

Retos de la Revolución Digital Segura: Regulación, formación y concienciación



El monográfico semestral de la Asociación Española para el Fomento de la Seguridad de la Información

CRÓNICA

¿Por qué la Directiva NIS?

ENTREVISTA

“Pensemos dos veces antes de divulgar información online”

María Bada

Member of Global Cyber Security Capacity Centre, Oxford Martin School, University of Oxford.

FIRMA INVITADA

Una mayor implicación colectiva en materia de ciberseguridad, clave para conseguir el ciberespacio que necesitamos

Alberto Hernández

Director General de INCIBE

EDITA
ISMS Forum Spain

PRESIDENTE
Gianluca D'Antonio

VICEPRESIDENTE
Carlos Alberto Saiz

DIRECTOR GENERAL
Daniel García Sánchez

REDACCIÓN, DISEÑO Y MAQUETACIÓN
Cynthia Rica Gómez

EQUIPO DE GESTIÓN
Cristina Mata Esteban
Cynthia Rica Gómez
Elena Alonso Rubio
Laura Do Campo Ruiz
Leire Ruiz Díaz-Rullo
Virginia Terrasa Bover

Copyright y derechos:

ISMS Forum Spain

Todos los derechos de esta Publicación están reservados a ISMS Forum Spain. Los titulares reconocen el derecho a utilizar la Publicación en el ámbito de la propia actividad profesional con las siguientes condiciones:

- a) Que se reconozca la propiedad de la Publicación indicando expresamente los titulares del Copyright.
- b) No se utilice con fines comerciales.
- c) No se creen obras derivadas por alteración, transformación y/o desarrollo de este Publicación.

Los titulares del Copyright no garantizan que la Publicación esté ausente de errores. En los límites de lo posible se procederá a corregir en las ediciones sucesivas los errores señalados.

El contenido de la Publicación no constituye un asesoramiento de tipo profesional y/o legal.

No se garantiza que el contenido de la Publicación sea completo, preciso y/o actualizado.

Los contenidos reflejados en el presente documento reflejan el parecer y opiniones de los autores, pero no necesariamente la de las instituciones que representan.

Eventuales denominaciones de productos y/o empresas y/o marcas y/o signos distintivos citados en la Publicación son de propiedad exclusiva de los titulares correspondientes.



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

Gonzalo Asensio, Bankinter.

Héctor Guantes, BT.

Carles Solé, CaixaBank.

David Barroso, miembro independiente.

Rubén Frieiro Barros, Deloitte.

Edwin Blom, FCC.

Guillermo Llorente, miembro independiente.

Luis Buezo, Hewlett Packard Enterprise.

Marcos Gómez, INCIBE.

Eduardo Argüeso, IBM.

Jesús Sánchez, Naturgy.

Joan Camps, CGCOM.

José Ramón Monleón, Orange.

Javier Urtiaga, PwC.

Guillermo Lázaro, S21sec.

Alfonso Fernández Jiménez, SIA.

Miguel Ángel Pérez, Telefónica.

Francisco Javier Sevillano, Vodafone.

JUNTA DIRECTIVA

CONTENIDOS



06

CARTA DEL PRESIDENTE

Gianluca D'Antonio



08

EN CLAVE NIS

¿Por qué la Directiva NIS?

Redacción ISMS Forum



14

UN CAFÉ CON LOS EXPERTOS

María Bada 15

Member of Global Cyber Security Capacity Centre, Oxford Martin School, University of Oxford.

Michael Kaiser 20

Executive Director, US National Cyber Security Alliance (NCSA)

Paula Walsh 24

Head of Cyber Policy Department at Foreign and Commonwealth Office, UK Government

ISMS FORUM MAG



28

FIRMA INVITADA

Una mayor implicación colectiva en materia de ciberseguridad, clave para conseguir el ciberespacio que necesitamos

Alberto Hernández
Director general de INCIBE



33

CYBER SECURITY CENTRE

Entrando en la nueva era de la Ciberseguridad 34

Daniel Largacha
Director del Centro de Estudios en Ciberseguridad de ISMS Forum Spain.

CSC: el espacio dedicado a la ciberseguridad de ISMS Forum 38

Dirección y Comité Operativo

Eventos

Foros de la Ciberseguridad

Estudios y Proyectos

Cyber Crisis Management
Ciberejercicios Multisectoriales 2018
Libro Blanco del CISO

Guía "Top 10 Cyber Risks", por AGERS e ISMS Forum

Certificación en Ciberseguridad

Cada vez más demanda de profesionales cualificados en ciberseguridad

Francisco Lázaro

Director del Centro de Estudios en Movilidad e Internet de las Cosas; miembro de la Junta Directiva de ISMS Forum Spain; CISO y DPO de Renfe.

CCSP: Certified Cyber Security Professional

Formación en Ciberseguridad

Curso de especialización en Ciberseguridad: Certified Cyber Security Professional

Plataforma de formación online: Moodle



52

LECTURAS IMPRESCINDIBLES

Guía Nacional de Notificación y Gestión de Ciberincidentes

Cryptojacking

Cyber Europe 2018: After Action Report

Threat Landscape Report 2018: 15 Top Cyberthreats and Trends

IoT Security Standards Gap Analysis

Good practices on interdependencies between OES and DSPs



CARTA
DEL PRESIDENTE



Estimados compañeros, socios y colaboradores de ISMS Forum Spain,

Arrancamos este nuevo año con la convicción de que se abre un nuevo ciclo para la comunidad de profesionales que trabajan en la gestión de los riesgos tecnológicos.

La proliferación de centros de estudio, observatorios y otras iniciativas relacionadas con el riesgo cibernético pone de manifiesto un proceso de acercamiento de la sociedad, en su conjunto, a las temáticas relacionadas con la gestión del riesgo digital.

Tras la aprobación del Real Decreto-ley 12/2018 que introduce en el ordenamiento jurídico español las líneas de actuación definidas en la Directiva NIS (Directiva (UE) 2016/1148), estamos asistiendo a la que podríamos denominar Transformación Digital 2.0, es decir, una reflexión razonada sobre los nuevos vectores de desarrollo e innovación tecnológica que sustentan la Transformación Digital, con la inclusión de una visión crítica de los riesgos que el paradigma digital introduce en el escenario actual.

Gartner ya avisó el año pasado que necesitamos redefinir el perímetro de la Ciberseguridad para que ésta abarque los nuevos dominios tecnológicos que la Transformación Digital ha traído en nuestras vidas como el Internet de las Cosas, la Inteligencia Artificial, las Tecnologías de la Operación, la Robótica y demás vectores de innovación que están colonizándonos. La otra cara de la moneda de este desarrollo tecnológico es el Riesgo Digital que engloba un panorama de amenazas creciente. Para asegurar que esta Transformación no ponga en riesgo la confianza digital que todos demandamos, la Ciberseguridad debe ampliar su espectro de acción y comprensión para convertirse en Seguridad Digital. ¿Empezamos?

Gianluca D'Antonio
Presidente de ISMS Forum Spain



EN CLAVE NIS

¿Por qué la Directiva NIS?

Redacción ISMS Forum



La Directiva del Parlamento Europeo y del Consejo relativa a medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión (Directiva NIS) entró en vigor el pasado 9 de agosto de 2017. Esta norma nace a raíz del aumento de incidentes graves en materia de ciberseguridad en el marco de la Unión Europea, cuya prevención resulta esencial para garantizar el correcto desarrollo de las actividades económicas y sociales y, sobre todo, para el mantenimiento del mercado interior.

Con el objetivo de conseguir ese elevado nivel común de seguridad, la Directiva NIS rige sus acciones a través de cinco medidas principales. En primer lugar, todos los estados miembros están obligados a adoptar una estrategia nacional, debido a las desigualdades surgidas entre países en la protección de empresas y consumidores que han comprometido la seguridad de la Unión Europea en general.

En segundo lugar, recoge la creación de un grupo de cooperación con el objetivo de formular una estrategia común y de permitir el intercambio de información entre los estados miembros. Asimismo, también se ha acogido la disposición de una red de Equipos de Respuesta a Incidentes de

Seguridad Informática (red CSIRT) que ayude a constituir una cooperación más rápida y eficaz y a que se forme un clima de confianza entre los distintos países.

En el caso de España, hay tres CSIRT de referencia. El CSIRT para el sector público es el CCN-CERT, del Centro Criptológico Nacional. Los otros dos CSIRT son el INCI-BE-CERT, para la comunidad que no pertenezca al CCN-CERT, y el ESPDEF-CERT, del Mando Conjunto de Ciberdefensa, que cooperará con los otros dos CSIRT en aquellas situaciones en las que éstos requieran de apoyo por parte de los operadores de servicios esenciales y, necesariamente, en aquellos que tengan incidencia en la Defensa Nacional.

Otra de las medidas que la Directiva reúne se basa en el establecimiento de condiciones de seguridad para operadores de servicios esenciales y proveedores de servicios digitales. Además, las autoridades nacionales de cada estado miembro tendrán obligaciones en todas las tareas relacionadas con la seguridad de redes y sistemas de información.

Transposición de la Directiva al ordenamiento jurídico español

8 de septiembre de 2018. La Directiva Europea de Ciberseguridad o Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, más conocida como Directiva NIS, es transpuesta al ordenamiento jurídico español. Indiscutible es la necesidad de afianzar la fiabilidad de las redes y sistemas de información para el buen funcionamiento de la sociedad en general.

Tal y como estipula el Departamento de Seguridad Nacional (DSN) en su publicación oficial sobre la Directiva NIS, "(...) debido

debido al carácter transnacional de las operaciones, una perturbación grave de esas redes y sistemas, ya sea o no deliberada, y con independencia del lugar en que se produzca, puede afectar a diferentes Estados miembros y a la Unión Europea en su conjunto”.

El Real Decreto-ley 12/2018, de 7 de septiembre, mediante el cual se ha llevado a cabo la transposición de la Directiva NIS en nuestro país, se aplica a las entidades que presten servicios esenciales para la comunidad y dependan de las redes y sistemas de información para el desarrollo de su actividad. La NIS incorpora, al igual que el contenido del Reglamento Europeo de Protección de Datos, la necesidad y obligación de realizar la comunicación a la autoridad competente, e incluso clientes e interesados, de los incidentes de seguridad sufridos por las organizaciones.

“Esta figura, además, facilita a la autoridad competente un punto de contacto especializado para la coordinación de la Seguridad de la Información”



La necesidad de designar un responsable

El desarrollo de esta novedad, -la notificación de incidentes de seguridad-, viene recogido en el artículo 16 del texto de la Directiva. Asimismo, en el apartado 3 de dicho artículo, se especifica que “Los operadores de servicios esenciales designarán y comunicarán a la autoridad competente, en el plazo que reglamentariamente se establezca, la persona, unidad u órgano colegiado responsable de la seguridad de la información, como punto de contacto y de coordinación técnica con aquella. Sus funciones específicas serán las previstas reglamente-

Esta incorporación tiene origen y antecedentes en la consulta pública emitida por el Ministerio de Energía, Turismo y Agenda Digital, para la que ISMS Forum inició un sondeo entre la comunidad de CISOs en España sobre la inclusión de la figura del responsable de seguridad de la información en el nuevo marco normativo.

Siendo el “Anteproyecto de Ley sobre la Seguridad de las Redes y Sistemas de Información” una regulación específicamente enfocada a asegurar la fiabilidad y seguridad de los sistemas de información que dan soporte a los servicios esenciales, ISMS Forum entendió que la existencia en las organizaciones de la figura de Responsable de Seguridad de la Información o CISO, facilita el debido cumplimiento de las obligaciones que emanan de esta ley.

Esta figura, además, facilita a la autoridad competente un punto de contacto especializado para la coordinación de la Seguridad de la Información, de manera que se garantiza la aplicación de medidas de seguridad para reducir los riesgos a otros posibles intereses de las organizaciones o a otras posibles estrategias de tratamiento de riesgos que pudieran comprometer el aseguramiento de los sistemas de información.

El primer Libro Blanco del CISO: el documento de referencia sobre la figura del CISO en España

La consulta pública dejó entrever la carencia conceptual de la figura del CISO y la necesidad de contar con una guía que empezara a definir los márgenes de actuación de este responsable. De esta situación nació el Libro Blanco del CISO, una de las iniciativas más importantes que ISMS Forum ha llevado a cabo en 2018, que contó con el apoyo institucional del Instituto Nacional de Ciberseguridad (INCIBE) y que se creó sin precedentes en España.

En el documento han trabajado más de 20 directores de Seguridad de la Información para definir el estado de la figura del CISO en España, presentando una primera aproximación de las responsabilidades y funciones inherentes a dicha figura, modelos organizativos y soft skills, con el objetivo de poner en el mercado una guía de referencia para los directores de Seguridad de la Información.

“Sabemos qué color de pelo y qué zapatos debe llevar un DPO, ¿y el CISO?”, así empezaba su intervención Roberto Baratta, Global Executive VP and Director of Loss Prevention, Business Continuity and Security de Abanca y Board Member de ISMS Forum, durante la celebración del VII Foro de la Ciberseguridad de Asociación. “Con este libro tenemos la oportunidad de reivindicar la figura del CISO en España”, añade.

Durante los últimos años, los departamentos de seguridad han tenido que enfrentarse a un panorama de amenazas cada vez más difícil y el CISO ha desempeñado un papel mucho más visible dentro de las organizaciones. Como resultado, el rol del CISO ha experimentado una importante evolución y acercamiento al negocio.

“Hay muchas empresas que no tenían la necesidad de tener un responsable de la seguridad de la información, y ahora tienen que designar una persona específica para desempeñar esas funciones”, comentaba Carles Solé, CISO de CaixaBank, durante la presentación de la iniciativa en el foro.



Presentación de la iniciativa el Libro Blanco del CISO durante el VII Foro de la Ciberseguridad en el Círculo de Bellas Artes de Madrid



Roberto Baratta
VII Foro de la Ciberseguridad
(CaixaForum Madrid)

Mientras los procesos tecnológicos avanzan, los organismos públicos y los propios lobbies profesionales amenazan con un marco regulatorio cada vez más difícil, donde la figura del CISO tiene un papel fundamental para cohesionar los requerimientos normativos en materia de Seguridad de la Información.

Por otra parte, la responsabilidad del CISO dentro de las compañías puede solaparse con otras funciones desempeñadas por el CCO (Chief Communications Officer) o el DPD (Delegado de Protección de Datos), de última creación. “Se pone muchísima exigencia en las funciones del CISO, en cambio éstas no se especifican en ningún lugar. Existen estructuras muy definidas para profesiones nuevas, pero no somos capaces, al menos en el contexto europeo, de definir las para el CISO”, explicaba Baratta.



Carles Solé
VII Foro de la Ciberseguridad
(CaixaForum Madrid)

“Sabemos qué color de pelo y qué zapatos debe llevar un DPO, ¿y el CISO?”



Las funciones que cada uno de estos actores desempeñe dentro de la organización deberán definirse ad-hoc según la idiosincrasia de cada una sin olvidar la necesaria segregación de funciones entre los distintos roles, que garantice transparencia, independencia y control. “Las compañías necesitan un marco de referencia, y qué mejor que ese marco sea elaborado por los que están en el sector”, añade Solé.

De esta manera, ha nacido el primer Libro Blanco del CISO en España. Un documento que pretende servir de guía para los directores de Seguridad de la Información, y que define, determina y establece los principios básicos a partir de los cuales debemos entender sus responsabilidades y funciones. Un proceso que se torna hoy más necesario que nunca, tras la reciente incorporación y adaptación de la Directiva NIS a nuestro país.



UN CAFÉ CON

LOS EXPERTOS



“Pensemos dos veces antes de divulgar información online”

María Bada es una de las ponentes internacionales que participó en el VII Foro de la Ciberseguridad que organiza ISMS Forum Spain a través de su iniciativa Cyber Security Centre (CSC). Ella ha sido, durante mucho tiempo, miembro del Centro Global de Capacidades en Ciberseguridad (Global Cyber Security Capacity Centre, en inglés) de la Universidad de Oxford y ha sido participante del Cybersecurity Capacity Maturity Model for Nations (CMM): un modelo de madurez creado para evaluar el nivel de capacidades en ciberseguridad de los países. Este proyecto está permitiendo que cada vez sean más los estados que quieren medir su desarrollo en esta materia, fomentando así la cultura de la ciberseguridad.

¿En qué consiste el Modelo de Madurez de Ciberseguridad?

Es un modelo que desarrollamos para evaluar la capacidad de ciberseguridad a nivel nacional. Para ello, decidimos crear cinco dimensiones diferentes: política y estrategia; cultura y sociedad; educación; capacitación antes de la legislación; y estándares tecnológicos. Esto nos sirve para medir y evaluar el estado de un país en todo lo referente a la ciberseguridad, es decir, observarlos en su etapa inicial y decirles qué deben hacer para pasar a la siguiente etapa, de las cinco que acabo de mencionar. Ya hemos implementado el modelo en más de sesenta países ubicados en América Latina, Asia, África, Europa y Oceanía.

¿El modelo es efectivo?

Diría que el modelo ha funcionado bien y ha sido útil para los países, que pudieron identificar cuáles son las brechas y qué deben hacer a continuación. Son los propios países los que nos solicitan una visita y que les proporcionemos un informe con nuestras recomendaciones. Lo que está ocurriendo es que estas acciones se propagan. Por ejemplo, Albania se sometió a una evaluación y, enseguida, un país vecino quería hacerla también. Ahora ya contamos con otro centro en Australia y ha sido todo un éxito desplegando allí el modelo.

Además de las organizaciones públicas, ¿este modelo puede ser útil también para el sector privado?

Tal y como está creado el modelo en este momento, no. No obstante, ya lo hemos convertido para que eso ocurra, pero aún no lo hemos publicado. Además, a pesar de partir de la misma idea y metodología, se han incorporado cambios para que el modelo pueda adaptarse al sector privado porque, de lo contrario, no tendría utilidad.

¿A qué carencias debemos la creación de un modelo de madurez para la ciberseguridad?

En realidad, no es el único modelo que existe. De hecho, muchas organizaciones que están tratando de desarrollar otros modelos ya están triunfando. Nuestra principal diferencia es que nos hemos centrado en los aspectos sociales. Identificamos que otros



María Bada

Member of Global Cyber Security Capacity Centre, Oxford Martin School, University of Oxford.

Fotografía

**VII Foro de la Ciberseguridad
(Círculo de Bellas Artes Madrid)**

modelos carecen de algunos aspectos que nos parecen importantes. De todas formas, el CMM no es estático. A medida que lo hemos ido desplegando en cada país, hemos sido conscientes de los nuevos desafíos que enfrentan las sociedades con la llegada del RGPD y la Directiva NIS. Por lo tanto, cada poco tiempo el modelo vuelve a revisarse y, de hecho, ya se ha revisado por segunda vez, convirtiéndose así en una herramienta para conocer lo que está sucediendo en el mundo en esta materia y recopilar datos a partir de los cuales realizamos análisis.

El pasado 8 de septiembre de 2018, la Directiva NIS fue traspuesta al ordenamiento jurídico español. ¿Cree que tener un estándar común para todos los países proporcionará beneficios en términos de ciberseguridad?

Tener direcciones comunes para todos, como la Directiva NIS, es positivo. Ahora, junto al RGPD crea un punto de referencia en Europa y fuera de Europa, ya que muchos países no miembros de la Unión están intentando seguir estas líneas. Tener estos requisitos comunes es muy importante para que los países europeos utilicen el mismo lenguaje cuando se trata de cuestiones específicas en materia de ciberseguridad y protección de datos, aunque no sé qué tan rápido pueden todos los países miembros de la Unión implementar estos requisitos. También es cierto que cada país tiene necesidades diferentes. Por ejemplo, España podría tener unas carencias diferentes a las de Suecia en términos de cultura y riesgos, por lo que cada uno deberá adaptar estas normativas a sus circunstancias.

Con el *boom* del RGPD, todo está desarrollándose rápidamente. ¿Cree que el objetivo es llegar a un único modelo a nivel mundial en términos de protección de datos?

No lo creo. Por ejemplo, no creo que pueda existir un único modelo que establezca 72 horas para comunicar una brecha o incidente de seguridad, tal y como determina el RGPD. No creo que deba haber algo tan definitivo. Por eso el RGPD ha recibido críticas, porque es una norma cuyo rango es elevado, al tiempo que no aporta información detallada de las cuestiones relacionadas con los datos. Un país puede encriptar sus datos, seguir las normas ISO y tener a un Delegado de Protección de Datos, y no tener idea alguna de cómo manejar los datos. Creo que estamos en el inicio del proceso. Cada estado se encuentra ahora aprendiendo a adaptarse correctamente, pero creo que aún necesitaremos tiempo hasta que todo el mundo tome conciencia, no sólo de lo que dictamina el RGPD, sino también los pasos a seguir cuando se trata de ciberseguridad, que debe ir combinada con la protección de los datos. Aún no estamos en ese punto.

Por otra parte, los ciudadanos normalmente no ven el riesgo y eso también es un problema, ¿no?

Creo que hay una confianza ciega en general. Confiamos en todo lo que leemos *online* y ahora hay una gran cantidad de noticias falsas capaces de influir en la situación política de los países, así que la gente no puede confiar en lo que lee en Internet. Son muchos los riesgos a los que nos enfrentamos y la gente no es consciente, por lo que se pueden convertir fácilmente en víctimas.

“No creo que pueda existir un único modelo que establezca 72 horas para comunicar una brecha o incidente de seguridad, tal y como determina el RGPD”



“Cuando salimos de nuestra casa asumimos que tenemos que cerrar la puerta con llave, de la misma manera hay que actuar con nuestros dispositivos electrónicos”



Hemos visto ejemplos de usuarios publicando en Facebook su tarjeta de crédito junto a su nombre y sus datos. Ahora, más que nunca, son necesarios los programas de concienciación en los colegios sobre cómo mantenerse a salvo en Internet. Sé que Europa está esforzándose mucho por promover estas prácticas educativas porque en muchos países se están dando con frecuencia, por ejemplo, juegos de autolesión *online*, cuyo objetivo final es el suicidio. Estuve en Roma el año pasado hablando de este tema y el público no me creía. Menos mal que un agente del FBI se levantó y dijo: “Sí, esto es real y tenemos las pruebas que lo demuestran”. La gente piensa que esto no es real, que no pasa, pero sí lo es, está sucediendo.

Quizás solo en el momento en que las personas sufren un ataque, empiezan a preocuparse...

Y ni así. Las investigaciones realizadas nos dicen que, si una persona es víctima de un fraude cibernético, por ejemplo, seguramente volverá a ocurrirle una segunda vez. El hecho de que pasen por ello, no significa que tomen conciencia al cien por cien del alcance o impacto de lo que les ha sucedido. Después de un tiempo, olvidarán las precauciones que hay que tomar y alguien se lo volverá a hacer. Eso es básicamente debido a la falta de conciencia o de conocimiento.

A propósito, parte del foco de su trabajo se basa en la concientización sobre la seguridad cibernética a través de campañas para los colegios, por ejemplo. En su opinión, ¿quién o quiénes son los que deberían empezar a hablar sobre el tema para fomentar la cultura de la ciberseguridad?

Yo diría que la intención de hablar de ello y de fomentar que la sociedad sea consciente de los peligros que devienen de la actividad *online* debería venir por parte del gobierno de cada país a través de la promoción de programas, acciones de comunicación, etc. No obstante, también creo que cada uno de nosotros debería autoevaluarse y ser participe del proceso. Lleva un tiempo el cambio de comportamiento de los individuos, pero nada es imposible. Hay que dar el paso para poder incorporar esta mentalidad cibernética en nuestra rutina personal hasta llegar al punto en que no lo tengamos que pensar. Cuando salimos de nuestra casa asumimos que tenemos que cerrar la puerta con llave, de la misma manera hay que actuar con nuestros dispositivos electrónicos.

Para terminar, ¿qué primer paso deberían dar los ciudadanos para protegerse a sí mismos de las posibles ciber-amenazas?

Lo primero: pensar dos veces antes de hacer clic en correos electrónicos de remitentes desconocidos y pensar dos veces antes de divulgar información online. En general, la premisa debe ser pensar dos veces, porque muchas veces nos sentimos libres de expresar ciertas cosas en Internet que no diríamos nunca. ■

Fotografía

María Bada, con el primer número de ISMS Forum Magazine, en el VII Foro de la Ciberseguridad (Círculo de Bellas Artes Madrid)





Michael Kaiser

Former Executive Director of the US National Cyber Security Alliance (NCSA).

Fotografía

XX Jornada Internacional de Seguridad de la Información (Círculo de Bellas Artes Madrid)

“La expectativa de la perfección en materia de ciberseguridad y protección de datos es inalcanzable”

Ex director ejecutivo de la Alianza Nacional de Ciberseguridad de Estados Unidos (NCSA, sus siglas en inglés), Michael Kaiser cuenta con una larga trayectoria profesional en la que se ha focalizado en educar y concienciar a los usuarios en materia de ciberseguridad y protección de datos, sobretodo, a través de la plataforma *Stay Safe Online* que la Alianza dirige y promueve. El fin último es que los usuarios obtengan información sobre como mantenerse seguros en Internet en el ámbito personal, académico y laboral.

¿Cree que la sociedad es prudente en relación a los riesgos que entraña la vida *online*?

Creo que muchas personas son conscientes de algunos de los riesgos. No sé en España, pero en Estados Unidos la gente está verdaderamente preocupada por ciertos peligros. Especialmente, cuando se trata de cuestiones que conlleven perder dinero. En otras cosas tal vez no, quizás exista mayor conciencia en materia de privacidad en la Unión Europea.

En general, a los usuarios les preocupa que alguien robe los datos de su tarjeta de crédito y le quite el dinero. Es una reacción natural, el dinero es importante.

¿Hasta qué punto podrían combatirse los cibercrímenes si muchos de nosotros supiéramos lo que implica cada acción que efectuamos en Internet?

Creo que cada uno debe asumir la responsabilidad de sus propias actividades en línea. Los individuos deben tener conocimiento de cuestiones relativas a las buenas prácticas en la disposición de contraseñas o la actualización de los sistemas de sus dispositivos. Los consumidores deberían preocuparse un poco más por lo que ellos mismos hacen en estos entornos. No obstante, aunque la gente esté interesada en estar informada, no podemos caer en la trampa de proporcionarles consejos que sean demasiado complicados de entender y de realizar. Lo que debemos hacer es darles conocimientos que no sean tan técnicos y que a su vez hagan sus vidas más seguras. Por desgracia, los ciberdelincuentes siempre perseguirán las vulnerabilidades, por lo que si cada uno tenemos nuestros *softwares* actualizados o utilizamos la autenticación multi-factor, estos actores irán a por la siguiente persona que no los tenga.

¿Cómo educa y sensibiliza la plataforma *Stay Safe Online* sobre la privacidad y la ciberseguridad?

La organización desarrolla diversas acciones. Una de ellas, por ejemplo, es el mes de la concienciación sobre la seguridad cibernética en octubre o el día de la privacidad cada mes de enero, unidas a varios mensajes sobre cómo mantenerse seguros *online*. La seguridad es algo que

cada uno debemos aplicar dependiendo de lo que estemos haciendo en ese momento en Internet, ya sea comprar algo o interactuando en alguna red social. Existen medidas similares para cualquier tipo de acción, así como también las hay específicas para ciertos hábitos o actividades. Esto es una pequeña parte de lo que promueve la plataforma *Stay Safe Online*.

¿Qué problemas éticos entraña el Big Data?

La manera en la que Internet ha crecido tiene su razón de ser en las personas que se encargan de recopilar esa cantidad de datos sobre sus clientes, sus ciudadanos y quienes estén involucrados. Los datos son el combustible de Internet: hacen que los servicios funcionen. Si tal vez estás pensando en comprar un coche, te daré anuncios publicitarios sobre coches. Por supuesto, esto ha suscitado ciertas inquietudes acerca de la cantidad de información que poseen las empresas sobre nosotros y el peligro que conlleva que la pierdan o sea robada. Otro de los casos acontecidos es el que hemos visto en Estados Unidos. Nadie espera que su información personal en Facebook sea utilizada para influir en un proceso electoral. ¿Y cómo utilizar los datos correctamente? Esta es una de las preguntas que más deberíamos hacernos, porque el uso de los datos puede ser muy poderoso y tener gran impacto beneficioso para la sociedad. Eso sí, debe hacerse de una manera ética y saludable.

“Que los ciudadanos sepan que existe un nuevo malware por ahí haciendo de las suyas no significa nada para ellos. Hay que descubrir en qué se traduce eso para la sociedad e identificar qué mensaje va a hacerles cambiar el chip”



¿Cuáles son los desafíos éticos a los que nos enfrentamos en el ciberespacio y qué herramientas podemos utilizar para combatirlos?

El desafío está en la forma en la que se recopilan los datos y cómo se protegen. Los datos que sean recopilados de otros lugares deberían ser seguros y de confianza. Después, en lo que respecta a los individuos, la única forma adecuada de controlar los datos es teniendo permiso para manejarlos. Yo, como usuario, voy a hacer uso de tu servicio y te diré qué vas a hacer con mis datos. Creo que ese es el gran cambio que debería llevarse a cabo.

¿Qué resultados ha obtenido la campaña *Stop. Think. Conect hasta hoy?*

La campaña comenzó en 2009, basándonos en un concepto muy simple que creo que sigue siendo muy relevante hoy en día. Muchas son las personas que aprenderán las formas de mantenerse seguro *online* y, por supuesto, cada uno de nosotros es diferente, de ahí que tengamos diferentes cosas que proteger. La idea era investigar sobre el comportamiento de los consumidores y qué tipos de mensajes llaman su atención para cambiar sus hábitos. Muchos de los expertos en ciberseguridad saben explicarles a los usuarios cómo ser más seguros en Internet, pero no saben cómo decírselo de forma comprensible. Por ejemplo, que los ciudadanos sepan que existe un nuevo *malware* por ahí haciendo de las suyas no significa nada para ellos. Lo que hay que hacer es descubrir en qué se traduce eso para la sociedad e identificar qué mensaje va a hacerles cambiar el chip. Los cambios culturales son arduos y llevan tiempo. Solo hay que pensar, por ejemplo, en los constantes intentos por parte de los expertos de que la gente deje de fumar o recicle. Todos sabemos perfectamente qué hay que hacer y aún así no lo hacemos.

¿Qué significará el RGPD, no solo a nivel europeo, sino también a nivel mundial?

Todos los que hacen negocios en Europa deben cumplir con el RGPD porque tienen información sobre los ciudadanos europeos, residan o no residan en Europa. Las compañías tienden a crear sus propios procesos internos, lo que significará que, por ejemplo, las empresas estadounidenses cuyos negocios tengan relación con Europa deberán aplicar el RGPD.

¿Qué procesos, tecnologías y políticas se están desarrollando para la gestión de la identidad digital?

Es una pregunta complicada. Tenemos que diferenciar entre la autenticación y la identidad. La autenticación es un tipo de acceso a una cuenta específica, que normalmente no sabe quién soy, porque lo único que necesita saber es que tengo derecho a entrar. Y eso es bueno para muchas cosas, por ejemplo, para el correo electrónico o para las compras por Internet. Dicho con otras palabras, la autenticación no trata de identificar a una persona individual, porque tal vez una familia pueda compartir la misma cuenta. En cambio, con la identidad es total y absolutamente obligatorio saber quién es la persona que está intentando acceder. Debemos asegurarnos de que usamos la identidad solo en aquellos espacios donde es necesario y empleemos la autenticación en los lugares donde sea suficiente el simple acceso.

¿Cree que la transformación digital sana es posible a través de la concienciación?

Creo que va a suceder de todos modos, es inevitable. Entonces la pregunta es: ¿sucederá correctamente? Creo que deberíamos hacerlo con los ojos bien abiertos.



Fotografía

XX Jornada Internacional de Seguridad de la Información (Círculo de Bellas Artes Madrid)

Además de eso, considero necesario que todos formemos parte del proceso. Para ello, es vital que tanto las instituciones como las compañías sean capaces de comunicarse con nosotros, de manera que podamos entender los riesgos y, por ende, gestionarlos. Por otra parte, es cierto que la expectativa de la perfección en materia de ciberseguridad y protección de datos es inalcanzable. Creo que deberíamos educar nuestra mente pensando que los accidentes siempre van a suceder. Pero mientras nos movamos en la dirección correcta y comprendamos los beneficios que puede regalarnos el buen uso de nuestros datos, estaremos actuando bien. ■



Paula Walsh

Head of Cyber Policy Department at Foreign and Commonwealth Office, UK Government.

Fotografía

Círculo de Bellas Artes Madrid

“Muchas empresas y usuarios no toman las precauciones más simples, como la actualización del *software*, hasta que no se enfrentan a un problema de ciberseguridad.”

Paula Walsh dirige el Departamento de políticas en ciberseguridad de Reino Unido y afirma que la creación del Centro Nacional de Ciberseguridad (National Cyber Security Centre, NCSC, en inglés) ha sido una de las iniciativas que más éxito ha obtenido a nivel gubernamental en los últimos años. Esto les ha permitido intervenir de forma más proactiva y preventiva en la industria y protegerse como país a través del desarrollo de alianzas con otros estados y la búsqueda de innovación, con el fin de influir en la forma de actuar de los ciudadanos y aprendan a recurrir a prácticas sencillas, pero eficaces.

¿La ciberseguridad, en términos generales, es responsabilidad de todos?

La forma en la que percibimos la ciberseguridad en Reino Unido, desde un punto de vista operativo, tiene que ver con el establecimiento de un centro nacional de ciberseguridad que sea responsable de las respuestas operativas sobre la materia para el gobierno. No obstante, existen otros gobiernos que establecen otras políticas. Esto depende de muchos factores. Es un asunto que no es tan simple como podemos creer a simple vista, pero está claro que compartir esa responsabilidad entre todos es importante.

¿Qué significará el nuevo marco regulatorio europeo para la ciberseguridad y la protección de datos para Reino Unido?

Tanto el Reglamento Europeo de Protección de Datos (RGPD) como la Directiva NIS son muy importantes para Reino Unido. Por supuesto, el marco regulatorio tiene implicaciones para todos y creo que ya con el RGPD se está viendo un gran aumento en la cantidad de correos electrónicos que los usuarios reciben por parte de las compañías para asegurarse de que cumplen con la legislación. Por lo tanto, creo que es un momento importante y una experiencia de aprendizaje para todos.

Sobre cuestiones de ciberseguridad, ¿cómo define la visión del gobierno de Reino Unido?

Reino Unido lanzó en 2016 su tercera estrategia nacional de ciberseguridad, que abarca el período de 2016 a 2021, y se espera que en ese período de cinco años se convierta en transformador en términos

de ofrecer y aumentar la ciberseguridad. Lograr ese equilibrio es un reto. Esa es realmente la visión del gobierno, estar seguros y tener confianza, pero también permitir y buscar el crecimiento.

¿Qué medidas específicas está implementando el gobierno desde esa perspectiva?

Una de las medidas más grandes ha sido la creación del Centro Nacional de Ciberseguridad. El centro busca crear una estructura nacional y una estrategia de comunicación, trabajando de cerca con agencias nacionales de ciberdelincuencia. Desde su creación en 2016, hemos comprobado que se han reforzado las respuestas a los incidentes de ciberseguridad. Lo vimos, por ejemplo, con WannaCry: la primera prueba real del Centro Nacional de Ciberseguridad, con la que el jefe del centro pudo dar la cara y demostrar que estábamos respondiendo ante el problema.

¿En qué se basa la estrategia del Centro Nacional de Ciberseguridad de Reino Unido?

Creo que en la estrategia hay tres pilares: defensa, disuasión y desarrollo. La defensa incluye cuestiones como la gestión de incidentes, la aplicación de la ley y la defensa cibernética. La estrategia de Reino Unido es ahora más intervencionista que antes. Las estrategias previas dejaban la ciberseguridad más en manos del mercado. Las empresas y el público debían cambiar su comportamiento y cuidar su propia seguridad, y eso no estaba funcionando. Así que la nueva estrategia nos otorga algunas licencias, como las prevenciones automáticas. Efectivamente, sí, les decimos a la gente que necesitan tener contraseñas

“WannaCry fue la primera prueba real del Centro Nacional de Ciberseguridad, con la que el jefe del centro pudo dar la cara y demostrar que estábamos respondiendo ante el problema.”



más seguras y actualizar el *software*, entre otras medidas en torno a la ciberdefensa. Por su parte, la disuasión trata de hacer más difícil que Reino Unido se convierta en un objetivo. Se trata de construir coaliciones con países aliados sobre el uso de la defensa en el ciberespacio de acuerdo con el derecho internacional. Pero, básicamente, se trata de hacer que el Reino Unido sea más resistente y, en definitiva, un objetivo más difícil. Finalmente, desarrollar consiste en la capacidad de construcción, es decir, asegurar una innovación en la industria y en el gobierno, y buscar cambiar comportamientos. En definitiva, se trata de asegurarnos de que nuestra industria sea sólida y compartamos las mejores prácticas.

¿Qué papel interpreta la educación en este ámbito?

Desarrollar una estrategia educativa implica alentar un cambio de comportamiento, sobre todo porque sabemos que no contamos con suficientes personas capacitadas en el área de la ciberseguridad. Además, la educación nos servirá también para desarrollar las habilidades que necesitamos, tanto para el presente como para el futuro.

¿Cree que es necesario tener una formación o estudios continuos, por ejemplo, en el caso de los desarrolladores de ciberseguridad?

Definitivamente. Se trata de tener un aprendizaje continuo. Las profesiones y las habilidades están siendo cada vez más importantes, sobre todo, porque el ciberespacio cambia rápidamente y si no nos mantenemos actualizados y no hacemos las innovaciones pertinentes, nos quedamos atrás. Creo que es todo un desafío, pero es necesario seguir el camino de la formación continua.

El 24% de las empresas de Reino Unido han tenido una o más brechas de seguridad en los últimos 12 meses. Es un dato verdaderamente alarmante. ¿Cuál es el problema?

Parece mentira, pero muchas empresas, y también los usuarios a título individual, no toman las precauciones más simples, como puede ser el cambio de contraseñas y la actualización del software, hasta que no se enfrentan a un problema de ciberseguridad. Realmente muchos de los ciberataques no son tan sofisticados y pueden evitarse recurriendo a prácticas sencillas. En este sentido, una de las acciones que el Centro Nacional de Ciberseguridad lleva a cabo es dar herramientas de asesoramiento a las empresas para mejorar la seguridad de su ciberespacio. Otra de las iniciativas que desarrolla el centro consiste en una plataforma cerrada llamada CiSP (Cyber Security Information Sharing Partnership) que permite que algunas empresas de Reino Unido tengan acceso a información privada que contiene consejos técnicos e indicadores específicos sobre cuáles son las amenazas, y, por supuesto, cómo pueden protegerse a sí mismos. Con todo esto, nos hemos dado cuenta de los beneficios de este tipo de proyectos para la sociedad en general, debido a que las personas, por sí solas, no cambian sus hábitos.

Y si las empresas no predicán con ese cambio, los usuarios tampoco, ¿no?

Las personas no cambian hasta que una determinada situación les ocurre de manera reiterada en el tiempo y no están a gusto con ella. Mismamente, muchos de los casos escandalosos de Big Data no han causado el impacto suficiente para que la gente se sorprenda e intente modificar su rutina. ■



Fotografía

XX Jornada Internacional de Seguridad de la Información (Círculo de Bellas Artes Madrid)



FIRMA INVITADA

Una mayor implicación colectiva en materia de ciberseguridad, clave para conseguir el ciberespacio que necesitamos

El uso masivo e intensivo de la tecnología en nuestra sociedad ha introducido un conjunto de amenazas que hasta hace muy poco se creían restringidas únicamente para las grandes multinacionales. El ciberespacio o Internet constituye a día de hoy un dominio tan real como el mundo físico, pero con unas características que lo hacen especialmente atractivo para cometer numerosas acciones delictivas con menor riesgo de ser detectadas.

Sin ser los ataques más graves que se han producido en los últimos años, Wannacry y Petya han marcado un antes y un después en cómo es percibida la ciberseguridad y la ciberamenaza por nuestros ciudadanos y empresas. Tras estos ciberataques y las correspondientes crisis que desencadenaron, nuestra sociedad ha entendido que la ciberamenaza nos es algo tan lejano, sino que nos puede afectar desde económicamente hasta echar por tierra la imagen, el trabajo y la credibilidad que una empresa se ha forjado durante muchos años o incluso décadas. Como consecuencia de estas crisis, ha aumentado de forma positiva el nivel de concienciación general, aunque hay aún mucho camino por recorrer. Se ha acentuado también el compromiso de las organizaciones tanto públicas como privadas en mejorar la colaboración. La ciberseguridad como un “asunto de todos” es un leimotiv cada vez más repetido y escuchado en las diferentes conferencias y congresos a nivel nacional e internacional.



Alberto Hernández

Director general de INCIBE.

“El ciberespacio constituye a día de hoy un dominio casi tan real como el mundo físico, pero con unas características que lo hacen especialmente atractivo para cometer numerosas acciones delictivas con menor riesgo de ser detectadas”



Si bien los usuarios de las tecnologías, los empresarios, los expertos en ciberseguridad, las fuerzas y cuerpos de seguridad y las organizaciones internacionales, entre otros, son actores imprescindibles para mejorar la ciberseguridad a nivel global, es fundamental el liderazgo de los Estados y sus Gobiernos en la definición y puesta en marcha de estrategias de ciberseguridad que abarquen todos los campos de actuación.

El reciente mandato del Gobierno de España de revisar y actualizar la Estrategia de Ciberseguridad Nacional del 2013, tras la publicación en diciembre de 2017 de la nueva Estrategia de Seguridad Nacional, y el refuerzo de las capacidades del Instituto Nacional de Ciberseguridad (INCIBE) son un claro ejemplo del compromiso en nuestro país por el desarrollo de la ciberseguridad.

En el ámbito europeo, desde la aprobación en el año 2013 de la Estrategia de Ciberseguridad Europea, se han iniciado numerosas acciones con el objetivo de impulsar y fortalecer la ciberseguridad de la UE, teniendo en cuenta la dispersa y heterogénea situación de ésta en los diferentes países, centrándose no sólo en el reto que supone para la seguridad de los Estados sino también la oportunidad que representa para el desarrollo industrial.

De todas estas acciones la más conocida es la denominada Directiva NIS (Network and Information Security), que corresponde con la Directiva (UE) 2016/1148 del Parlamento y Consejo Europeo, que aborda las medidas para garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la UE. La aprobación de esta Directiva ha supuesto un paso fundamental hacia el desarrollo de un mercado único digital y también ciberseguro en la UE.

La Directiva, que fue transpuesta al ordenamiento jurídico español 7 de septiembre de 2018 mediante el Real Decreto-Ley (RDL) 12/2018 y que se está tramitando actualmente en el Congreso como proyecto de ley, establece unos requisitos mínimos de ciberseguridad para los operadores de servicios esenciales y los proveedores de servicios digitales, a los que insta a adoptar las medidas oportunas para gestionar los riesgos de seguridad y, por primera vez, estableciendo la obligatoriedad de notificar a las Autoridades Competentes nacionales los incidentes que puedan tener un impacto significativo en éstos. Es en el marco de esta notificación en el que los centros de respuesta ante incidentes nacionales denominados CERTs (Computer Emergency Response Teams) o CSIRTs (Computer Security Incidents Response Teams), juegan un papel fundamental a la hora de apoyar en la resolución de los mismos.

Hasta la aprobación de dicho RDL, el papel de los CSIRTs públicos nacionales ha sido fundamental a la hora de apoyar no sólo en la resolución de los ciberincidentes o ciberataques que han afectado a los activos tecnológicos de nuestro país, sino también en la detección proactiva de éstos. Ejemplo de ello han sido los incidentes gestionados por el antiguamente denominado CERT de Seguridad e Industria, ahora INCIBE-CERT, que han pasado en tan solo cuatro años de 18.000 en el 2014 a más de 123.000 en el año 2017. No obstante, no ha sido hasta la transposición de la Directiva NIS a nuestro ordenamiento jurídico, que la contribución de los CSIRTs públicos nacionales a la ciberseguridad nacional no ha venido acompañada de la obligatoriedad de notificar y colaborar con ellos por parte de los operadores de los servicios esenciales. Esta notificación es esencial para poder mejorar la protección

“Es fundamental el liderazgo de los Estados y sus Gobiernos en la definición y puesta en marcha de estrategias de ciberseguridad que abarquen todos los campos de actuación”



del resto de operadores y, por lo tanto, la alerta temprana.

Pero la Directiva NIS no constituye una iniciativa aislada en el ámbito europeo, sino que forma parte de un conjunto de acciones que a día de hoy están en fase de diseño o dando sus primeros pasos. En septiembre de 2017 la Comisión Europea presentó un ambicioso conjunto de medidas de reforma en materia de ciberseguridad, con el objetivo de hacer frente a la creciente amenaza en Europa que plantean los ataques cibernéticos, así como aprovechar las oportunidades que presenta la nueva era digital. Tan sólo un mes más tarde, los días 19 y 20 de octubre de 2017, y como consecuencia de la propuesta de dichas medidas por la Comisión Europea, el Consejo Europeo solicitó la adopción de un planteamiento común de la ciberseguridad en la UE. Son precisamente los retos de ciberseguridad asociados al Internet de las Cosas o Internet of Things (IoT) y la importancia del uso seguro de las redes y de los sistemas de información y telecomunicaciones en el marco de la UE, lo que hace además prioritario la adopción de este planteamiento común. El reforzamiento de la agencia europea de ciberseguridad ENISA, el desarrollo de un esquema europeo de certificación de productos y servicios de ciberseguridad y la creación de un Centro Europeo de Competencias en ciberseguridad que permita impulsar el desarrollo de la I+D+i e industria de ciberseguridad en la UE, son algunas de las medidas presentadas en este ambicioso plan.

Pero todas estas medidas no podrán ser desarrolladas adecuadamente si no contamos con profesionales formados y experimentados en el campo de la ciberseguridad y que además tengan una asignación clara de

funciones y responsabilidades dentro de las organizaciones. La figura del CISO (Chief Information Security Officer) adquiere a día de hoy aún más relevancia puesto que este profesional tiene un papel fundamental para cohesionar y garantizar el cumplimiento de los requisitos normativos en materia de ciberseguridad. La regulación de su función y por lo tanto su incorporación al conjunto normativo en materia de ciberseguridad, es un reto a abordar a corto plazo no sólo en el ámbito nacional sino en el europeo e internacional.

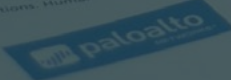
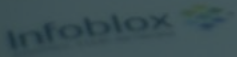
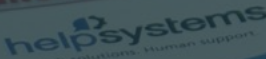
En este sentido, y dentro de las líneas de colaboración que INCIBE mantiene con diferentes organismos públicos y privados, hemos trabajado junto a ISMS Forum Spain en la elaboración del Libro Blanco del CISO, una herramienta muy útil para definir y profesionalizar un perfil que cada vez es más demandado y que juega un papel de vital importancia en las organizaciones. Este documento tiene como objetivo fundamental el contribuir a lograr la especialización máxima de este profesional y a delimitar su ámbito de competencia y sus responsabilidades hasta que éstas puedan estar incluidas a nivel normativo.

Estrategias de ciberseguridad, liderazgo nacional, nuevos desarrollos normativos, esquemas de certificación, fortalecimiento de los CSIRTs, promoción del talento en ciberseguridad, regulación de las funciones de los responsables de ciberseguridad, etc., son, en definitiva, partes de un plan global en el que la colaboración y la acción conjunta a nivel nacional e internacional son imprescindibles para abordar los retos que la ciberamenaza nos presenta. ■



FORO DE LA CIBERSEGURIDAD

PLATINUM SPONSORS



GOLD SPONSORS

CYBER SECURITY CENTRE



Daniel Largacha

Director del Centro de Estudios en Ciberseguridad de ISMS Forum.

Entrando en la nueva era de la ciberseguridad



El presente año será principalmente recordado como el año en el que la privacidad marcó un punto de inflexión, no sólo en Europa sino en el mundo entero. No obstante, con independencia de que la GDPR se centra en la privacidad de los individuos estableciendo unas reglas de uso razonable y legítimo sobre el tratamiento de datos de los ciudadanos, este nuevo marco normativo introduce de forma implícita implicaciones importantes sobre la ciberseguridad. No podemos obviar que nuestros datos, ya sea como ciudadanos, consumidores o clientes se almacenan, se tratan y se transmiten por redes y sistemas de información, y los únicos soportes para garantizar del uso adecuado y su protección y acceso por parte de terceros está fundamentado en el grado de control que las organizaciones sean capaces de implementar en sus sistemas y tecnologías por medio de la ciberse-

Pero más allá de la privacidad, este año también hemos visto la transposición al marco legal español de la directiva NIS que, aunque tiene un alcance más limitado que la GDPR, ya que tan sólo afecta a los

operadores de servicios esenciales y proveedores de servicios digitales, tendrá un efecto potenciador de la ciberseguridad en las organizaciones en general que muy probablemente, por efecto de la transitividad o simplemente por contagio, facilitará un estímulo de la ciberseguridad en toda la industria y, por ende, en la sociedad.

Además, como tercer catalizador tenemos una creciente tendencia de digitalización de las empresas que está presente en las agendas de todas las empresas. El proceso transformador de la industria en la que estamos inmersos ofrece muchas oportunidades que llevan asociados diferentes riesgos para cada sector, pero uno común para todos, y es que en la medida en la que este proceso aumente el apalancamiento tecnológico de las operaciones de las empresas, aumentará en la misma medida la exposición de las empresas frente a los riesgos, especialmente los ciberriesgos relacionados con la ciberseguridad.

A tenor de lo anteriormente expuesto, es evidente visualizar la importancia actual y futura que la ciberseguridad va a tener tanto en las empresas, ya sea para el cumplimiento de la legislación como para la protección de los intereses de sus clientes, accionistas y demás stakeholders, como también para los ciudadanos y estados, puesto que el actual estado de bienestar como lo conocemos hoy en día requerirá de un elemento estabilizador fundamental que es la ciberseguridad y su preservación en el futuro.

Este escenario supone un cambio sustancial del contexto al que se encuentran expuestas las empresas que van a tener que desarrollar una capacidad de adaptación que les permita seguir conectados al ciclo de la evolución.

“El actual estado de bienestar como lo conocemos hoy en día requerirá de un elemento estabilizador fundamental que es la ciberseguridad y su preservación en el futuro”



Este proceso de adaptación es complejo dado que va a requerir que esta capacidad de adaptación se siga desarrollando, sin dejar de atender otros escenarios o modelos de negocio más clásicos, de cara a poder sobrevivir. Todo ello, en un escenario global que no despeja las incertidumbres del futuro y de agotamiento del ciclo económico actual que obligará a las empresas a ser eficientes y selectivas en la dedicación de recursos.

La colaboración sectorial entre todos los actores (empresas públicas, privadas, organismos gubernamentales, proveedores, otras asociaciones, etc.) tendrá un papel crítico en la consecución del éxito, mediante la facilitación de herramientas y medios a la industria, que ayuden y favorezcan la estimulación del desarrollo de una industria de la ciberseguridad sólida y madura que permita afrontar estos nuevos retos. ISMS Forum Spain siempre ha tenido este carácter vocativo hacia la industria, y desde el Centro de Estudios de Ciberseguridad (CSC, sus siglas en inglés) se contribuye al desarrollo y potenciación de la ciberseguridad mediante iniciativas que se desarrollan en el seno de ésta gracias a la colaboración de sus miembros.

Entre estas iniciativas se pueden identificar los siguientes objetivos:

- Iniciativas para la creación de escenarios de colaboración. Proyectos como el de Gestión de Crisis Cibernéticas o el de los Ciberejercicios Multisectoriales, que permiten ofrecer una visión clara del estado de la ciberseguridad de las organizaciones frente al resto, de cara a conocer de forma más real la eficiencia de los controles y procedimientos ante eventos ciber.
- Intercambio de información de ciberseguridad. Mediante la creación de una plataforma común y neutral de intercambio de las principales amenazas y ataques que pueden afectar a las empresas.
- Fomento de la concienciación y divulgación de la ciberseguridad. Mediante la elaboración de guías y documentos de referencia que ayuden al establecimiento de terminologías, conceptos y buenas prácticas comunes que permitan establecer un consenso en el sector y faciliten el entendimiento con otros sectores (Libro Blanco del CISO, en colaboración con INCIBE, o
- Potenciar la compartición de conocimiento y la capacitación de profesionales, en ciberseguridad. La realización de foros orientados a profesionales del sector en los que se aborden las últimas tendencias y las futuras, junto con la elaboración de cursos son unas de las principales actividades que han estado presentes en la asociación.

Desde la fundación de ISMS Forum Spain hace 12 años, el carácter vocacional de sus miembros ha estado siempre presente con el fin de ayudar a las empresas y a la sociedad, con el principal ánimo de contribuir a una mejora de la ciberseguridad. Y, con independencia de la complejidad del escenario actual, podemos sentirnos orgullosos de contar con un sector empresarial en general y sectorial específico de la ciberseguridad y enormemente colaborativo, que permite allanar el terreno despejando incertidumbres frente a los riesgos que presentan el escenario actual. ■

CSC: el espacio dedicado a la ciberseguridad de ISMS Forum

E

l Cyber Security Center (CSC) fomenta el intercambio de conocimientos entre los principales actores y expertos implicados en el sector para impulsar y contribuir a la mejora de la Ciberseguridad en España.

CSC pretende crear un estado de conciencia sobre la necesidad de la Ciberseguridad para controlar y gestionar los riesgos derivados de la dependencia actual de la sociedad respecto a las Tecnologías de la Información y la Comunicación (TIC), siendo un aspecto clave para asegurar el desarrollo socioeconómico del país.

Para alcanzar la misión anteriormente descrita, el CSC lleva a cabo una importante labor de análisis (estudios), concienciación (eventos) formación (Curso de especialización en Ciberseguridad), y certificación (certificación profesional de ciberseguridad), entre otras actividades relacionadas con la ciberconcienciación.

Dirección y Comité Técnico Operativo

Director: Daniel Largacha, Mapfre.

- Carles Solé Pascual, CaixaBank.
- Gianluca D'Antonio, ISMS Forum/ Deloitte.
- Enrique Fojón Chamorro, profesional independiente.
- Adolfo Hernández, Sabadell.
- Justo López Parra, Endesa.
- Francisco Lázaro, RENFE.
- Eduardo Di Monte, Oylo.
- José Ramón Monleón, Orange España.
- Daniel García, ISMS Forum.



Eventos

Foros anuales de la Ciberseguridad

El CSC organiza cada año su foro de debate sobre el estado de la ciberseguridad y lleva a cabo otras actividades como la certificación de profesionales, o la elaboración de análisis y estudios a través de sus correspondientes grupos de trabajo, o cursos de formación especializada.

Su evento anual cuenta ya con siete ediciones, logrando convertirse en uno de los encuentros entre profesionales, empresas e instituciones expertas en materia de ciberseguridad, más importantes del panorama nacional.

En su última edición, celebrada el pasado 20 de septiembre en el Círculo de Bellas Artes de Madrid, fueron más de 300 profesionales de la seguridad de la información los que se dieron cita en este encuentro anual, esta vez para debatir sobre el futuro ya presente de la ciberseguridad en las organizaciones, los modelos de madurez y gobierno de la ciberseguridad, la importancia de la ciberseguridad en el ámbito del Data Science y la ética del dato, las posibilidades de integración y orquestación del ecosistema de seguridad corporativo, entre otros temas de máxima actualidad como la trasposición de la Directiva NIS al ordenamiento jurídico español.

La sesión contó con las intervenciones especiales de Rogier Holla, subdirector de CERT-EU (Comisión Europea); Paolo Passeri, fundador de Hackmageddon; y Maria Bada, miembro del Global Cyber Security Capacity Centre (Universidad de Oxford), así como con la representación del Instituto Nacional de Ciberseguridad (INCIBE).



Rogier Holla

VII Foro de la Ciberseguridad
Círculo de Bellas Artes de Madrid


Estudios y Proyectos

El Departamento de Seguridad Nacional e ISMS Forum han impulsado la mejora de la resiliencia empresarial por medio de simulacros de crisis cibernéticas

El Departamento de Seguridad Nacional e ISMS Forum Spain desarrollaron conjuntamente la segunda edición del proyecto “Cyber Crisis Management” con el objetivo de fomentar las buenas prácticas en materia de ciberseguridad y gestión de crisis. Este proyecto ha sido dirigido y organizado por el Departamento de Seguridad Nacional (DSN) e ISMS Forum Spain, en colaboración con terceras entidades públicas como el Instituto Nacional de Ciberseguridad (INCIBE), el Centro Nacional para la Protección de Infraestructuras Críticas y Ciberseguridad (CNPIC), y entidades privadas tales como Ecix Group, Forcepoint, Prosegur Ciberseguridad, LRS, Mapfre, Oylo, Open Cloud, Suez y UCM.

Cyber Crisis Management tiene como principal objetivo evaluar el comportamiento de las empresas en una situación de crisis en la que se produzca un incidente grave de ciberseguridad, así como la capacidad de estas para reestablecer la seguridad de nuevo y resolver el incidente. La finalidad de este proyecto es generar concienciación sobre los riesgos existentes a todos los niveles, reforzar la comunicación y la coordinación (interna y externa) y, en definitiva, entrenar a las empresas en la gestión de ciber-crisis.

Esta segunda edición de Cyber Crisis Management ha alcanzado la participación de 25 entidades; compañías procedentes de sectores clave como banca, seguros, transportes, salud, telecomunicaciones, servicios y energía.



El coronel de la Guardia Civil Andrés Sanz, jefe del SEPROSE, junto con Carlos A. Saiz, vicepresidente de ISMS Forum Spain.



GESTION DE CRISIS CIBERNÉTICAS

El medio especializado, Red Seguridad, entregó el 19 de junio los Trofeos de la Seguridad TIC, que anualmente concede nuestra publicación a los profesionales, instituciones, organizaciones de todo tipo e iniciativas más destacadas del año anterior por su actividad a favor de la ciberseguridad en España. En esta duodécima edición, el Trofeo a la Capacitación, Divulgación, Concienciación o Formación en Seguridad TIC le fue otorgado a la asociación ISMS Forum Spain,

por su Proyecto de Gestión de Ciber crisis, una iniciativa innovadora que tiene como fin fortalecer tanto la capacitación y mejora de procedimientos de los equipos de ciberseguridad de las empresas a través de ciberejercicios.

Recogió el premio Carlos Saiz, vicepresidente de ISMS Forum Spain, entregado por el coronel de la Guardia Civil Andrés Sanz, jefe del SEPROSE.

Estudios y Proyectos

ISMS Forum, con el apoyo institucional de INCIBE, ha puesto a prueba la ciber-resiliencia de 18 compañías españolas

ISMS Forum Spain, a través de su iniciativa Cyber Security Centre (CSC), ha realizado la quinta Edición de los Ciberejercicios Multisectoriales, también denominados como “CiberMS 2018”, con el objetivo de generar concienciación sobre los riesgos en ciberseguridad y fomentar las buenas prácticas entre 18 grandes organizaciones participantes, que se fundamentan en la evaluación de la resiliencia, la medición del estado de madurez y la mejora de las capacidades de detección y respuesta de las organizaciones en materia de ciberseguridad.

La presente edición del proyecto ha sido organizada por la Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum Spain), con el apoyo institucional del Instituto Nacional de Ciberseguridad (INCIBE) y con la colaboración de terceras entidades privadas. Entre ellas, se encuentra Accenture

como empresa evaluadora, la cual ha analizado los resultados obtenidos en el desarrollo del ejercicio. Por su parte, Ecix Group ha sido la entidad encargada de elaborar un estudio que aporta información sobre las implicaciones legales de cada tipo de ataque sobre los resultados obtenidos en las simulaciones y cuáles serían las sanciones a las que las empresas tendrían que enfrentarse. Asimismo, Cymulate y Telefónica han participado bajo el rol de atacantes a las entidades objetivo con objeto de poder evaluar su respuesta.

La iniciativa se ha desarrollado a través de un ejercicio de ciberseguridad consistente en la realización de un conjunto de pruebas de seguridad y simulacros de ataque a los sistemas de las 18 grandes compañías españolas participantes de este año. Las pruebas han estado exclusivamente orientadas a poner a prueba los mecanismos de seguridad lógica de la entidad, así como la cultura de seguridad de los empleados y su capacidad para detectar y comunicar de forma correcta estos incidentes a los equipos de respuesta.

Las pruebas han permitido contrastar la relación entre ataques lanzados y el impacto originado en la entidad participante, a la vez que comparar los resultados con otras



entidades, en una representación anonimizada que permite su identificación. Tras las mismas, el resultado obtenido ha sido que en el 77% de las compañías participantes, el nivel de riesgo -considerando el grado de penetración de las pruebas- ha sido superior al nivel medio. A excepción de este dato genérico, la información obtenida durante la ejecución del proyecto ha sido y será estrictamente confidencial.

La finalidad de los Ciberejercicios Multisectoriales es generar concienciación sobre los riesgos existentes a todos los niveles, reforzar la comunicación y la coordinación, entrenar a las empresas en la gestión de incidentes de ciberseguridad y, en definitiva, generar buenas prácticas sobre ciberseguridad en las organizaciones.

“Como se ha ido demostrando en los últimos años, iniciativas como la de ISMS Forum en colaboración con INCIBE en materia de ciberejercicios multisectoriales demuestran tres cosas. Una, que España es ya un país muy maduro en este tipo de proyectos, lo cual nos hace ser una

referencia, incluso, fuera del entorno europeo. En segundo lugar, que cualquier herramienta que permita entrenar a equipos técnicos con las capacidades operativas o de resiliencia frente a un incidente es fundamental. Y, en tercer lugar, desde INCIBE vamos a seguir apoyando cualquier tipo de iniciativa desde el ámbito privado porque creemos que la colaboración público-privada es uno de los mecanismos de éxito para cualquier iniciativa que fomente la ciberseguridad”, comentó Marcos Gómez, Subdirector de Servicios de Ciberseguridad de INCIBE, durante la presentación de los resultados globales de la quinta edición de los Ciberejercicios Multisectoriales en Accenture.

De esta manera, CyberMS pone de manifiesto, un año más, el importante papel que tiene el sector privado en la ciberseguridad nacional y el bienestar de los ciudadanos, así como los beneficios de la colaboración público-privada.

Presentación de los resultados globales de CyberMS 2018 en Accenture.



Estudios y Proyectos

ISMS Forum, con el apoyo institucional de INCIBE, publica el primer Libro Blanco del CISO: el documento de referencia sobre la figura del CISO en España

La publicación del Libro Blanco del CISO es una iniciativa de la Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum Spain), que cuenta con el apoyo institucional del Instituto Nacional de Ciberseguridad (INCIBE) y que no tiene precedentes en España. En el documento han trabajado más de 20 directores de Seguridad de la Información para definir el estado de la figura del CISO en España, presentando una primera aproximación de las responsabilidades y funciones inherentes a dicha figura, modelos organizativos y soft skills, con el objetivo de poner en el mercado una guía de referencia para los directores de Seguridad de la Información, que a su vez constituye una primera referencia para las propias organizaciones en su definición organizativa.

El papel del CISO (Chief Information Security Officer), director de la Seguridad de la Información en español, es hoy más complejo que nunca. Durante los últimos años, los departamentos de seguridad han tenido que enfrentarse a un panorama de amenazas cada vez más difícil y el CISO ha desempeñado un papel mucho más visible dentro de las organizaciones. Como resultado, el rol del CISO ha experimentado una importante evolución y acercamiento al negocio.



Además, mientras los procesos tecnológicos avanzan, los organismos públicos y los propios lobbies profesionales amenazan con un marco regulatorio cada vez más difícil, donde las empresas deben adaptarse al Reglamento Europeo de Protección de Datos, la Directiva NIS, la Directiva PSD-2, etc., y donde la figura del CISO tiene un papel fundamental para cohesionar los requerimientos normativos en materia de Seguridad de la Información.

Por otra parte, la responsabilidad del CISO dentro de las compañías puede solaparse con otras funciones desempeñadas por el CCO (Chief Communications Officer) o el DPD (Delegado de Protección de Datos), de última creación. Las funciones de cada uno de estos actores desempeñe dentro de la organización deberán definirse ad-hoc según la idiosincrasia de cada una sin

olvidar la necesaria segregación de funciones entre los distintos roles, que garantice transparencia, independencia y control.

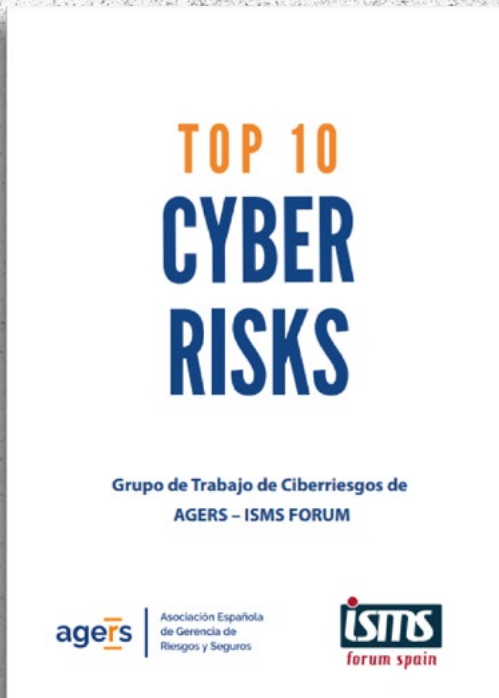
La propia sociedad aumenta el conocimiento en habilidades digitales más rápidamente que la propia concienciación en los riesgos derivados del uso de estas tecnologías digitales, y la función del CISO trasciende el marco puramente empresarial para convertirse en un elemento concienciador y formador en el uso seguro de las nuevas tecnologías, tanto dentro de las empresas como en la misma sociedad.

Por todo ello, ISMS Forum Spain ha impulsado la iniciativa de elaborar el Libro Blanco del CISO, un documento que pretende servir de guía para los directores de Seguridad de la Información, que define, determina y

establece detalladamente sus responsabilidades y funciones. El lanzamiento tuvo lugar bajo el marco de la duodécima edición del Encuentro Internacional de Seguridad de la Información (ENISE), un evento organizado por INCIBE en León, en una mesa redonda que ha contado con la participación de Eva Cristina (Chief of Information Security Officer de Caser), Beatriz Soto (Jefa de Gabinete, INCIBE), Pablo López (2º Jefe del Departamento de ciberseguridad, CCN), Carles Solé (Chief of Information Security Officer de Caixabank), Francisco Lázaro (Chief of Information Security Officer de Renfe) y Gianlucca d'Antonio (Presidente de ISMS Forum Spain).

Guía "Top 10 Cyber Risks", por el grupo de trabajo de ciberriesgos de AGERS e ISMS Forum

Esta guía nace con la necesidad de satisfacer, facilitar el entendimiento entre el experto y el no experto en materia de ciberseguridad. En el manual se exponen 10 tipos de ciberataques diferentes que se desprenden de una encuesta realizada por ISMS Forum y cada uno de ellos cuenta con descripciones y casos reales para su posterior análisis. Este documento pretende servir de ayuda para acercar el ciberriesgo a la sociedad y así saber cómo gestionarlo en caso de necesidad.





Francisco Lázaro

Director del Centro de Estudios en Movilidad e Internet de las Cosas; miembro de la Junta Directiva de ISMS Forum Spain; CISO y DPO de Renfe.

Cada vez más demanda de profesionales cualificados en ciberseguridad

Es evidente que vivimos una época de cambios en el mundo de la Ciberseguridad y esos cambios conllevan nuevas exigencias, las cuales en muchos casos son legales y de aplicación a sectores en los que algunas empresas, o bien por su dimensión o por falta de madurez o ausencia de demanda de las empresas a las que provee productos o servicios, no sentían la necesidad de disponer de profesionales en seguridad de la información (como plantilla propia o como asistencia técnica externa).

Sin embargo, aunque la simple necesidad de protección de sus activos debería haberle llevado a esa necesidad, ha sido la obligación de notificar incidentes y brechas lo que están provocando una alta demanda de profesionales y no sólo en las actividades directamente relacionadas con la gestión de incidentes.

Sea cual sea la motivación, la realidad es que las previsiones de demanda en Europa cifran entre un cuarto de millón y un millón de profesionales los que se necesitan en las diferentes ramas de la Seguridad de la información. En apoyo de esas previsiones para los próximos dos años, lo cierto es que constantemente vemos la dificultad para cubrir puestos en esta práctica.

En el estudio “EXABEAM 2018 CYBER SECURITY PROFESSIONALS SALARY AND JOB REPORT: COMPENSATION, JOB SATISFACTION, EDUCATION, AND TECHNOLOGY OOUTLOOK” de exabeam, podemos analizar la demanda desde la perspectiva de los salarios medios y el grado de satisfacción y estabilidad que el estudio aporta.

El estudio, identifica una ventana salarial media de 42.500 a 60.000 euros en Europa para personal de 0 a 5 años de experiencia, con variaciones según el perfil de especialización (CISOs, gerentes, analistas, respuesta a incidentes, Gestores del Riesgo, arquitectos, consultores, ingenieros de seguridad, simulación de adversarios, seguridad en aplicaciones, gestores del programa de seguridad -proyectos-, cumplimiento, seguridad de equipos de trabajo, analistas de malware, hacking ético, especialistas SIEM, analistas de red, especialistas SOCs, entre otros).

Actitud, conocimientos, habilidades, capacidades, exigencia, experiencia, constante actualización y colaboración, son los ejes sobre los que un profesional de ciberseguridad desarrolla de una forma eficaz y eficiente su exigente trabajo. La Certificación CCSP se ha construido sobre esos mismos pilares, con la intención de transmitirlos con rigor y pasión a los alumnos de la Certificación.

Actitud, conocimientos, habilidades, capacidades, exigencia, experiencia, constante actualización y colaboración, son los ejes sobre los que un profesional de ciberseguridad desarrolla de una forma eficaz y eficiente su exigente trabajo. La Certificación CCSP se ha construido sobre esos mismos pilares, con la intención de transmitirlos con rigor y pasión a los alumnos de la Certificación.

“Actitud, conocimientos, habilidades, capacidades, exigencia, experiencia, constante actualización y colaboración, son los ejes sobre los que un profesional de ciberseguridad desarrolla de una forma eficaz y eficiente su trabajo”



intención de transmitirlos con rigor y pasión a los alumnos de la Certificación. La Certificación comenzó a impartirse en el 2016, al identificarse por parte del comité de la iniciativa del CYBER SECURITY CENTRE (CSC) del ISMS Forum, la necesidad de formar en este campo a profesionales que tuvieran la necesidad de adquirir conocimientos globales y de calidad, compaginando los conocimientos teóricos con la experiencia de expertos y reputados profesionales y que la duración y horario del curso sea compatible con su trabajo.

El temario de la certificación fue creado por 9 profesionales en activo con una dilatada experiencia en puestos de responsabilidad en Seguridad de la información, Riesgo, Auditoría, Legal, Hacking y Gestión de Incidentes de Seguridad. El claustro de profesores, elaboraron el temario en base a los conocimientos que identificaron como necesarios para la práctica y desde las diferentes esferas de operación y cumplimiento, lo que incluye las infraestructuras críticas y los servicios esenciales sobre redes y sistemas de información. El temario y su contenido se revisa anualmente.

El examen que debe realizarse al terminar la formación garantiza la asimilación y aprendizaje del alumno, poniendo en valor el certificado profesional.

En las tres ediciones celebradas hasta el momento, la nota media del curso ha sido mayor que 4, sobre 5, resaltando los alumnos la capacidad para transmitir la experiencia de los diferentes profesores y valorando muy positivamente como esa experiencia hace más fácil la tarea de asimilar los conceptos y contenidos.

Queremos destacar que la preparación a la Certificación más allá del espacio temporal en la que se desarrolla, al ser una actividad del ISMS garantiza una vez finalizada, la colaboración con otros profesionales y el intercambio de conocimientos y experiencias en el seno de las actividades y relaciones del ISMS Forum.

El personal objetivo es aquel que desea estar capacitado para puestos de mayor responsabilidad, servir de apoyo a las capas de gestión y gobierno, complementar el conocimiento que dispone en áreas relacionadas – DPO, cumplimiento, auditoría – o directamente capacitarse en ciberseguridad, entre otros. La obtención de la Certificación puede realizarse también por Reconocimiento de Méritos. Para obtener la Certificación con arreglo a este Programa, los candidatos deberían contar con 10 años de experiencia en el Área y obtener al menos 30 puntos en el esquema de reconocimiento.

Por todo lo expuesto, es por lo que afirmábamos que la Certificación CCSP se construye sobre los pilares que definen un profesional de la Ciberseguridad: actitud, conocimientos, habilidades, capacidades, exigencia, experiencia, constante actualización y colaboración. ■

Certificación en ciberseguridad

CCSP: Certified Cyber Security Professional

Certified Cyber Security Professional (CCSP) nace con el objetivo de ser la primera certificación española dirigida a los profesionales del ejercicio de gobierno de la ciberseguridad. La obtención de la certificación acredita un alto nivel de especialización en ciberseguridad y reconocimiento del ejercicio de la profesión.

¿Para qué una certificación de profesionales de la Ciberseguridad?

La información se ha convertido en uno de los activos que toda empresa debe proteger y salvaguardar frente a un entorno adverso que atenta contra su confidencialidad, integridad y disponibilidad. Gestionar adecuadamente la seguridad de la información debe ser un medio encaminado a minimizar las amenazas a las que está expuesta, al tiempo que se optimiza la inversión en seguridad que una empresa debe afrontar, e incluso se mejoran las oportunidades de negocio. En este sentido, la certificación de profesionales de la ciberseguridad se hace imprescindible ante una demanda de profesionales cada vez mayor.

¿A quién está dirigida?

La certificación está pensada para directores de seguridad; abogados; auditores; consultores; técnicos de seguridad y de sistemas con responsabilidades en esta área de creciente importancia en todo tipo de organizaciones.



Certified Cyber Security Professional

¿Cómo obtener la certificación?

La certificación Cyber Security Professional (CCSP) se podrá obtener superando una prueba teórica y acreditando experiencia profesional de al menos 3 años en el ámbito de la seguridad de la información. La experiencia profesional deberá acreditarse una vez superado el examen, en un plazo no superior a 3 años. La certificación también se podrá obtener a través del Programa de Reconocimiento de Méritos Profesionales, acreditando al menos 10 años de experiencia profesional, así como otros criterios de formación y puesta en práctica de la seguridad de la información.

Áreas de la certificación

- Área 1: Gobierno de seguridad (21%)
- Área 2: Análisis y gestión de riesgos (11%)
- Área 3: Cumplimiento legal y normativo (11%)
- Área 4: Operativa de Ciberseguridad (16%)
- Área 5: Gestión eficaz de incidentes (11%)
- Área 6: Infraestructuras críticas (11%)
- Área 7: Ciberinteligencia, cooperación y capacidad (5%)
- Área 8: CISO Soft Skills (5%)
- Área 9: Examen práctico y tutorías (9%)

Inscripción

Para inscribirse envíe un email a: atencio-nasociado@ismsforum.es.

Formación en ciberseguridad

Curso de especialización en Ciberseguridad: Certified Cyber Security Professional

Este curso ofrece profundos conocimientos sobre los fundamentos y gobierno de la ciberseguridad, arquitecturas, políticas, estrategia y estándares, análisis y gestión de riesgos, marco normativo, operativa de ciberseguridad, infraestructuras críticas, ciberinteligencia, gestión de incidentes, buenas prácticas y soft skills de la figura del Director de Seguridad de la Información.

El curso está dirigido a directores de Seguridad de la Información, consultores, abogados, auditores, técnicos de seguridad y técnicos de sistemas con responsabilidades en la seguridad y de sistemas.

Plataforma de formación online: Moodle

ISMS Forum ha puesto en marcha la creación de una plataforma de formación online que configura un Aula Virtual para que los alumnos de los cursos CEPD Y CCSP puedan realizar un seguimiento de la organización de los contenidos del curso en cuestión.

Además, la Asociación ha identificado la necesidad de iniciar una modalidad de formación no presencial vía streaming a través de la cual el alumno puede seguir las clases en directo, o bien en diferido, hasta el plazo límite que se haya establecido para visualizar ese contenido antes de ser retirado de la plataforma.



LECTURAS IMPRESCINDIBLES

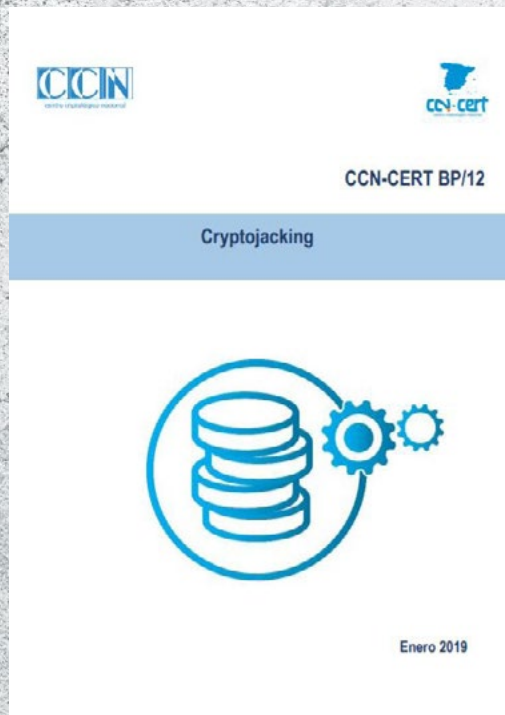


Guía Nacional de Notificación y Gestión de Ciberincidentes

El Ministerio de Interior ha creado una guía con directrices para notificar y gestionar ciberincidentes, con el objetivo de tener un marco de referencia y evitar disparidad de criterios en este ámbito.

España es el primer país de la UE que cuenta con una guía de este tipo, que fue aprobada el 9 de enero por el Consejo Nacional de Ciberseguridad y fue coordinada por el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).

La guía es un documento técnico que contiene directrices para denunciar ciberincidentes y describe criterios determinados que clasifican los incidentes en cinco niveles de peligrosidad: crítico, muy alto, alto, medio y bajo.



Cryptojacking

El Centro Criptológico Nacional (CCN-CERT) ha creado una Guía de buenas prácticas en materia de cryptojacking. Su auge ha ido aparejado al alza de las cotizaciones de las monedas virtuales, además se caracteriza por ser fácil de efectuar y automatizar, con la dificultad de detectar su presencia en el dispositivo infectado. Durante el año 2017 se produjo un incremento del 34.000% en ataques relacionados con el cryptojacking. Tan sólo en los tres últimos meses de 2017 el crecimiento de este tipo de prácticas fue del 8.500 %. Con este informe, el CCN-CERT pretende orientar al usuario en el correcto empleo de las tecnologías, para evitar así los riesgos derivados del cryptojacking.



Cyber Europe 2018: After Action Report

ENISA ha elaborado un informe en el que recopila toda la información extraída de los ejercicios cibernéticos que realiza cada año, analizando e identificando posteriormente los desafíos a los que se enfrentan los participantes y realizando recomendaciones útiles para los participantes.

Threat Landscape Report 2018: 15 Top Cyberthreats and Trends

2018 ha sido un año que ha traído cambios significativos en el panorama de amenazas cibernéticas contra las que luchamos. Esos cambios han tenido su origen en las numerosas tácticas y estrategias de los diversos grupos de cibercriminales y actores que trabajan para un estado. ENISA ha elaborado su informe anual de amenazas.

IoT Security Standards Gap Analysis

Este estudio realizado por ENISA proporciona directrices para el desarrollo de estándares, facilitando la puesta en marcha de aspectos concretos que determina la Directiva NIS.

Good practices on interdependencies between OES and DSPs

Este estudio, también de ENISA, se ocupa de las dependencias e interdependencias entre los Operadores de Servicios Esenciales (OES) y los Proveedores de Servicios Digitales (DSP), tal como se definen en la Directiva NIS.



accenturesecurity

Aiuken
Cybersecurity

Akamai

Check Point
SOFTWARE TECHNOLOGIES LTD.

CYLANCE

Deloitte.

FORCEPOINT
POWERED BY Raytheon

FORTINET.

GuardiCore

helpsystems

HUAWEI

IBM

Infoblox
NEXT LEVEL NETWORKING

KASPERSKY lab

McAfee™

GLOBAL SPONSORS





La Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain, 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

Paseo de la Habana, 54, 2 Izquierda, 1
28036, Madrid, Spain



[@ISMSForumSpain](https://twitter.com/ISMSForumSpain)



[ISMS Forum Spain](https://www.linkedin.com/company/ismsforumspain)