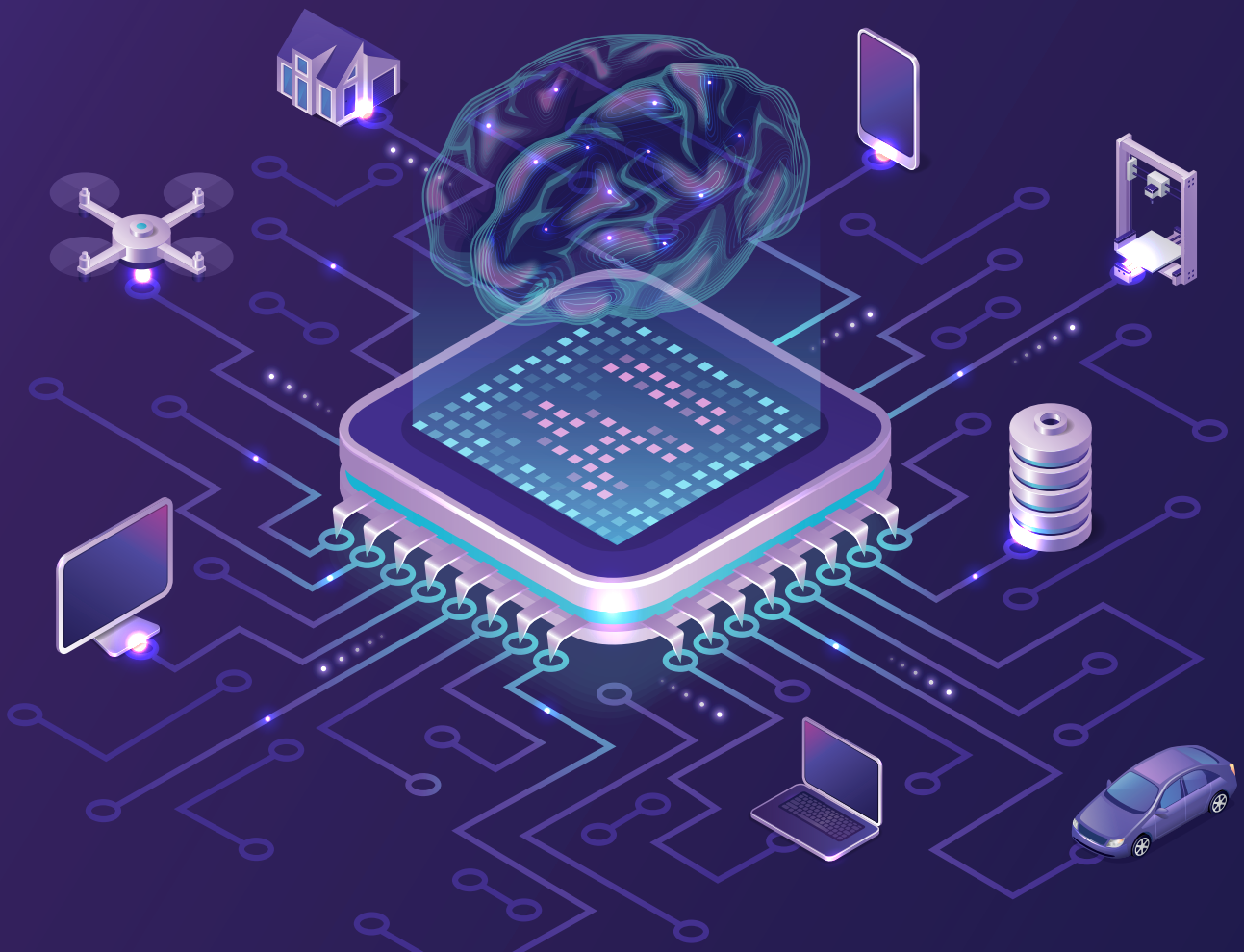
isms forum | INTERNATIONAL INFORMATION SECURITY COMMUNITY

CSC CYBER SECURITY CENTRE

INTELIGENCIA ARTIFICIAL Y CIBERSEGURIDAD

ANALIZAR, DETECTAR Y RESPONDER A LAS AMENAZAS



XII FORO DE LA CIBERSEGURIDAD

ORGANIZADO POR EL CYBER SECURITY CENTRE (CSC) DE ISMS FORUM

MAYO 2023

ENTREVISTAS
Ángel Pérez (Abertis)
Inteligencia artificial y ciberseguridad

ESTUDIO
Observatorio de la Ciberseguridad
Comparativa personalizada

ACTUALIDAD
Cristina Dolan (NetWitness)
Tecnologías disruptivas y ciberseguridad

www.ismsforum.es

DANIEL LARGACHA LAMELA

Director del Cyber Security Centre de ISMS Forum

ISMS FORUM

ismsforum.es

La transformación cibersegura

LA CIBERSEGURIDAD DEBE SER PARTE INHERENTE DE LA TECNOLOGÍA

Tristemente, la guerra irrumpió el año pasado en la vida de los ucranianos frente a las puertas de los países de la Unión Europea. El inicio del escenario bélico estuvo precedido —tan solo unas pocas horas antes— por varios ataques cibernéticos por parte de las fuerzas rusas. De nuevo, esta situación pone en escena la ciberguerra como un dominio más en la que se opera.

Es evidente que el inicio de la guerra puso al mundo empresarial en una nueva ventana, que ha cambiado drásticamente el modo en el que las organizaciones perciben los conflictos y cómo les afectan.

> **La clave no será centrarse en el oportunismo, sino entender que la ciberseguridad es parte inherente de la tecnología**

Poco más de un año después, el panorama que vivimos es un poco diferente, desde luego, mucho más positivos a algunos de los escenarios que se barajaban de forma previa, especialmente a los más catastrofistas. Si atendemos a los datos oficiales que se manejan (muy escuetos, de momento), los ataques contra la sociedad parecen haber disminuido en número, tal y como muestra la comparativa en cuanto al número de ataques proveniente del informe IC3 del FBI de 2023.

Grandes están mejor protegidas

Aunque se trata de un dato sesgado, sobre el que habría que hacer varias lecturas, lo que parece evidente es que las grandes empresas, aquellas que venían siendo las principales víctimas de los ataques de *fjfiffiH ffjffiffiffiflfiffi*, van dejando de ser noticia, precisamente debido a este tipo de ataques.

Esto se debe a varios factores. El primero de ellos, y creo que el que tiene un mayor nivel de relevancia, es que estas organizaciones han incrementado significativamente su nivel de protección, elevando el grado de sofisticación —y de medios necesarios— para que los cibercriminales puedan tener éxito en un ataque.

Como si fuera una ley de mercado del cibercrimen, esta postura ha provocado que el cibercrimen se haya recompuesto, buscando víctimas menos preparadas —más fáciles— que permitan incrementar las posibilidades de éxito. Esto ha provocado un aumento de los incidentes en empresas de menor tamaño que, a pesar de tener una menor visibilidad, también cuentan con un nivel de madurez inferior en cuanto a ciberseguridad. Lógicamente, todo ello a costa también de que estos ciberdelincuentes reduzcan los ingresos que venían obteniendo.

El segundo factor tiene que ver con el conflicto bélico, que también parece que ha concentrado las capacidades de algunos estados en las partes involucradas directamente en el conflicto. Además, también ha afectado a las infraestructuras críticas de los estados que apoyan a cada uno de los bandos, con especial atención a los colindantes con alguno de los países del conflicto.

Confiabilidad de la tecnología

Esta tensa calma la están aprovechando aquellas empresas y organizaciones que han visto la oportunidad para mejorar el nivel de ciberresiliencia, dotándose de tecnología y capacidades que le permitan encarar el futuro en una mejor posición. Todo ello al compás de una transformación tecnológica que empieza a tomar forma en su seno.

El factor clave del éxito de estas iniciáticas, al buen entender del que suscribe el texto, no será centrarse en el oportunismo de las actuales circunstancias, sino entender realmente que la ciberseguridad es una parte inherente de la tecnología. Debe verse como un elemento determinante en su uso, un factor que es capaz de aportar uno de los valores fundamentales en cuanto a las necesidades del ser humano: la confiabilidad.

Las nuevas tecnologías serán, o no, parte inseparable del futuro de la sociedad en función de lo confiables que —entre todos— consigamos que sean. Y esto es algo que nos concierne a cada uno de nosotros como usuarios, trabajadores de una empresa y ciudadanos de un país. «

DIRECTOR GENERAL
Daniel García

SUBDIRECCIONES
Beatriz García
Leire Ruiz

CONSEJO EDITORIAL/ REDACCIÓN
Cynthia Rica
Rim Souri

EQUIPO DE GESTIÓN
Beatriz Lozano
Beatriz García
Cynthia Rica
Leire Ruiz
Rim Souri
Virginia Terrasa
Wasim Escribano
Marta García

HAN COLABORADO
Ángel Pérez
Cristina Dolan
Daniel Largacha
David Moreno
Enrique Cervantes
Francisco Lázaro

PÁGINA WEB
www.ismsforum.es

JUNTA DIRECTIVA

PRESIDENTE
Gianluca D'Antonio, miembro independiente

VICEPRESIDENTE
Carlos Alberto Sáiz, Ecix Group

TESORERO
Roberto Baratta, Abanca

VICESECRETARIO
Francisco Lázaro, RENFE

CONSEJO ASESOR
Juan Miguel Velasco, secretario
Fernando Sánchez, miembro

VOCALES
Xabier Michelena, Accenture
Carles Solé, Santander
Gonzalo Asensio, Bankinter
Ricardo Sánz, Evolution
Rafael Hernández, Cepsa
David Barroso, miembro independiente
Rubén Frieiro Barros, Deloitte
Edwin Blom, FCC
Jesús Sánchez, Naturgy
Guillermo Llorente, independiente
Luis Buezo, Hewlett Packard Enterprise
Susana del Pozo, IBM
Marcos Gómez, Incibe
Virginia Rodríguez, CaixaBank
Laura Iglesias, Vodafone
Javier Urtiaga, PWC
Javier García Quintela, Repsol
Roberto Pérez, SIA, An Indra Company
Ivan Garrido, S21sec
Miguel Á. Pérez Acevedo, Telefónica
Iván Sánchez, Sanitas
Toni García, independiente
José Ramón Monleón, Orange
Miguel Ángel Pérez, Telefónica
Francisco Javier Sevillano, Vodafone

XII Foro de la Ciberseguridad

INTELIGENCIA ARTIFICIAL: ANALIZAR, DETECTAR Y RESPONDER A LAS AMENAZAS

ISMS Forum (International Information Security Community) organiza una nueva edición de su Foro de Ciberseguridad, el encuentro de referencia para los profesionales relacionados con la seguridad de la información. En esta ocasión, atendiendo al aforo necesario y el nivel de interés que ha suscitado, se han elegido las instalaciones de Kinépolis (Ciudad de la Imagen, Madrid) para su celebración.

Este XII Foro de la Ciberseguridad es un interesante evento que reúne a expertos internacionales y nacionales en el ámbito de la ciberseguridad, que aportarán su visión y conocimiento sobre cómo afrontar los retos presentes y futuros en este ámbito. La decimosegunda edición de este congreso está dirigido a un amplio conjunto de perfiles relacionados con este tema, como pueden ser directores de seguridad de la Información, profesionales con responsabilidad en seguridad, técnicos de seguridad y de sistemas, *data privacy officers* (DPO), responsables de protección de datos, asesores jurídicos, consultores, abogados y auditores.

> **Uno de los objetivos de esta edición es profundizar sobre todo lo que aporta la IA en el contexto de la ciberseguridad**

A lo largo de la jornada se han definido una serie de *tracks* en los que se abordarán temas de una especial relevancia en este ámbito, como son las estrategias, las tendencias y las buenas prácticas de ciberseguridad. A lo largo de estas sesiones se han planteado una serie de ponencias que han sido desarrolladas por expertos y especialistas de primer nivel, tanto en el ámbito nacional como el internacional.

En cualquier caso, el *leit motiv* de esta nueva edición está centrado en todo lo que aporta la inteligencia artificial (IA) en el contexto de la ciberseguridad, teniendo en cuenta el enorme protagonismo que ha ido adquiriendo en organizaciones de cualquier tamaño y sector. Es evidente la importancia de este tipo de herramientas y tecnologías a la hora de responder ante el creciente volumen de amenazas, que, además, cada vez presentan un mayor nivel de complejidad. Estas tecnologías son el único medio para simplificar y reducir drásticamente el número de alertas diarias que se reciben, y también de responder a las amenazas en los tiempos adecuados.

Otro de los puntos importantes de esta edición será la presentación de la Guía DevSecOps, elaborada por el grupo de trabajo de ISMS Forum, que se plantea como una inestimable ayuda para que los especialistas del ámbito de la ciberseguridad puedan integrar este elemento en el nuevo modelo de trabajo que integra a los equipos de desarrollo y de operaciones. El objetivo: seguridad desde el diseño y por defecto.

Ciberejercicios

Una de las iniciativas que se van a desarrollar durante este XII Foro de la Ciberseguridad son estos Ciberejercicios, que se fundamentan en la evaluación de la resiliencia, la medición del estado de madurez y la mejora de las capacidades de las organizaciones en materia de ciberseguridad.

La iniciativa se desarrolla a través de un conjunto de pruebas de seguridad y simulacros de ataques a los sistemas de las organizaciones participantes. A partir del análisis de fuentes externas, y de los resultados de cada ataque, se realizará una evaluación del nivel de madurez, así como de la capacidad de detección y respuesta de cada organización.

La finalidad de las pruebas es la generación de buenas prácticas y el fomento de la concienciación de los riesgos y de la cultura de la seguridad en las organizaciones.

El ciberejercicio pretende cubrir los vectores más importantes de un ataque real siguiendo una metodología definida: recolectar información, analizar activos y explotar vulnerabilidades. Estas fases se ejecutan una y otra vez para conseguir objetivos concretos, cubriendo las fases más importantes de la gestión de incidentes: perfil de la entidad, detección y análisis, y contención, eliminación y recuperación.

Para ello, se han diseñado una serie de pruebas a las que se someterán las entidades participantes, que estarán orientadas a contrastar 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.

Dichas pruebas permitirán contrastar la relación entre los ataques lanzados y el impacto originado. Además, se les ofrecerá también un *ranking* de empresa, un documento en el que se posicionan —en una representación anonimizada— los resultados obtenidos en comparación con los de otras entidades similares. La empresa evaluadora es NCC Group.

Prueba 1 — Rating & Risk Quantification

Mastercard proporcionará el *rating* de ciberseguridad de las compañías participantes para evaluar su situación de riesgo en TI y conocer el potencial impacto económico de dichos riesgos. En base al "Internet Surface" de las compañías participantes, Riskrecom producirá perfiles integrales de TI, de seguridad y de valor de activos de TI para generar *risk-prioritized ratings* y hallazgos comparativos entre los participantes como resultado de tres capacidades de creación de datos primarios.

» **Perfiles de TI detallados**. Descubrimos y catalogamos todos los sistemas orientados a internet administrados por la organización, así como aquellos que externaliza a proveedores de infraestructura. Luego, operamos un conjunto de técnicas pasivas para identificar las redes, la ubicación geográfica, los *hosts* y los servicios de *host*, el contenido del sitio web y el software instalado.

» **Evaluación de problemas**. Evaluamos cada sistema descubierto utilizando más de cuarenta criterios de seguridad y configuraciones de TI. Esto se complementa con fuentes confiables de inteligencia de amenazas.

» ***Compliance***. Proporcionaremos los indicadores positivos de cumplimiento en los principales indicadores de la industria: NIST, DORA, GDPR, ENS, etc.

Prueba 2 — Explotación y últimas amenazas

Se realiza la simulación de un ataque en fase de explotación en los *endpoints* de los asistentes. En estos ciberejercicios, Cymulate nunca ejecutará *malware* o *exploits* comerciales, sino que utilizará su propio software de simulación:

» **Amenazas inmediatas**. Se probarán diez amenazas a nivel de correo, *endpoint* y tráfico de red. Estas amenazas serán de alta probabilidad y alto impacto, recién encontradas en el mundo tecnológico.

» **DLP**. Comprobar a exfiltrar varias plantillas de datos de múltiples formas.

» **WAF**. Comprobar las configuraciones de los WAF perimetrales .

Prueba 3 — Detección de dominios maliciosos

Fortra realizará una búsqueda de dominios creados por terceros que podrían suplantar el principal dominio de la marca de las empresas, y generará un informe de los riesgos encontrados. Los resultados darán una indicación del nivel de riesgos digitales de la marca, de

la exposición de los clientes a amenazas (estafas y robos de identidades), y de si, tanto la empresa como sus clientes, son un objetivo para cibercriminales.
Se buscarán amenazas como dominios similares (*look-alike domains*), sitios web falsos, apropiación de marca, redirección de tráfico web o páginas creadas para robar credenciales de los clientes, que pueden afectar a la reputación. Lamentablemente esto es habitual si la marca tiene exposición pública.

> **Se entrega un *ranking* de empresa, en el que se comparan los resultados obtenidos con los de otras entidades similares**

Para el ejercicio se usará la solución Phishlabs de Fortra, que recolecta múltiples fuentes de datos para detectar dominios maliciosos, incluyendo nuevos registros de dominios, certificados SSL, histórico de registros, así como técnicas avanzadas de *pivoting* y algoritmos. Todos los datos recolectados están alojados en internet y fuera de la organización, por lo que la prueba es no intrusiva.
Durante la prueba se procesarán millones de datos y los resultados clasificarán las amenazas de forma precisa para evitar ruido. La clasificación de dominios se realiza mediante algoritmos e inteligencia artificial, a través de la tecnología PhishLabs, y serán curados con el análisis manual de los consultores del SOC de Fortra.
El informe que recibirán los participantes consiste en el listado de dominios no legítimos, que se clasificarán según el potencial impacto para la marca. Un ejemplo de severidad alta podría ser un dominio similar a la marca que apunta a un sitio para realizar *phishing* o robo de credenciales. Un ejemplo de severidad baja es un dominio similar al de la marca que ya se ha registrado, pero que aún no apunta a un sitio web, o bien aloja un *site* creado para monetizar tráfico.
Opcionalmente, en el marco del ciberejercicio los participantes podrán optar por solicitar la baja (*takedown*) de un dominio que se confirme como malicioso.

Prueba 4 — *Phishing* interno

Este ciberejercicio se centrará en el estudio del comportamiento del usuario final frente a un *phishing* real. Para ello, Fortra analizará el patrón completo de actuación sobre el *phishing* (si lo abre, si hace clic en sus posibles enlaces, si accede a otros sitios web referenciados o si compartiría información de la empresa con terceros).
El resultado de este ciberejercicio muestra información concluyente sobre el número de empleados que:

- Abren el email.
- Hacen clic en el enlace incluido.
- Introducen sus credenciales o datos requeridos en la web a las que les redirigirá esa URL en la que han hecho clic.
- Han reportado el *phishing* siguiendo el protocolo de la empresa (botón en Outlook, etc.).

Para ello, hay una serie de requisitos previos, como contar con un listado de correos electrónicos de los empleados objetivo del *phishing*. En cualquier caso, no se recopilará ningún dato confidencial de la organización, ni de los empleados.

Prueba 5 — Exfiltración

Por último, a través de un autoejecutable, utilizaremos la técnica de movimiento lateral y trataremos de explorar posibilidades de escalado de privilegios, búsqueda de archivos o configuraciones susceptibles y vulnerabilidades. En definitiva, se trata de explorar dimensiones muy superiores al nivel de afectación posible en el vector de origen. «

AGENDA XII FORO DE LA CIBERSEGURIDAD

Track 1 — Estrategias de ciberseguridad

- Regulación de la inteligencia artificial.
- Plataforma de madurez ciber.
- Implementación de la inteligencia artificial en ciberseguridad.
- Fraude digital y protección de identidad.

Track 2 — Tendencias de la ciberseguridad

- Estudio de la ciberseguridad.
- Protección contra futuros escenarios.
- Estrategias de ciberseguridad.
- Identificación de amenazas y protocolo de actuación dentro de las herramientas de la inteligencia artificial.

Track 3 — Buenas prácticas para la ciberseguridad

- Comisión Nacional de Mercado de valores.
- Código de buen gobierno de la ciberseguridad.
- Guía de cifrado AEPD (Agencia Española de Protección de Datos).
- Guía DevSecOps.

XIII ENCUENTRO
CLOUD SECURITY ALLIANCE ESPAÑA

XIII Spanish Cloud Security Alliance Summit

ORGANIZA

isms forum

CSA Spanish Chapter

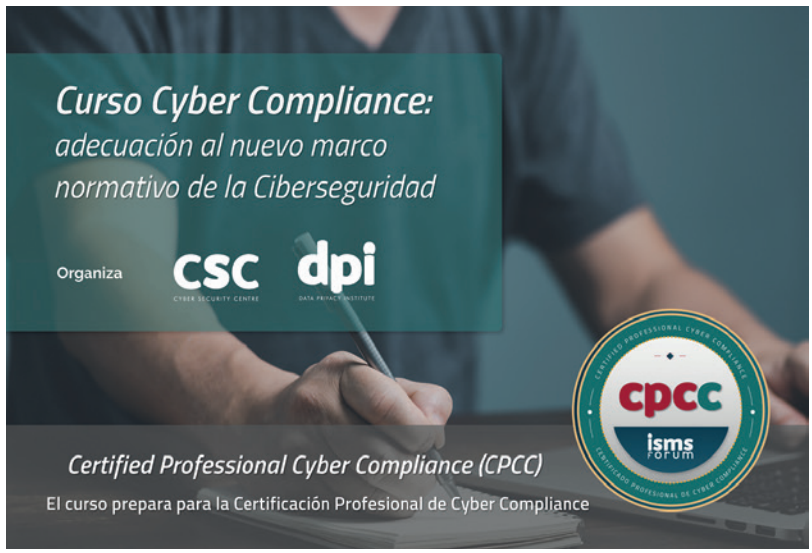
21 SEPT 2023

@ISMSForum
#13CSAISMS

www.ismsforum.es

Curso Cyber Compliance

Adecuación al nuevo marco normativo de la ciberseguridad



Este curso de treinta horas lectivas ofrece una visión completa y detallada del marco legal y regulatorio de la ciberseguridad y de la importancia del cumplimiento normativo. El curso se divide en cinco bloques temáticos que abarcan desde la normativa y los estándares internacionales, hasta las metodologías de riesgo legal y las claves para la implantación de sistemas de gestión de cumplimiento.

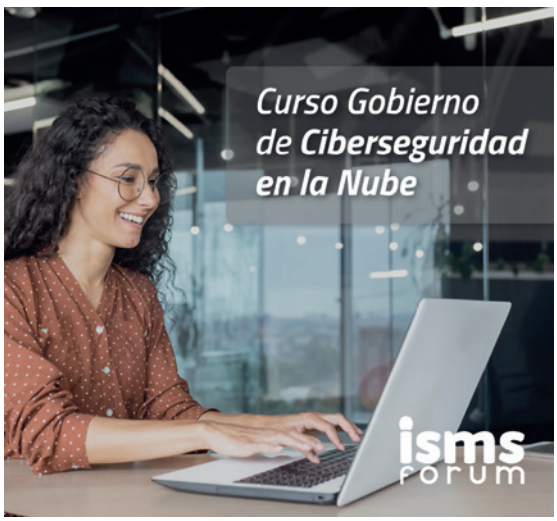
Esta formación ayuda a adquirir las habilidades y conocimientos necesarios para identificar los riesgos tecnológicos, implementar procedimientos internos de seguridad, establecer una cultura de cumplimiento y diseñar planes de ciberseguridad a medida de las necesidades de cada organización. Además, se profundizará en los estándares y buenas prácticas de la ciberseguridad, incluyendo la norma ISO 27001, ISO 27701 e ISO privacy by design.

Este curso prepara para la Certified Professional Cyber Compliance (CPCC).
1ª edición del 6 al 19 de junio.
8 sesiones.
De 16:00h a 20:00h.
Modalidad *online*.
formacion@ismsforum.es

Curso Gobierno de Ciberseguridad en la Nube

Formación sobre cloud

Este curso, con una duración de 52 horas lectivas, surge por la necesidad de contar con una formación específica en esta materia, que profundice en los aspectos clave de la ciberseguridad *cloud* o en la nube. Será impartido por más de 25 profesionales expertos, que tienen responsabilidades a nivel directivo en los departamentos de ciberseguridad de varias de las compañías más representativas del tejido empresarial español.



De forma transversal, el programa abarca un amplio rango de aspectos, que van desde los conceptos básicos relacionados con la nube, *cloud-conomics* o el análisis y gestión de los riesgos en este entorno, hasta aspectos relacionados con el cumplimiento legal y la normativa aplicable en este contexto, los marcos de control existentes o las medidas de seguridad específicas en este tipo de infraestructuras.

Todo ello, lógicamente, sin dejar de lado aspectos tan importantes como la contratación y la gestión de los servicios *cloud*, las tendencias tecnológicas en este tipo de modelos o la evolución que tienen que desarrollar las organizaciones en su viaje a la nube.

Próximas convocatorias: formacion@ismsforum.es

Modalidad *online*.
Evaluación a través de examen presencial.
Horario: de 16:00h a 20:00h.
formacion@ismsforum.es

¿Quieres conocer nuestras certificaciones profesionales en ciberseguridad y protección de datos? ¡Te las presentamos!

Certified Cyber Security Professional (CCSP)

Certified Cyber Security Professional (CCSP) es la certificación de ISMS Forum dirigida a los profesionales de la Ciberseguridad. La obtención de la certificación acredita un alto nivel de especialización en ciberseguridad y reconocimiento del ejercicio de la profesión.

Certified Data Privacy Professional (CDPP)

Certified Data Privacy Professional (CDPP) es la certificación de ISMS Forum dirigida a los profesionales de la Privacidad. La obtención de esta certificación acredita un alto nivel de especialización en la normativa española en materia de Protección de Datos de carácter personal, en un contexto local, europeo e internacional, así como un dominio de los fundamentos de la seguridad de la Información.

Certified Professional Cyber Compliance (CPCC)

Certified Professional Cyber Compliance (CPCC) es la primera certificación española dirigida a los profesionales del Cyber Compliance. La obtención de esta certificación acredita un alto nivel de especialización en la normativa española en materia de cumplimiento en ciberseguridad.

Para estas certificaciones disponemos de dos vías posibles de obtención: proceso de examen de certificación y proceso de acreditación de diez años de experiencia y méritos profesionales.
¡Escríbenos a certificacion@ismsforum.es e infórmate en detalle sobre el proceso y la tasa de obtención!

https://www.ismsforum.es/certificaciones/

"La IA forma parte de los sistemas de protección en la mayoría de las organizaciones"

Lleva más de veinte años colaborando en diversas divisiones y funciones dentro del grupo Abertis, las más destacadas son las de organización y transformación de Autopistas, así como las actuales de CISO, coordinador de gestión de crisis, responsable de continuidad de negocio y coordinador de transformación digital. Además, compatibiliza sus funciones en Abertis con la docencia, y es también colaborador habitual de ISMS Forum.

¿Qué propone la inteligencia artificial en el actual panorama de ciberseguridad?

Aunque la inteligencia artificial (IA) lleva mucho tiempo entre nosotros, este año 2023 está alcanzando un importante nivel de relevancia. Esto es debido a que se están poniendo a disposición del público en general las capacidades de la denominada inteligencia artificial generativa.

> **En ISMS Forum estamos planteando un estudio sobre la relación de la inteligencia artificial y la seguridad**

En el panorama específico de la ciberseguridad, los profesionales del sector estamos observando con especial interés esta evolución, teniendo en cuenta tanto el elevado ritmo de novedades que van surgiendo como la oferta de capacidades en el ámbito de ciberseguridad.

Yendo a los *basics de ciber* —que son proteger, detectar y responder—, podemos ver que prácticamente todos los proveedores de soluciones de ciberseguridad han incorporado tecnologías de IA en sus productos. Sin ánimo de ser exhaustivo, algunos casos relevantes son:

- Evaluación de la identidad mediante comportamiento biométrico.
- Verificación de fortaleza de código y configuraciones.
- Complemento de la estrategia *zero trust* para asistir en la detección de amenazas evasivas y desconocidas.

¿Sería impensable mantener un adecuado sistema de protección sin tener en cuenta la IA?

Casi sin darnos cuenta, la IA ya forma parte de los actuales sistemas de protección en la mayoría de las organizaciones. Sin ir más lejos, un ejemplo actual del uso de inteligencia artificial en la protección de las organizaciones son los sistemas EDR *(endpoint detection and response)* que contienen algoritmos capaces de detectar comportamientos anómalos en los sistemas; pero también se incorporan en los sistemas de detección antifraude.

De forma más genérica, la inteligencia artificial en ciber tiene aplicación en campos tales como la detección de amenazas y de *malware* en la red, o a la hora de complementar a analistas humanos en el SOC para filtrar falsos positivos y evitar el agotamiento por triaje de casos de nivel 1.

Es una herramienta de ayuda a las empresas, pero, en malas manos…

Una IA utilizada con fines maliciosos puede suponer una amenaza real para las empresas, y también para el conjunto de la sociedad. De hecho, ya se han visto casos de uso con fines maliciosos de estas tecnologías.

En el caso de las inteligencias artificiales generativas —como ChatGPT— se han publicado numerosos casos de

ataques de *prompt*, en los que se consiguen vencer los límites marcados por la herramienta para obtener respuestas no deseadas por sus creadores. Es conocido el canal ChatGPT en Reddit, en el que se muestra el caso de la entidad DAN *(do anything now)*: se logra crear una entidad a partir de ChatGPT con un comportamiento muy alternativo al establecido.

En el caso de las inteligencias artificiales más tradicionales, como machine learning, es conocido, por ejemplo, el concepto de ataque por algoritmo adversario. Básicamente, si se conoce el comportamiento del algoritmo se podría llegar a generar un resultado no deseado en función de los datos introducidos. Afortunadamente, la comunidad de desarrolladores ya hace tiempo que propone mecanismos de mitigación de estos riesgos.

Recientemente, la comunidad *ciber* ha observado un auge de *plugins* de IA para navegadores, hojas de cálculo y aplicaciones de todo tipo. Este hecho plantea retos importantes sobre la privacidad, al estar basados en algoritmos públicos, así como retos sobre el sesgo, ya que no se tienen certezas sobre la calidad de los datos que enriquecen dichos algoritmos.

¿De qué forma estáis trabajando en estos temas desde ISMS Forum?

Hace tiempo que estamos siguiendo el desarrollo de la IA y fomentando el debate sobre su relación con la seguridad. De hecho, estamos planteando realizar un estudio en torno a este tema. Un grupo importante de miembros de la Asociación, junto con algunos expertos relevantes en la materia, ya están trabajando en él. En estos momentos, el trabajo se estructura en los siguientes ámbitos:

- Aspectos generales de la inteligencia artificial: teoría, modelos existentes, etapas de evolución e impacto en la sociedad.
- Relación de la inteligencia artificial con la ciberseguridad: cómo son los proyectos de adopción de herramientas de IA.
- Relación de la inteligencia artificial con la ciberseguridad: uso de la IA a favor de la seguridad (casos de uso existentes y buenas prácticas).
- Relación de la inteligencia artificial con la ciberseguridad: uso de la IA como amenaza de seguridad (tipos de ataques conocidos y acciones de mitigación).
- Ética y *compliance* en el uso de la IA.

¿Cómo se está trabando en este aspecto desde las instituciones públicas?

Como Asociación nos consta la preocupación de las instituciones públicas por la rápida adopción de estas tecnologías.

El principal reto es la falta de regulación frente a la velocidad de cambio que estamos viviendo. A nivel territorial, nacional o incluso en el ámbito de la Unión

> **El principal reto de la inteligencia artificial es la falta de regulación frente a la velocidad de cambio que estamos viviendo**

ÁNGEL PÉREZ,
CISO y responsable de resiliencia de Autopistas, la unidad de negocio del Grupo Abertis en España.

Europea se están creando grupos de expertos para velar por la correcta adopción de la IA. Todos tenemos en la cabeza el reciente escrito de un nutrido número de científicos, empresarios y personalidades relevantes solicitando pausar el desarrollo de la IA hasta que haya un marco regulatorio claro.

Entre otras iniciativas cabe destacar la Agencia Española de Supervisión de la Inteligencia Artificial, que no es fruto de una decisión precipitada por los últimos acontecimientos mediáticos en esta materia, sino que ya fue anunciada en diciembre de 2021. La agencia tiene su sede en A Coruña y, tal y como anuncia el Ministerio de Asuntos Económicos y Transformación Digital, *"se encargará de supervisar el desarrollo de un ecosistema respetuoso y garantista en el uso de esta tecnología y potenciará el ecosistema de investigación, empresarial y social relacionado con este ámbito"*. «

"A pesar del miedo que pueden generar, las tecnologías siempre crean oportunidades"

Cristina Dolan es ingeniera, autora y empresaria. Licenciada en Ingeniería Eléctrica, está especializada en Ciencias de la Computación, Comunicaciones de Datos y Negocios, y máster en el MIT Media Lab. Actualmente, dirige Americas Channel, Global Alliances y es la responsable para LATAM en RSA NetWitness. Ha desarrollado su carrera profesional en empresas como Hearst, Disney, Oracle o IBM. Ha participado en la organización y puesta en marcha de Dream it. Code it Win it y es también coautora de libro Transparency in ESG and the Sustainable Economy, Capture Opportunities through Data publicado en 2021.

¿LA CIBERSEGURIDAD ESTÁ EVOLUCIONANDO AL MISMO NIVEL QUE LA TECNOLOGÍA?

La ciberseguridad es un subproducto que agrega un mayor valor a nuestras tecnologías en red y también a los datos que crean y utilizan estos valiosos ecosistemas. A medida que la tecnología evoluciona, la complejidad de la superficie de ataque también aumenta, lo que requiere contar con defensas más sofisticadas para poder mantenerse al día con la innovación.

> **Estadísticamente, muchas de las pequeñas empresas quebrarán dentro de los seis meses posteriores a una violación de datos**

El riesgo cibernético se incrementa con la evolución de las tecnologías en red porque hay más puntos de vulnerabilidad, mayor complejidad y la cantidad de datos generados está aumentando exponencialmente. Este crecimiento de la complejidad de las tecnologías en red crea nuevos desafíos y vulnerabilidades, que son explotadas por *hackers* —y también por estados— que están constantemente refinando sus habilidades para aumentar su capacidad de tener éxito en sus objetivos.

Hoy en día tenemos dispositivos informáticos distribuidos en red que monitorizan y controlan muchos aspectos críticos de nuestras vidas. Las herramientas de defensa cibernética para la detección y respuesta a la red también se han vuelto más sofisticadas.

Todas las organizaciones deben planificar la respuesta a incidentes. Incluso las pequeñas empresas están en riesgo, con una tasa de crecimiento de los ataques que es realmente asombrosa: un 424%. El número de pequeñas empresas que experimentaron un ataque el año pasado aumentó alrededor de un 42%.

Desgraciadamente, las estadísticas están demostrando que muchas de las pequeñas empresas quebrarán dentro de los seis meses posteriores a una violación de datos. Las pequeñas empresas son el corazón de la mayoría de las economías, representan el 95% del tejido empresarial en gran parte de los países y son responsables de casi la mitad de los nuevos empleos.

Los estados nación reconocen que los ataques cibernéticos son armas invisibles que pueden crear una mayor devastación que la costosa guerra tradicional y los ataques físicos.

CRISTINA DOLAN,
Jefa de Canal de las Américas y Alianzas Globales en RSA Security.

¿Cuáles de estas tecnologías disruptivas están teniendo un mayor protagonismo y en qué áreas?

Hay muchas discusiones sobre las herramientas que utilizan las posibilidades de la inteligencia artificial (IA) y su capacidad para replicar e imitar, lo que dificulta la capacidad para diferenciar entre representaciones fraudulentas, auténticas y generadas.

Todos hemos visto los falsos *videoclips* con famosos líderes mundiales o nuevas creaciones artísticas generadas por estas nuevas herramientas. Todos los días se está generando temor entre la sociedad a través de artículos en torno a cómo personas malintencionadas podrían usar estas herramientas para crear estrategias de ataque y *scripts*. Por ejemplo, recientemente se publicó un artículo sobre la velocidad a la que ahora se pueden adivinar las contraseñas utilizando estas herramientas generativas.

Sin embargo, a pesar del miedo que pueden generar todas estas noticias, las tecnologías siempre crean oportunidades. Por ejemplo, los procesadores de texto pueden haber eliminado la necesidad de contar con máquinas de escribir, ya que cambiaron drásticamente el trabajo de los asistentes administrativos. La IA finalmente dará a luz a muchas innovaciones interesantes y valiosas. En cualquier caso, sí es cierto que estas tecnologías requieren de una enorme cantidad de computación y almacenamiento.

La actualización y la innovación constante es un must para el área de ciberseguridad de las empresas ¿Qué retos conlleva?

La ciberseguridad requiere contar con personas inteligentes que estén continuamente innovando para mantenerse a la vanguardia y poder responder con garantías a las amenazas que van apareciendo. A medida que nuestra dependencia de las tecnologías continúa aumentando, también se incrementará el número y nivel de las amenazas a la sostenibilidad de nuestra sociedad.

Hay muchos artículos sobre la brecha en el talento; la formación, la capacitación y la conciencia forman una parte muy importante de la solución. Todas las organizaciones tienen que estar preparadas.

Desde ISMS Forum ¿cómo se puede apoyar a las empresas en este escenario?

Es importante que las organizaciones que formen parte del Foro SGSI (Sistema de la Seguridad de la Información) compartan sus ideas para que, de esta forma, puedan aprender unas de otras. Esta es la mejor manera para que las organizaciones comprendan los riesgos a los que se enfrentan otras empresas en un contexto similar. Además, también les permite explorar el modo en el que los líderes de la industria de la ciberseguridad se preparan para abordar estos riesgos crecientes.

> **La formación es una parte muy importante a la hora de luchar contra la brecha en el talento**

En este contexto, el Foro de la Ciberseguridad que organiza ISMS Forum es uno de los principales eventos de esta industria. A lo largo de este encuentro esperamos compartir nuestra experiencia y modelos de liderazgo con nuestros compañeros, y disfrutar de la oportunidad de aprender de ellos también. «

Observatorio de la Ciberseguridad

El Instituto Nacional de Estándares y Tecnología (NIST) de EEUU define la gestión de riesgos como el proceso continuo de identificación, evaluación y respuesta al riesgo; y para gestionar el riesgo, las organizaciones deben comprender la probabilidad de que ocurra un evento y los posibles impactos resultantes. Esta es la premisa con la que se lanza una nueva edición del Observatorio de la Ciberseguridad de ISMS Forum.

Parte de las actividades de ISMS Forum están dirigidas a promover la formación y la excelencia, fomentar el intercambio de conocimientos o impulsar y contribuir a la mejora de la ciberseguridad en España.

En 2020, la asociación identificó la necesidad de actuar como referente y ofrecer una plataforma para el desarrollo de indicadores que permita la puesta en común y el análisis de aquellas áreas que generan mayor preocupación y, en general, de los riesgos y retos más relevantes. De este modo, se constituye el primer Observatorio de la Ciberseguridad para empresas y profesionales del sector.

Entre los objetivos de este informe anual se encuentran la necesidad de generar claridad sobre el estado del arte de la ciberseguridad empresarial nacional, así como facilitar información de utilidad a través de un indicador que permita interpretar la evolución interanual de los riesgos cibernéticos y su relación con los factores externos. A grandes rasgos se trata de:

- Definir una plataforma para el análisis del nivel de madurez, evolución y nuevos fenómenos en el ámbito de la seguridad de la información.
- Generar indicadores nacionales en empresas y entidades privadas y públicas.
- Promover el conocimiento y la investigación.
- Generar métricas y referencias nacionales.
- Colaborar y mejorar la interlocución con instituciones y reguladores.

Metodología

El indicador de nivel de madurez en ciberseguridad utiliza el marco metodológico basado en el estándar creado por el NIST en 2013, utilizado por entidades de distintos sectores y tamaños. Además, sirve de referencia a las organizaciones que apliquen los principios y buenas prácticas para medir y mejorar sus capacidades de identificación, protección, detección, respuesta y recuperación.

Es importante aclarar que NIST proporciona un marco de políticas de orientación no vinculantes, que cada organización deberá adaptar a sus necesidades, regulación aplicable y naturaleza propias.

Teniendo en cuenta las novedades incorporadas en esta edición *(ver Cuadro)*, en la edición de 2023 se espera contar con una mayor representatividad, superando las 85 entidades que ya se involucraron en esta iniciativa el pasado año. «

INFORME PERSONALIZADO

La edición de 2023 del Observatorio de la Ciberseguridad va a tener una importante novedad. A diferencia de otros años, para recopilar la información se ha creado una plataforma *web* que tendrá una función adicional: todos los CISOs, responsables o *managers* de ciberseguridad que cumplimenten la encuesta tendrán acceso, tanto al informe —similar al de otros años— como a una comparativa personalizada. Es decir, además de tener los datos relativos a un sector en concreto, se entregará también un gráfico con la ubicación de su empresa dentro de su sector.

https://observatoriociber.ismsforum.es/

Guía DevSecOps

INTEGRAR LA SEGURIDAD EN LOS MODELOS DEVOPS

En la actualidad, la mayoría de las organizaciones, sean empresas públicas o entidades privadas, están viviendo un fuerte proceso de adaptación y transformación digital que, en la mayoría de los casos, afecta tanto a procesos de negocio como a aquellos vinculados directamente con las Tecnologías de la Información.

Cada vez es más evidente la necesidad de modernizar los procesos, adaptarse rápidamente a las necesidades del cliente y del mercado, así como aumentar la competitividad. Esta transformación exige a las áreas y equipos de TI una mayor optimización en la generación de valor, lógicamente, con unos tiempos de entrega adecuados.

Desarrollo y operaciones

Teniendo en cuenta este escenario, desde hace varios años ha ido cogiendo protagonismo un modelo de trabajo denominado *DevOps*, que es una combinación de los términos *development* (desarrollo) y *operations* (operaciones). Básicamente, propone la definición de una serie de equipos multidisciplinares capaces de desarrollar, desplegar y operar, autónomamente, soluciones de software de forma continuada y con un alto nivel de automatización.

Lo que tradicionalmente se concebía a través equipos separados —por un lado para la gestión y operación de la infraestructura y, por el otro, para el desarrollo de software—, ahora se convierte en un proceso coordinado y reiterativo. El objetivo es eliminar las ineficiencias y optimizar al máximo la entrega de valor.

DevOps y seguridad

De forma adicional, los equipos de ciberseguridad también han de adaptarse a este nuevo paradigma, aprovechando algunas de sus virtudes como puede ser la idoneidad de los entornos para solucionar *bugs* de manera ágil. Lógicamente, también hay que hacer frente a los retos asociados a este nuevo paradigma en cuanto a la autonomía, la automatización y, sobre todo, al volumen y velocidad que demanda el negocio en los desarrollos. Todo esto es lo que da origen al concepto o filosofía *DevSecOps*.

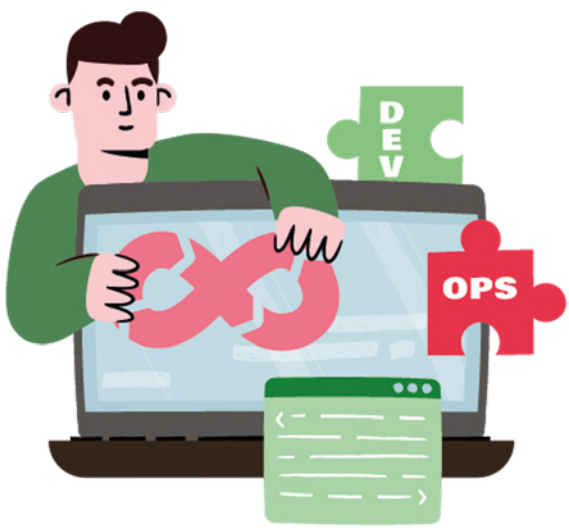
En ISMS Forum somos conscientes de la importancia de este nuevo paradigma de trabajo, y también de la necesidad de integrar la seguridad de la información en todos y cada uno de los procesos implicados.

Guía DevSecOps

Por ese motivo se ha desarrollado la Guía DevSecOps, cuyo objetivo es ayudar a los profesionales de la ciberseguridad a comprender este modelo e identificar sus puntos fuertes o los cambios culturales y organizativos que representa. Además de esto, muestra también el modo adecuado de trasladarlo a la realidad de sus corporaciones, con el único fin de que se cumpla la máxima "Seguridad desde el diseño y por defecto".

> **La Guía DevSecOps ayuda a comprender este modelo e identificar sus puntos fuertes o los cambios culturales y organizativos que representa**

Este es un documento que cubre diversos aspectos de este modelo de trabajo, que van desde los ámbitos más teóricos —sobre el propio modelo DevSecOps, sus orígenes y motivaciones—; pasando por cómo adecuar de forma efectiva los procesos de seguridad en el ciclo de vida de los sistemas, las herramientas disponibles en el mercado o los modelos de madurez; hasta una hoja de ruta que puede servir de guía para los profesionales que estén interesados en su implantación. «



PARTNERS

Platinum Sponsors

CROWDSTRIKE
MANDIANT | Google Cloud
NETWITNESS An RSA Business
paloalto NETWORKS
PENTERA
Recorded Future
SentinelOne
SpyCloud
TIER8
WIZ
zscaler

Gold Sponsors

cyvens Security for the greater good
Akamai
aruba a Hewlett Packard Enterprise company
BITSIGHT
CISCO
Delinea
DEVO
elastic
ENTRUST
Forcepoint
FORESCOUT
FORTINET
HUAWEI
KELA
MNEMO
NEXTVISION & SecurityScorecard
NOZOMI NETWORKS
serval NETWORKS
SIA An Indra company
STORMSHIELD
S21SEC
TREND MICRO
VECTRA
WatchGuard | CYTOMIC

Silver Sponsors

vaultree
zerOD

isms forum
INTERNATIONAL INFORMATION SECURITY COMMUNITY

www.ismsforum.es
@ISMSForum
ISMS Forum