen los esfuerzos a escala regional, nacional y europea:

"En colaboración con los sectores público y privado, los objetivos del marco son movilizar recursos para obtener un "ecosistema de excelencia" a lo largo de toda la cadena de valor, partiendo de la investigación y la innovación, así como crear los incentivos adecuados para acelerar la adopción de soluciones basadas en la inteligencia artificial,

también por parte de las pequeñas y medianas empresas (pymes)". Este "ecosistema de excelencia" se une a un "ecosistema de confianza", que será el encargado del cumplimiento de la normativa europea, sobre todo, aquellas referentes a la protección de los derechos fundamentales y los derechos de los consumidores, y en concreto con relación a los sistemas de inteligencia artificial que operan en la UE y presentan un riesgo elevado. Se trata de "generar un ecosistema de confianza que constituya un objetivo político en sí mismo, y debe ofrecer seguridad a los ciudadanos para que adopten las aplicaciones de la inteligencia artificial y seguridad jurídica a las empresas y organismos públicos para que innoven usando esta última. La Comisión respalda firmemente un enfoque antropocéntrico que se base en la generar confianza en la Inteligencia Artificial centrada en el ser humano, y tendrá en cuenta también los resultados obtenidos durante la fase de prueba de las directrices éticas elaboradas por el grupo de expertos de alto nivel sobre la IA".

El nuevo marco regulador de la IA debe ser eficaz para alcanzar sus objetivos sin ser excesivamente prescriptivo, ya que podría generar una carga desproporcionada, en especial para las pymes. La Comisión considera que debe seguir un enfoque basado en el riesgo. Sin embargo, es necesario contar con criterios específicos para medir las diferencias entre las distintas aplicaciones de la Inteligencia Artificial. ¿Cómo saber si el riesgo es elevado o no? La Comisión establece que una aplicación de IA debe considerarse de "alto riesgo" en función de lo que esté en juego, ponderando entre el sector que la desarrolla, el uso de la misma, los derechos de los consumidores y los derechos fundamentales.

La revisión de la Directiva NIS, una Europa apta para la era digital

Por otro lado, se está llevando a cabo la revisión de la Directiva NIS sobre la seguridad de las redes y los sistemas de información, que surgió debido al incremento de los incidentes relacionados con la ciberseguridad en la Unión Europea y fue aprobada por el Parlamento Europeo el 6 de julio de 2016 entrando en vigor en agosto de ese mismo año.

La revisión Directiva NIS prevé medidas jurídicas para impulsar el nivel general de ciberseguridad en la UE garantizando la preparación de los Estados Miembros, de manera que les exigirá estar debidamente equipados, por ejemplo, mediante un Equipo de respuesta a incidentes de seguridad informática (CSIRT) y una autoridad nacional competente en materia de NIS. De la misma manera, pretende fomentar la cooperación entre todos los Estados miembros, mediante la creación de un grupo de cooperación, a fin de apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros, promoviendo una cooperación operacional rápida y eficaz en relación con incidentes concretos de seguridad cibernética y el intercambio de información sobre

los riesgos.

Es necesario avanzar hacia una cultura de seguridad en todos los sectores que son vitales para nuestra economía y sociedad y que, además, dependen en gran medida de las TIC, como la energía, el transporte, el agua, la banca, las infraestructuras de los mercados financieros, la atención sanitaria y la infraestructura digital. La directiva establece que "las empresas de estos sectores, que son identificadas por los Estados miembros como operadores de servicios esenciales, tendrán que adoptar las medidas de seguridad adecuadas y notificar los incidentes graves a la autoridad nacional competente". Asimismo, los principales proveedores de servicios digitales (motores de búsqueda, servicios de computación en la Nube y mercados en línea) tendrán que cumplir con los requisitos de seguridad y notificación de la nueva Directiva.

El artículo 23 de la Directiva exige que la Comisión Europea revise periódicamente el funcionamiento de esta Directiva. Como parte de su objetivo político clave de hacer que "Europa sea apta para la era digital", así como en consonancia con los objetivos de la Unión de Seguridad. La Comisión anunció en su Programa de Trabajo 2020 que llevaría a cabo la revisión a finales de 2020, por lo que el 7 de julio de 2020 se abrió una consulta que finalizará el próximo 2 de octubre de 2020. Los resultados de esta consulta se utilizarán para la evaluación y la valoración de los efectos de la Directiva NIS.

”

El artículo 23 de la Directiva exige que la Comisión Europea revise periódicamente el funcionamiento de esta Directiva. Como parte de su objetivo político clave de hacer que "Europa sea apta para la era digital"

UN CAFÉ CON LOS EXPERTOS

"La colaboración público–privada y con la sociedad civil se ha convertido en una necesidad real"

Mar López entró a formar parte de la Oficina de Asuntos Estratégicos del Departamento de Seguridad Nacional en 2012, y en abril de 2013 es nombrada Jefa de Seguridad, para posteriormente ocupar el puesto de Jefa de la Oficina de Seguridad y Tecnologías de la Información del DSN. En la actualidad es la Jefa de la Oficina de Ciberseguridad y se encarga de desarrollar y dirigir los proyectos e iniciativas de su área de competencia, participando en el desarrollo estratégico de la Ciberseguridad a nivel nacional.

El pasado 21 de febrero se aprobó en la reunión del Consejo Nacional de Ciberseguridad, ratificándose su constitución oficial el 10 de julio la creación del Foro Nacional de Ciberseguridad, ¿con qué objetivo se constituye?

El Foro Nacional es un organismo de debate, consulta y cooperación, y sus actividades se ciñen a los aspectos más estratégicos relacionados con la formulación de la política de Seguridad Nacional en este ámbito. Su constitución ya se anunciaba en el capítulo cinco de la Estrategia Nacional de Ciberseguridad de 2019. En concreto, una de las medidas de su línea de actuación cuatro "Impulsar la Ciberseguridad de ciudadanos y empresas" propone la creación del Foro Nacional de Ciberseguridad con el objetivo de dar respuesta a las dudas y preocupaciones que se asocian a la ciberseguridad en un entorno de colaboración global.

Es importante resaltar que el Foro es un órgano que asiste al Consejo Nacional de Ciberseguridad en su condición de órgano de apoyo en materia de ciberseguridad al Consejo de Seguridad Nacional y, por tanto, ya forma parte de la gobernanza de la ciberseguridad nacional. Se centra principalmente en articular y cohesionar un entorno de colaboración público-privada que, a través de diferentes líneas de acción, genere el máximo conocimiento sobre los desafíos a la Seguridad Nacional en el ciberespacio, ya sean oportunidades o amenazas. También es importante destacar la amplia participación, la integración multidisciplinar, y el compromiso de las partes bajo el paraguas de la responsabilidad compartida y la reciprocidad.

¿Quiénes serán los encargados de ponerlo en marcha y establecer las líneas de acción del Foro?

El Consejo Nacional de Ciberseguridad, tal y como se produjo el día 10 de julio, es el principal líder del equipo. Sus documentos de referencia son las estrategias, la de Seguridad Nacional y la de ciberseguridad, por tanto, las líneas de acción a seguir son las que propusimos entre todos. Entre las funciones del Consejo

MAR LÓPEZ

Jefa de la Oficina de Seguridad y de Tecnologías de la Información del Departamento de Seguridad Nacional (DSN).

dsn.gob.es

de Ciberseguridad se establece el examinar las propuestas de trabajo del foro, así como el nombramiento para ocupar la presidencia, vicepresidencias y vocalías del foro. Además, este es un canal bidireccional. Del Consejo al foro y del foro al Consejo, un constante feedback de actuaciones que se encuadran en el desarrollo de la Estrategia Nacional de Ciberseguridad.

En dicho marco, el Consejo aprobó la constitución y puesta en marcha con una estructura basada en una Presidencia (DSN), dos Vicepresidencias (INCIBE y CCN), una Secretaría y las unas Vocalías que representaran ampliamente a la sociedad civil (Asociaciones empresariales y de usuarios, universidad, Think-tanks, medios de comunicación…), sin limitar la posibilidad de convocar a otros representantes. Esto es un equipo multidisciplinar responsable de establecer la priorización de actuaciones que recoge la Estrategia de ciberseguridad y de elevar propuestas al Consejo para su ejecución y puesta en marcha.

Iván Redondo, jefe del Gabinete de la Presidencia del Gobierno, ha destacado la colaboración público-privada para el desarrollo del Foro Nacional de Ciberseguridad, ¿por qué cree que es tan importante?

Sin duda, la colaboración público–privada y con la sociedad civil se ha convertido en una necesidad real que nos permite afrontar los problemas relacionados con la seguridad digital y la ciberseguridad. Esta colaboración permite trabajar de forma coordinada tanto a las Administraciones públicas, como a las empresas y la ciudadanía con el objetivo de alcanzar el mismo fin común. El objetivo

es perfeccionar dicha colaboración para conseguir cohesionar las actuaciones público-privadas generando el máximo conocimiento y articulando respuestas eficaces y eficientes.

¿Cuáles son los principales ejes a abordar?

Entre las funciones especificas que abordará el foro se encuentran algunas como la propuesta de iniciativas al Consejo Nacional de Ciberseguridad dirigidas a la potenciación y creación de sinergias público-privadas en materia de ciberseguridad o ciberdefensa. También el análisis y estudio de determinadas propuestas, que permitan apoyar la toma de decisiones del Consejo Nacional de Ciberseguridad.

Por otro lado, contribuirá a la valoración y análisis de los riesgos y amenazas; podrá apoyar la realización y evaluación de ejercicios de gestión de crisis en el ámbito de la ciberseguridad y la ciberdefensa; así como contribuir a la identificación de las necesidades de la industria y de los centros de investigación, o colaborar en la realización de catálogos de recursos que identifiquen los medios y capacidades del sector privado y la sociedad civil. Asimismo, es uno de los medios para canalizar y formular propuestas sobre el marco regulatorio y normativo con incidencia sobre la ciberseguridad; impulsará la realización proactiva de estudios, informes y análisis, e ideará iniciativas tendentes a promover la cultura Nacional de Ciberseguridad, entre otras.

¿Qué requisitos son necesarios para participar en él?

El Consejo Nacional de Ciberseguridad

"Es un canal bidireccional, del Consejo al foro y del foro al Consejo, un constante feedback de actuaciones que se encuadran en el desarrollo de la Estrategia Nacional de Ciberseguridad."

"Quizás nos queda avanzar más en la mejora de la cualificación de profesionales y en el marco de la recualificación, por ello, una de las líneas prioritarias del foro es la promover la capacitación en ciberseguridad de los profesionales y detectar, fomentar y retener el talento."

ha establecido una serie de criterios centrados en aglutinar a las principales organizaciones que representan a la sociedad civil, al mundo académico y a los sectores público y privado de España como punto focal de sus actuaciones. En este sentido, las principales organizaciones que conforman el foro en representación del sector privado son: la CEOE; CEPYME; ATA o las Cámaras de Comercio de España, entre otras, entre las que se incluyen ISMS Forum.

Por otra parte, el Foro tiene la capacidad de crear grupos de trabajo que complementarán el desarrollo de las medidas recogidas en la Estrategia Nacional de Ciberseguridad y a través de los cuales, se ampliará la participación de otros actores de la ciberseguridad nacional. Los expertos que formarán dichos grupos de trabajo serán propuestos a través de los vocales representantes en el foro.

El Foro se crea como una necesidad de apoyo a la Estrategia Nacional de Ciberseguridad, ¿cuáles son las líneas estratégicas a desarrollar tanto en emprendimiento como en lo que a incentivos se refiere para mejorar la ciberseguridad en España?

La Estrategia Nacional de Ciberseguridad en sus líneas de acción 4 y 5 establece por una parte Impulsar la ciberseguridad de ciudadanos y empresas y por otra Potenciar la industria española de ciberseguridad y la generación y retención de talento, para el fortalecimiento de la autonomía digital. En este sentido, el foro ha creado un grupo de trabajo para proponer el desarrollo de las medidas incluidas en dichas líneas de acción.

En años anteriores se ha hablado de la necesidad de fomentar medidas para la formación de profesionales en ciberseguridad, ¿en qué punto se encuentra esta cuestión?

Este mismo año, y en lo que se refiere a formación para el empleo, el pasado 4 de julio el Consejo de Ministros, a propuesta del Ministerio de Educación y Formación Profesional, aprobó dos nuevos títulos de especialización de Formación Profesional de Grado Superior en ciberseguridad en el entorno de las tecnologías de la operación, la ciberseguridad y las tecnologías de la información, complementando así las competencias de quienes ya disponen de un título de FP.

Quizás nos queda avanzar más en la mejora de la cualificación de profesionales y en el marco de la recualificación, por ello, una de las líneas prioritarias del foro es la "promover la capacitación en ciberseguridad de los profesionales" y "detectar, fomentar y retener el talento".

Las amenazas en internet son uno de los principales retos para la seguridad nacional. En 2019 el Instituto Nacional de Ciberseguridad (INCIBE) registró 72.858 ciberataques y el Centro Criptológico Nacional (CCN) gestionó 42.997 incidentes, la mayoría contra la Administración. ¿Cómo puede el Foro Nacional de Ciberseguridad ayudar a reforzar la concienciación sobre el riesgo de los ciberataques?

No hay duda alguna que la cultura de ciberseguridad nacional es uno de los temas que más nos preocupan. Tanto la Ley de Seguridad Nacional de 2015 como la Estrategia de Seguridad Nacional de 2017 apuntan a la acción prioritaria de acercar la Seguridad Nacional a la sociedad en general.

Por otro lado, la ENCS19 establece un objetivo concreto para el desarrollo de una Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas y le dedica una Línea de acción completa, la última, y quizás una de las más importantes: Desarrollar una Cultura de Ciberseguridad. En este sentido y a fin de ampliar la capilaridad de la ciberseguridad en la sociedad, el foro ha creado un tercer grupo de trabajo, que desarrollará un plan que será trasversal a todas las acciones que desarrolle el foro y, a la par, contribuirá al Plan Nacional de Cultura de Seguridad Nacional, actualmente en desarrollo.

¿Qué supone la creación de un Foro Nacional de Ciberseguridad tanto a nivel nacional como internacional y europeo?

Tener instrumentado el foro supone, por un lado, estar en constante comunicación con la sociedad sobre las materias trabajadas en el contexto internacional y europeo; canalizar acciones y solicitar contribuciones a las iniciativas que se lancen y apoyen la toma de decisiones.

Esto resulta en la creación de un importante y participado conglomerado en el que España, en su conjunto, participe y sea cada vez más influyente en el ámbito de la ciberseguridad, lo cual no se consigue sino existe un alineamiento y visión común de cómo y dónde queremos estar, con una filosofía de trabajo conjunto y en equipo que, sin duda, el foro facilita.

"La protección de datos no existe para poner trabas al desarrollo tecnológico"

LEONARDO CERVERA

Director, European Data Protection Supervisor (EDPS).

edps.europa.eu

Fotografía
XII Foro de la Privacidad de ISMS Forum (CaixaForum Madrid)

Leonardo Cervera comenzó su carrera como abogado en ejercicio y profesor de derecho internacional público y ha trabajado en cuestiones de protección de datos y propiedad intelectual en la Comisión Europea. En el año 2006 recibió el Premio Barbara Wellbery por su contribución legal y doctrinal a las transferencias internacionales de datos, y en el año 2007- 2008 fue seleccionado como EU fellow en la prestigiosa Universidad de Duke. También es autor de diversos artículos doctrinales en materia de protección de datos.

Ya han pasado casi dos años desde la aplicación del Reglamento, ¿qué balance se puede sacar en este tiempo? ¿se contemplan mayores avances?

El balance de la aplicación del Reglamento es claramente positivo. Con la aprobación del Reglamento, los niveles de concienciación y cumplimiento por parte de las empresas y la ciudadanía son hoy en día mucho más elevados que en el pasado y la Unión Europea ha consolidado su liderazgo a nivel mundial. Eso no quiere decir que todo funcione a la perfección y el informe de la Comisión Europea, por ejemplo, establece una larga lista de propuestas de mejora que habrá que ir abordando poco a poco. Pero el balance es netamente positivo y es evidente que se avanza en la buena dirección.

¿Reforzar los derechos individuales en materia de privacidad a través del RGPD se traduce en un mercado con mejores garantías?

Es obvio que el refuerzo de los derechos individuales no se ha hecho por razones mercantiles, pero a largo plazo el impacto sobre el mercado será también positivo. Esto no es algo exclusivo del mercado digital. Lo mismo sucede en otros mercados en los que intereses puramente económicos pueden comprometer la sostenibilidad del sistema, por ejemplo desde el punto de vista del respeto al medio ambiente. Como ha dicho recientemente y con gran acierto David Sassoli, Presidente de Parlamento Europeo, el modelo de crecimiento infinito no es sostenible y lo mismo se puede decir sobre el tratamiento de los datos personales en Internet.

En ocasiones, las empresas no notifican las brechas de seguridad hasta que el riesgo es muy alto, ¿a qué se debe este comportamiento?

En mi opinión, el sistema de notificaciones en casos de brechas de seguridad está funcionando razonablemente bien. Por lo menos, esa es la experiencia que tenemos como autoridad de supervisión de las instituciones europeas. Es posible que algunas empresas, quizás por miedo a las sanciones o a la mala publicidad, traten de minimizar los riesgos, pero yo creo que las empresas con un delegado de protección de datos y un buen sistema de control cumplen bien con los requisitos de la normativa a este respecto.

En una entrevista al periódico *El Economista* en mayo de 2019 declaró "Veremos multas importantes por Protección de Datos en pocos meses". ¿Se están dando ya estas multas de cantidades cuantiosas? ¿Cuáles son los objetos de sanción más comunes?

Ha habido muchas sanciones a nivel nacional por incumplimiento del Reglamento y en un amplio espectro de cuestiones. Lo que muchos echamos en falta, y de ahí la reciente propuesta del Supervisor Europeo de crear un "Support Pool of Experts" en el Comité Europeo de Protección de Datos, es un mayor número de operaciones conjuntas entre las autoridades nacionales y una mayor cooperación práctica a la hora de abordar casos transfronterizos de particular relevancia. Es evidente que en este sentido queda todavía mucho que hacer.

Durante su intervención en el XII Foro de la Privacidad de ISMS Forum afirmó lo siguiente: estoy echando en falta esquemas de certificación y códigos de conducta. En su opinión, ¿cuáles deberían ser indispensables?

La filosofía de los sistemas de certificación y de los códigos de conducta es que sean los propios interesados los que se sienten alrededor de una mesa y hagan propuestas al regulador. Hay infinidad de sectores y la investigación pública o los sistemas de salud son ejemplos evidentes, en los que los operadores públicos y privados se beneficiarían mucho de estos mecanismos que aumentan en la práctica las garantías para los ciudadanos y dotan de mayor claridad y seguridad jurídica a los operadores.

Recientemente se ha publicado una revisión de la Directiva E Privacy, ¿hasta qué punto el RGPD y esta normativa son complementarias?

La complementariedad del RGPD y la Directiva E-Privacy ha sido objeto de estudio por parte del Comité Europeo de Protección de Datos. Es difícil hacer juicios de valor definitivos teniendo en cuenta que la Directiva se encuentra en estos momentos en proceso de reforma, probablemente será el Comité Europeo de Protección de Datos el encargado de recibir las competencias de garantizar la consistencia en la aplicación del futuro Reglamento E-Privacy, como ya las tiene para el RGPD, por lo que no veo motivos para pensar que la complementariedad entre ambas normas vaya a ser un problema serio.

El Big Data, el Machine Learning, la Inteligencia Artificial o la robótica son el futuro, pero ¿son también un peligro para las buenas prácticas en las empresas o se prevé una guerra sucia digital?

Fotografía
XII Foro de la Privacidad de ISMS Forum (CaixaForum Madrid)

Una de las novedades más significativas del nuevo Supervisor Europeo, Wojciech Wiewiorowski, es una aproximación mucho más positiva y constructiva hacia la tecnología en general. La protección de datos no existe para poner trabas al desarrollo tecnológico o la innovación sino para que el desarrollo tecnológico se haga conforme a nuestros valores y la garantía última de la inviolabilidad del principio de la dignidad del individuo. Europa, y España en particular, tienen que estar en la vanguardia del desarrollo tecnológico en los albores de la Cuarta Revolución Industrial, con tecnologías verdes, seguras y sostenibles desde la perspectiva de los derechos y libertades de los ciudadanos.

¿Cuáles son los primeros problemas que surgen a la hora de "ponerle límites" a la Inteligencia Artificial?

Existe la tendencia a considerar Inteligencia Artificial a infinidad de aplicaciones que en realidad no son más que desarrollos tecnológicos basados en sistemas existentes desde hace años. La recomendación del Supervisor Europeo es que para la mayoría de las aplicaciones prácticas de la denominada Inteligencia Artificial basta con establecer algunos sistemas de transparencia y control. Solo en casos excepcionales, en los que la tecnología no haya sido testeada mínimamente y un análisis de riesgo determine una alta probabilidad de daño para las personas, habría que considerar controles ex-ante y regulación específica, pero siempre con la debida preocupación de que estos límites no terminen actuando como una barrera a la innovación bien entendida.

¿Es posible la convivencia entre la innovación y la protección de los datos personales? ¿Qué opina de que algunas empresas se "salten" la barrera de seguridad en detrimento de esa innovación?

En la Unión Europea, la convivencia de la innovación y la protección de datos no es solo posible sino legalmente exigible, como se deriva de los principios de privacidad por diseño y por defecto establecidos en el Reglamento. Una innovación que no respete el derecho fundamental a la protección de datos no tiene cabida en el sistema de valores de nuestra Unión. Los principios de responsabilidad proactiva y procesamiento basado en el riesgo del Reglamento otorgan suficiente flexibilidad para que los datos personales se puedan tratar y puedan circular libremente en el territorio de la Unión.

Actualmente, cuando no pagamos por un servicio, solemos "pagar" con nuestros datos, ¿qué opina de la monetización de nuestros datos personales? ¿Hasta qué punto puede ser peligrosa?

El Supervisor Europeo está firmemente en contra de la monetización de los datos personales. Un derecho fundamental no puede ser objeto de mercadeo. Los modelos de negocio basados en la obtención de ingresos mediante la publicidad personalizada deberían reflexionar sobre su sustentabilidad a medio o largo plazo y considerar posibles alternativas. Ya se observan en el mercado algunos movimientos en este sentido, por ejemplo, en lo relativo a las cookies.

"Las pymes no siempre disponen de los conocimientos especializados"

PROKOPIOS DROGKARIS

Network and Information Security Expert, European Union Agency for Cybersecurity (ENISA).

enisa.europa.eu

Fotografía
XII Foro de la Privacidad de ISMS Forum
CaixaForum Madrid

Prokopios Drogkaris trabaja en las áreas de Privacidad y Protección de Datos, Certificación de Seguridad y Servicios de Confianza, y ha participado en varios proyectos de investigación financiados por la UE en el área de Seguridad de la Información dentro del Hellenic Ministry of Citizen Protection. Es autor de varias publicaciones científicas y ha colaborado como miembro de programas y comités organizadores en conferencias científicas internacionales y europeas.

¿Cree que las pequeñas y medianas empresas se están adaptando y evolucionando al mismo nivel que las grandes organizaciones al nuevo Marco Europeo de Protección de Datos?

El Reglamento General de Protección de Datos lleva en vigor más de dos años y las pymes de la Unión Europea se están adaptando y evolucionando, concretamente, en lo que respecta a la seguridad del tratamiento de datos personales, creo que se han dado pasos importantes, tanto en lo que se refiere a la sensibilización como al despliegue de medidas técnicas y organizativas adecuadas.

En los últimos años, la ENISA ha emprendido actividades de presentación de directrices, casos de uso práctico y una herramienta on line, con énfasis en las

pymes, sobre la adopción de medidas de seguridad para la protección de los datos personales. Asimismo, la Agencia también ha publicado informes sobre el concepto de la privacidad por diseño como principio fundamental de la incorporación de salvaguardias de protección de datos en el núcleo de los productos TIC y los servicios on line. En este contexto, también trabajamos con las Privacy enhancing technologies (PETs) que pueden apoyar la integración de la privacidad en los sistemas y servicios modernos.

Desde el punto de vista de la ENISA, ¿están las pymes preparadas para asumir los requerimientos del RGPD y aplicar las medidas adecuadas para la protección de datos personales? ¿Es frecuente la falta de capacitación y recursos en las pequeñas y medianas empresas?

Una de las obligaciones fundamentales de todas las empresas, incluidas las pymes, que actúan como controladoras o procesadoras de datos, es la de la seguridad de los datos personales. Según el RGPD, la seguridad abarca por igual la confidencialidad, la integridad y la disponibilidad, y debe considerarse siguiendo un enfoque basado en el riesgo: cuanto mayor sea el riesgo, más rigurosas serán las medidas que el controlador o el encargado del tratamiento deban adoptar.

Aunque este enfoque basado en el riesgo no es un concepto nuevo, solo se han presentado unos pocos marcos específicos de evaluación de riesgos para la privacidad, centrados principalmente en la evaluación de riesgos de datos personales y la adopción de las medidas de seguridad pertinentes. Si bien las grandes empresas tienen la posibilidad de responder a esos marcos y aplicarlos adecuadamente, las pymes no siempre disponen de los conocimientos especializados y los recursos necesarios para hacerlo. En muchos casos, a las pymes les resulta difícil comprender las especificidades de los riesgos relacionados con el procesamiento de datos personales, así como evaluar y gestionar esos riesgos siguiendo una metodología formal. Esto puede poner en peligro los datos personales procesados por las pymes, obstaculizando al mismo tiempo el cumplimiento de sus obligaciones con respecto al PIB. Y es aquí donde los documentos de orientación, el intercambio de mejores prácticas y la formación y la sensibilización específicas podrían ser de gran ayuda.

¿Cuál es la principal función de la nueva herramienta de la ENISA "Evaluación del nivel de riesgo de una operación de tratamiento de datos personales"?

La plataforma en línea de la ENISA para la seguridad del procesamiento de datos personales se basa en un conjunto de directrices publicadas por la Agencia en 2017 y tiene como objetivo proporcionar una herramienta sencilla que apoye la seguridad de los datos personales. La plataforma consta de dos partes principales: un enfoque de evaluación de los riesgos de seguridad para el procesamiento de datos personales, y una herramienta de autoevaluación de la seguridad para los controladores y procesadores de datos.

La primera parte guía a las organizaciones a través de sus operaciones específicas de procesamiento de datos y les ayuda a comprender y evaluar los riesgos

de seguridad pertinentes, así como a seleccionar las medidas de seguridad adecuadas. El enfoque propuesto se basa en cinco pasos principales: i) Definición de la operación de tratamiento y su contexto; ii) comprensión y evaluación del impacto; iii) definición de las posibles amenazas y evaluación de su probabilidad; iv) evaluación del nivel de riesgo; y v) selección de las medidas de seguridad, siguiendo la categorización prevista en el anexo A de la norma ISO/CEI 27001:2013 y en la norma ISO/CEI 27002:2013.

La segunda parte es la opción de autoevaluación, que tiene por objeto seguir apoyando a los controladores/procesadores de datos después de la evaluación inicial de los riesgos, presentando un instrumento práctico de autoevaluación sobre la forma en que avanza el despliegue de las medidas de seguridad.

¿Cuáles son los errores más cometidos según la herramienta a la hora de realizar un análisis del riesgo de la empresa? ¿Qué conclusiones podemos sacar para realizar una buena evaluación de impacto?

La seguridad de los datos personales se ajusta en la práctica a los principios generales de la seguridad de la información y la gestión de los riesgos para la seguridad de la información, sin embargo, tienen ciertas especificidades que deben tenerse en cuenta al analizar los riesgos de seguridad y adoptar medidas. Esas especificidades se derivan principalmente del marco jurídico subyacente de la Unión Europea en materia de protección de datos (RGPD), así como de la naturaleza de los datos personales per se.

En el proceso "típico" de evaluación de riesgos, los riesgos se estiman sobre la base de sus posibles repercusiones en la organización. Sin embargo, en el caso del procesamiento de datos personales, los impactos se consideran con respecto a las libertades y derechos de las personas. Esta es una diferencia significativa, ya que se cambia el análisis de los impactos hacia los posibles efectos adversos que pueda sufrir un individuo, incluidos, por ejemplo, el robo o fraude de identidad, las pérdidas financieras, los daños físicos o psicológicos, la humillación, los daños a la reputación o incluso la amenaza de muerte. Al realizar ese análisis, la escala (por ejemplo, el número de personas afectadas) puede no ser pertinente: el impacto es elevado aunque pueda acarrear graves efectos adversos solo para una persona.

En estos últimos años se ha ido desdibujando la barrera que separaba la ciberseguridad de la privacidad llegando a converger absolutamente, ¿a qué se debe este cambio?

Cuando se habla de seguridad y protección de los datos personales, suele existir la percepción de que estos dos conceptos son distintos, o incluso son contradictorios. Aunque la seguridad de los datos personales siempre ha sido una obligación jurídica para los responsables del tratamiento de datos en virtud de la Directiva sobre la protección de datos, el RGPD refuerza las disposiciones pertinentes (tanto en cuanto al fondo como al contexto), extendiendo al mismo tiempo esta responsabilidad directamente también a los responsables del tratamiento de datos.

Es importante señalar que la seguridad

(en el sentido de integridad y confidencialidad) se establece como uno de los principios relativos al tratamiento de datos personales (artículo 5 de la RBP). Esto sitúa la seguridad en el centro de la protección de los datos junto con el resto de los principios de protección de los datos, es decir, la legalidad, la equidad y la transparencia, la limitación de los fines, la exactitud y la limitación del almacenamiento. Siguiendo este principio general, la seguridad del tratamiento de los datos personales se ordena principalmente en el artículo 32 de la RBP.

A nivel particular, como experto en seguridad de redes e información, ¿cuáles son las actividades en las que se centra actualmente?

El año pasado entró en vigor la Cybersecurity Act Regulation que, entre otras cosas, estableció el marco de certificación de seguridad cibernética de la UE. La ENISA desempeña un papel fundamental en el establecimiento del marco y en la propuesta de planes de certificación de la seguridad cibernética candidatos a la Comisión Europea. Si bien estos planes de certificación establecidos en virtud de la Ley de ciberseguridad no abordan explícitamente la protección de los datos y la privacidad, contribuyen a aumentar la confianza de los consumidores en los servicios, productos y servicios digitales.
Además de la labor de apoyo a la ENISA en la aplicación de políticas de seguridad y privacidad, estoy trabajando en la interacción entre la seguridad y la privacidad, las tecnologías de mejora de la privacidad (PET) y la orientación práctica sobre los principios de la seguridad y la privacidad por diseño.

En muchos casos, a las pymes les resulta difícil comprender las especificidades de los riesgos relacionados con el procesamiento de datos personales, así como evaluar y gestionar esos riesgos siguiendo una metodología formal."

FIRMA INVITADA

FIRMA INVITADA

El futuro de la ciberseguridad

Soledad trabaja en Berkeley Lab, uno de los centros científicos más prestigiosos del mundo y uno de los primeros nodos de ARPANET, la red precursora de Internet, como ingeniera del departamento de ciberseguridad. Además, compagina su trabajo en Berkeley Lab con la responsabilidad de ser la jefa de seguridad de SC, la conferencia anual de supercomputación de Estados Unidos, protegiendo y construyendo la arquitectura de red de SCinet, la red mas rápida del mundo.

¿ESTÁ LA CIBER GUERRA PERDIDA O TODAVÍA SE PUEDE GANAR?

Por un lado, la ventaja es que la guerra es interminable. No hay fin. Hay mil batallas que luchar. No hay descanso. Aun así puede parecer que el barco ya zarpó hace muchísimo tiempo. Solo algunos avanzados lograron atajar a tiempo lo que se veía venir hace años: que íbamos a salir perdiendo. Una de las premisas de la ciberseguridad es que cuanto más se tarda en atajar un problema de seguridad más costoso es arreglarlo, tanto en tiempo como en dinero. Ya no hablemos si el agujero de seguridad ha sido explotado, lo que conlleva pérdidas económicas y de reputación bastante grandes.

Adoptar una cultura de seguridad "from the ground floor" en este caso es lo correcto si se quiere ganar. La seguridad se debe instalar y anclar en la cultura corporativa desde los niveles de gestión hasta los niveles técnicos. Esto significa que en cada paso de los ciclos de vida de cualquier tecnología usada ya sea software, hardware o redes de transmisión de datos, exista una base de seguridad. Se debe invertir para crear una

SOLEDAD ANTELADA

Ingeniera en Ciberseguridad en NERSC, Berkeley Lab, U.S Departamento de Energía. Jefa de seguridad en red de SC20.

nersc.gov

Fotografía: Jesús Chacón

cultura sostenible que no sea un simple esfuerzo, de esa forma la seguridad se instalará para siempre.

La seguridad debe ser vista por todos como un complemento positivo e importante para el trabajo cotidiano. Una cultura de seguridad que se pone en práctica sensibiliza y alerta a los empleados sobre los riesgos, algo que también beneficia a la empresa. Por lo tanto, el elemento más central de la cultura de la ciberseguridad es el comportamiento humano.

LOS VENDE HUMO

La World Wide Web se inventó en 1989. El primer sitio web entró en funcionamiento en 1991. Hoy en día, hay unos 1800 millones de sitios web (no todos activos) y unos cinco mil millones de usuarios de Internet (51% de la población mundial de 7 mil millones), frente a los 2 mil millones en 2015. Habrá 6 mil millones de usuarios de Internet para 2022 (75% de la población mundial proyectada en 8 mil millones) y más de 7,5 mil millones de usuarios de Internet para 2030 (90% de la población mundial proyectada de 8,5 mil millones).

Al igual que el crimen callejero, que históricamente creció en relación al crecimiento de la población, estamos presenciando una evolución similar del delito cibernético. No se trata solo de ataques más sofisticados, se trata tanto del creciente número de objetivos humanos como digitales. Entonces, ¿a qué tipo de personas estamos encomendando nuestra seguridad? Evitar los típicos "vende humo" es esencial.

Este tipo de profesionales tampoco guardan la ética digna de esta profesión en la cual es clave establecer relaciones de confianza. Alejarse de esas empresas y profesionales es determinante para elevar la profesionalidad del sector y hacer que las mejores soluciones que realmente protegen a las empresas y entidades públicas sean las que queden. Pedir credenciales de los que están al mando y saber, por ejemplo, con quién y qué países están haciendo negocios, ya que puede resultar tan informativo como relevante a la hora de tomar una decisión de compra de un producto.

Se encuentran casos de personas cuya mayor hazaña en su curriculum ha sido trabajar en Opencor, y de repente han pasado a tener un puesto de jefe de ventas de una empresa de ciberseguridad que vende soluciones de ciberseguridad a grandes entidades financieras, o se presenta a concursos públicos para ofrecer dichas soluciones por parte del Estado. Lo único que les importa es vender y lo que venden es humo, haciendo que la ciberseguridad y la profesión no alcance el nivel de excelencia necesario.

EL FUTURO

En 1985 Clifford Stoll astrónomo en Lawrence Berkeley National Laboratory en Berkeley, California, perteneciente al Departamento de Energía de Estados Unidos, descubrió un error de contabilidad de 75 centavos en las cuentas de usuarios que utilizaban los sistemas. Stoll rastreó el error hasta un usuario no autorizado que aparentemente había usado nueve segundos de tiempo de

computación y no había pagado por ello. Stoll finalmente se dio cuenta de que el usuario no autorizado era un hacker que había adquirido acceso de superusuario al sistema del LBNL al explotar una vulnerabilidad en la función movemail del GNU Emacs original.

Stoll conectó 50 terminales e impresoras a las 50 líneas de teléfono entrantes del LBNL los fines de semana y por las noches para monitorear la actividad. Tras identificar la línea por la que provenía la intrusión, Stoll y algunos compañeros en LBNL monitorearon por meses la actividad del hacker. Vieron como los sistemas de LBNL eran utilizados para saltar a otros sistemas de organismos militares de Estados Unidos. Stoll se inventó un departamento en LBNL que tendría un contrato con una red clasificada y ficticia con el fin de despertar la curiosidad del hacker y mantenerlo el tiempo suficiente en línea para que la compañía de telefono localizara su ubicación física real.

El hacker mordió el anzuelo y pasó días intentando conectarse a esta misteriosa red, robando ficheros de información que habían sido creados especialmente para confundirlo. Con el tiempo ganado gracias al *honeypot* y la ayuda de las compañías de telefono en EE.UU y Alemania, Marcus Hess fue detenido en su casa de Hannover. Este fue el primer caso documentado de *hacking*, uso de *honeypot* y monitoreo de actividad de red.

Hoy en día, el problema de monitorear todo lo que pasa en una red, ya sea internet o redes independientes privadas o públicas, se ha convertido en un pro-

> ***"Lo que muchos echamos en falta, y de ahí la reciente propuesta del Supervisor Europeo de crear un "Support Pool of Experts" en el Comité Europeo de Protección de Datos, es un mayor número de operaciones conjuntas entre las autoridades nacionales y una mayor cooperación práctica a la hora de abordar casos transfronterizos de particular relevancia."***

"Los modelos de negocio basados en la obtención de ingresos mediante la publicidad personalizada (y por ende en el tratamiento masivo de datos personales con perfiles de los usuarios cada vez más sofisticados) deberían reflexionar sobre su sustentabilidad a medio o largo plazo y considerar posibles alternativas. "

blema de Big Data. Se están generando grandes cantidades de datos como resultado de la expansión de la redes, la implementación de nuevas herramientas de seguridad y la cantidad y sofisticación de los ataques cibernéticos. Como controlar y mantener seguras redes de hasta múltiples *Terabits* por segundo que generan miles de *Terabytes* de datos y millones de *logs* de red diarios es el reto. Los algoritmos tradicionales ya no sirven para resolver este problema, ¿es la Inteligencia Artificial el futuro de la ciberseguridad?

Si bien hay un enorme debate en torno a la Inteligencia Artificial en general, la intersección de la IA y la ciberseguridad está poco estudiada y subestimada. En este campo hay varias cosas a tener en cuenta:

En primer lugar, la posibilidad de que la Inteligencia Artificial pueda ayudar en la ciberdefensa. Esta idea también es objeto de muchas exageraciones pero parece que hay formas en que la IA ayuda a proteger los sistemas informáticos, descubriendo vulnerabilidades antes de que los hackers lo hagan, detectando intrusos, descubriendo vectores de ataque, o detectando la presencia de código malicioso. Sin embargo, debemos tener cuidado de no dejar que la publicidad (y los vende humo) superen la realidad en este frente.

En segundo lugar, la IA también puede cambiar los ciberataques ofensivos tradicionales. Los hackers modernos en la mayoría de casos no necesitan inteligencia artificial para lograr sus fines, pero también es verdad que algunos

Fotografía: Jesús Chacón

de los ciberataques más potentes que hemos visto presentan algunas formas de propagación automatizada y capacidad de ataque. Por lo tanto, imaginar un mundo en el que las futuras operaciones cibernéticas utilizarán sistemas automatizados más sofisticados y capacidades para lograr tareas particulares, como el descubrimiento de vulnerabilidades, selección de objetivos, comando y control, y ejecución de ataque no está nada lejos de la realidad.

Por último, y no por ello menos importante, es la ciberseguridad de los propios sistemas de Inteligencia Artificial. Estos sistemas tienen la misma probabilidad de ser susceptibles a los tipos de vulnerabilidades que están presentes en otros tipos de software. No hay razón para pensar que los piratas informáticos no intentan explotar esta vulnerabilidades,

La arquitectura de red neuronal que sustenta muchos sistemas de la IA moderna es inmensamente poderosa, pero presenta una nueva clase de ciberseguridad y riesgos que solo estamos comenzando a descubrir. Llamamos a este campo *adversarial learning*, una técnica que intenta engañar a los modelos de aprendizaje al proporcionar información engañosa. De esta forma se pueden hacer que las redes neuronales creen errores extraños, causando que los sistemas que dependen de esas redes fallen o revelen información confidencial, entre otras muchas cosas. Este es un campo que requiere mucha más atención y estudio, no dejemos que pase lo mismo y perdamos la guerra, otra vez.

PROYECTOS DE INTERÉS

Guardedbox, tus secretos a buen recaudo

GuardedBox es un gestor online de almacenamiento seguro y compartición de datos e información, que reúne los requisitos mínimos para almacenar e intercambiar información y datos sensibles de manera segura y de forma sencilla e intuitiva, ya que no requiere de conocimientos técnicos para su uso. La solución utiliza técnicas de criptografía avanzada para garantizar la seguridad, confidencialidad e integridad de la información.

La realidad da lugar a dudas: la pandemia del COVID-19 ha generado una mayor concienciación de la importancia que tiene la ciberseguridad en un escenario como el actual, en el que numerosas organizaciones, instituciones y profesionales desarrollan el grueso de su actividad profesional y personal de forma remota. El intercambio y almacenamiento de secretos digitales como: claves de acceso a sistemas y servicios, credenciales para la autenticación de usuarios (por ejemplo, en conexiones VPN), contraseñas que protegen ficheros confidenciales, certificados digitales, claves criptográficas, entre otros, ponen en riesgo evidente su confidencialidad y favorecen el acceso ilegítimo a sistemas y redes de comunicaciones, y a los datos que estos gestionan.

Por este motivo, Juan José Torres y DinoSec han liberado la versión 1.00 de GuardedBox, una solución de almacenamiento seguro y compartición de secretos online gratuita para toda la comunidad.

Algunos de los principales elementos diferenciadores de la solución GuardedBox son:

- Permite la compartición de información y datos entre individuos y entre grupos.
- Utiliza técnicas de criptografía avanzada.
- El servidor no almacena ningún dato sensible en claro.
- El compromiso del servidor por parte de un atacante no pone en riesgo la información de ningún usuario.

IronChip, la startup vasca que ya triunfa en el mercado internacional

Ironchip es una stratup dedicada a ofrecer servicios técnicos de ingeniería y otras actividades relacionadas con el asesoramiento técnico en ciberseguridad. Fue creada en 2017 por un equipo de dos ingenieros de telecomunicaciones de la universidad de San Mamés de la UPV-EHU, Jose Fernando Gómez, CEO y Julen Martinez Higuero, COO .

La startup comenzó desarrollando una plataforma segura de inversión para un broker después de ser seleccionada para resolver un problema con la autenticación de los usuarios. Como las alternativas eran demasiado complejas, o no eran lo suficientemente seguras Jose Fernando Gómez y Julen Martínez se lanzaron a desarrollar su propio sistema de autenticación de usuarios basado en localización e inteligencia artificial.

Ironchip ha desarrollado y entrenado un conjunto de algoritmos de inteligencia artificial que son capaces de analizar las ondas de radio del ambiente, como pueden ser las señales WiFi o todo tipo de señales móviles, y a partir de ellas, crea una firma única que identifica a cada usuario para acceder a cualquier servicio, sustituyendo contraseñas. Su tecnología evita que un atacante remoto pueda acceder a su servicio si no posee un dispositivo móvil concreto en una geoposición determinada. De esa manera se protegen los accesos a los servicios o datos más críticos de las empresas y organizaciones. Esta tecnología que une el mundo físico y virtual para crear una identidad única asociada a un lugar permite a estas entidades poder protegerse de los cibercriminales de una de las maneras más efectivas del mercado, incluso podrán sustituir sus password por identidades asociadas a lugares físicos.

LO QUE NO TE PUEDES PERDER

ISMS lanza la Guía de Buenas Prácticas en Auditorías RGPD

El pasado 28 de mayo de 2020, durante la celebración de la primera edición de su Foro Digital, ISMS Forum lanzó la Guía de Buenas prácticas en Auditorías RGPD

El principal objetivo de esta Guía es establecer una serie de pautas generales para los responsables del tratamiento de los datos, en relación con la realización de auditorías de cumplimiento con la normativa vigente de protección de datos, dando respuesta a las dudas más frecuentes, en particular, relativas a la necesidad de llevar a cabo auditorías, las obligaciones que forman parte del alcance de la auditoría y la periodicidad de realización de las mismas. La Guía se estructura conforme a las fases que se han considerado necesarias en un proyecto de auditoría RGPD. La primera fase consiste en la determinación del alcance y planificación, seguida por la obtención de evidencias, y en la segunda fase de la auditoría RGPD, se exponen los criterios que se consideran relevantes a la hora de valorar las evidencias obtenidas y, por otro lado, se especifican las recomendaciones sobre métodos de cálculo del grado de cumplimiento con las obligaciones del RGPD.

Conoce la Guía para la gestión de crisis por ciberincidente en la cadena de suministro

La Guía para la Gestión de Crisis por Ciberincidente en la cadena de suministro, elaborada por ISMS Forum con el apoyo institucional de entidades como el Departamento de Seguridad Nacional (DSN), el Centro Criptológico Nacional (CCN), el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), el Instituto Nacional de Ciberseguridad (INCIBE) y la Agència de Ciberseguretat de Catalunya fue presentada en el marco de la celebración de la primera edición de su Foro Digital, bajo el título "Cyber Security & Data Protection Online Forum".

Resulta necesario contar con mecanismos de respuesta a incidentes que tengan en cuenta el nivel de dependencia de terceros y, en consecuencia, el riesgo directo e indirecto que ello supone. Si bien todavía en algunos sectores no existe una obligación legal de responder en función del incidente, como sí ocurre ya en otros (como es el caso de operadores de servicios esenciales), sí que muchas empresas podrían sufrir un daño elevado a expensas del impacto directo o indirecto del mismo.

En este sentido, el documento ofrece recomendaciones y buenas prácticas sobre cómo deben abordar las empresas una estrategia de protección y respuesta a incidentes de ciberseguridad con origen en proveedor que pueda llegar a provocar una amenaza grave para la propia empresa, así como las convenientes medidas de monitorización, contención y vuelta a la normalidad en la propia Entidad.

Este trabajo complementa al ya publicado por ISMS Forum bajo el título "Protocolo de actuación frente a incidente en proveedor", de forma que el primero aporta recomendaciones y guías de acción rápida frente a un incidente y este lo complementa desde una perspectiva más estratégica.


Aiuken
Cybersecurity

Akamai

ALSID

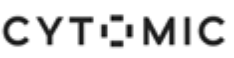
aruba
a Hewlett Packard
Enterprise company

BeyondTrust

BIOCATCH
Less Friction. Less Fraud.

cipher
a PROSEGUR company

CROWDSTRIKE

cybereason

CYTOMIC

Deloitte.

Forcepoint

FORESCOUT

FORTINET

helpsystems

HUAWEI

IBM

McAfee

mobileiron

netskope

OneTrust
PRIVACY, SECURITY & THIRD-PARTY RISK

GLOBAL


paloalto NETWORKS
proofpoint.
Pulse Secure
Qualys.
radware
Recorded Future
retarus
global messaging
riskrecon
S21 SEC
SAMSUNG
sia
SentinelOne
SOPHOS
thycotic
transmit SECURITY
TREND MICRO
VARONIS
vmware
zscaler

SPONSORS

ISMS Forum - International Information Security Community, es una organización sin ánimo de lucro que promueve el desarrollo, conocimiento y cultura de la Seguridad de la Información en España. Creada con una vocación plural y abierta, se configura como un foro especializado de debate para empresas, organizaciones públicas y privadas, investigadores y profesionales donde colaborar, compartir experiencias y conocer los últimos avances y desarrollos en materia de Seguridad de la Información.

915 63 50 62
www.ismsforum.es
info@ismsforum.es

Calle Segre 29, 1B
28002, Madrid, Spain

@ISMSForum

ISMS Forum