Boletín de Novedades del Centro de Documentación

23 de noviembre de 2023 - Nº 22

Ciberseguridad

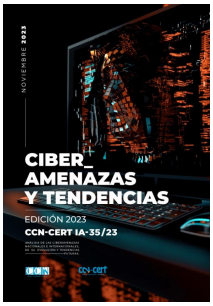
KPMG International ; Haward-Grau, Jason — 16 páginas

[Cibervigilancia: guía para garantizar la resiliencia en ciberseguridad]

En este informe se muestran las propuestas de KPMG para ayudar a las organizaciones a enfrentarse con confianza y de forma proactiva a las ciberamenazas, a recuperarse de los ataques y a salir aún más fortalecidas. Para ello se especifican los pasos a seguir tras la intromisión, se plasman acciones a desarrollar para fortalecer la resiliencia de la organización, y se hace hincapié en la vigilancia para anteponerse ante posibles imprevistos.

Destaca como primer paso tras el ataque definir en qué estado crítico se encuentra, focalizándose en lo realmente importante y ofreciendo la ayuda necesaria a quienes están confrontando la situación. La comunicación, reflexión y adaptabilidad son esenciales para retomar el control. En la siguiente fase de construcción de resiliencia se apunta a la honestidad como base para forjar el aprendizaje de la situación, así como a la necesidad de adelantarse a posibles ciberataques para estar preparados. La vigilancia debe ser contínua para ayudar en la prevención así como mantenerse actualizado sobre las novedades del sector.

Centro Criptológico Nacional — 69 páginas



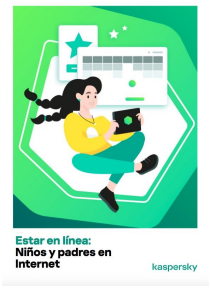
[Ciberamenazas y Tendencias. Edición 2023]

El informe detalla las principales tendencias del año 2023 en relación a las ciberamenazas, repasando las campañas de malware, vulnerabilidades e incidentes registrados en 2022. También se analizan en profundidad las acciones de mayor relevancia, haciendo hincapié en aquellas que han tenido a Ucrania como objetivo a raíz de la invasión por parte de Rusia y la posterior guerra abierta entre ambos países.

Las tendencias de 2023 señalan los nuevos métodos de guerra multidominio, en los que se llevan a cabo operaciones combinadas utilizando los métodos de guerra convencionales junto a las capacidades del ciberespacio. Así mismo, los actores de mayor sofisticación siguen utilizando vulnerabilidades de día cero como vector de entrada, es decir, recurren a fallos no detectados por el desarrollador o el usuario para poder acceder al sistema y atacar. Respecto al ransomware, se espera que siga en aumento el número de ataques, así como el número de grupos activos que llevan a cabo ataques de triple extorsión. Sin duda la inteligencia artificial ha venido a cambiar la manera de entender muchos de los procesos informáticos: se ha visto un aumento en integración de algoritmos no supervisados en las herramientas de seguridad.

En las conclusiones se pone de manifiesto que a lo largo de 2022 se ha podido observar que el ciberespacio ya representa un dominio de batalla de gran importancia y donde los grandes actores asociados a Estados están llevando a cabo una inversión muy importante para disponer de capacidades de la más alta sofisticación. Aunque dicha mejora no solo se está llevando a cabo desde los Estados; el cibercrimen también está invirtiendo en la automatización de sus procesos con el objetivo de minimizar el margen de error y dominar el tiempo de compromiso de la organización, aumentando así el margen de beneficio de los ataques que lanza.

Kaspersky ; Soler, Alberto — 17 páginas



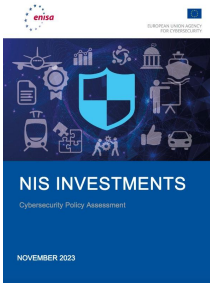
Estar en línea: niños y padres en Internet

Los dispositivos conectados a Internet forman parte del día a día de la ciudadanía española desde edades tempranas. A través de este informe Kaspersky ha realizado un análisis del uso que los progenitores creen que los hijos hacen de Internet. Con este estudio, la compañía quiere visibilizar la importancia de que ambas generaciones estén alineadas en materia de ciberseguridad para que sean conscientes de que las amenazas virtuales y cuenten con herramientas que les permitan mantenerse protegidos. Asimismo, el estudio analiza el nivel de educación en materia de ciberseguridad que los menores reciben, tanto en sus hogares como en las escuelas, a la hora de utilizar tablets, ordenadores o smartphones.

Los datos de este informe proceden de una encuesta realizada por Beruby para Kaspersky entre 1007 madres y padres españoles durante octubre de 2023, a través del método CAWI (Computer Assisted Web Interview).

De acuerdo con los padres encuestados, casi la mitad de los menores españoles (47%) tiene su primer contacto con un dispositivo conectado a Internet antes de cumplir los 7 años. Y 4 de cada 10 (39%) tienen su primer dispositivo con menos de 11 años. Así, las pantallas forman parte de la vida diaria de los más jóvenes. Las respuestas de los padres revelan que la mayoría (38%) pasa entre una y dos horas diarias en Internet y un 30% está conectado más de dos horas. A pesar del tiempo que pasan conectados, el 24,5% de los padres y madres españoles nunca ha hablado con sus hijos sobre los peligros de Internet y solo un 36% de los menores ha recibido varias formaciones sobre ciberseguridad en sus centros educativos, de acuerdo con las respuestas de sus progenitores.

European Union Agency for Cybersecurity (ENISA) ; Adamczyk, Monika et al. — 91 páginas



NIS Investments Report 2023

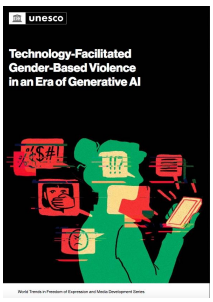
El objetivo de este informe es proporcionar a los responsables políticos pruebas para evaluar la eficacia del actual marco de ciberseguridad de la Unión Europea (UE). Para ello se analizan los datos sobre cómo invierten sus presupuestos de ciberseguridad los Operadores de Servicios Esenciales (OES) y los Proveedores de Servicios Digitales (DSP) identificados en la Directiva de la Unión Europea sobre seguridad de las redes y sistemas de información (Directiva NIS). La influencia de la Directiva NIS en esta inversión es otro de los puntos que abarca el documento.

Además, ofrece un análisis más profundo de la OES en el sector del transporte, examinando, entre otros temas, la influencia y la interacción entre la Directiva SRI y las normativas sectoriales relativas a la protección y la seguridad del transporte.

Para garantizar la representatividad de los 27 Estados miembros de la UE, se encuestó a 40 organizaciones de cada Estado miembro, lo que hace un total de 1.080 organizaciones encuestadas en toda la UE.

Los OES/DSP destinan el 7,1% de sus inversiones de Tecnologías de la Información a la seguridad de los datos, lo que supone un aumento del 0,4% respecto al año pasado. El 42% ha suscrito una solución de ciberseguro dedicada en 2022, frente al 30% del año pasado, aunque solo el 13% de las pymes suscriben un ciberseguro. Los OES/DSP emplean una media del 11% de mujeres a jornada completa en seguridad de la información. El 47% de las organizaciones encuestadas declara no disponer de presupuesto específico para formación en ciberseguridad.

Chowdhury, Rumman ; UNESCO — 34 páginas



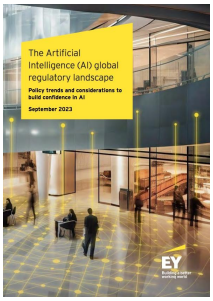
La tecnología al servicio de la violencia de género en la era de la IA generativa

Este informe presenta los resultados de experimentos en profundidad sobre los riesgos asociados al diseño, despliegue y uso de Inteligencia Artificial (IA) generativa como potencial tecnología al servicio de la violencia de género. Evalúa el posible impacto de la IA al permitir la creación de falsos medios realistas, sesgos en los resultados, campañas de acoso automatizadas y la capacidad de construir historias ficticias. Se abordan las ideas extraídas de los experimentos realizados sobre cómo se generan y pueden generarse plantillas de ciberacoso basadas en el género.

Para ello se recurre al análisis de literatura gris, el cual articula la base metodológica de este documento.

Este análisis permite extraer las medidas que deben poner en marcha las empresas de IA generativa y las empresas tecnológicas que les sirven de plataforma, los reguladores y los responsables políticos, las organizaciones de la sociedad civil y los investigadores independientes, así como los usuarios. En el caso de los distribuidores de contenido se les anima a crear soluciones proactivas para identificar contenidos falsificados, incluida la comprobación automática de marcas de agua, mejorando la identificación de contenidos. Respecto a los generadores de contenido estos deben fomentar y apoyar observatorios e iniciativas independientes para supervisar y hacer frente a las campañas de acoso coordinadas y automatizadas. A los formuladores de políticas se les incita a revisar las leyes y normativas relacionadas con los generadores y distribuidores de contenidos para que estén en consonancia con las normas internacionales de derechos humanos, a fin de garantizar la transparencia, la rendición de cuentas, la diligencia debida y la capacitación de los usuarios.

Ernst & Young ; Morini Bianzino, Nicola et al. — 21 páginas



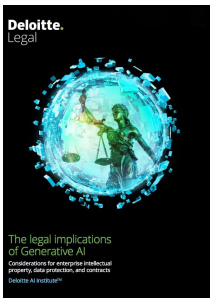
El panorama normativo mundial de la Inteligencia Artificial

Para evaluar la evolución del panorama regulador de la Inteligencia Artificial (IA), el siguiente informe analiza los enfoques reguladores de ocho jurisdicciones que tienen un papel vital que desempeñar en tal desarrollo normativo.

Estas jurisdicciones se seleccionaron en función de su actividad legislativa y reguladora relativas a la IA y de su mayor alcance en el mercado. Se trata de Canadá, China, la Unión Europea (UE), Japón, Corea, Singapur, el Reino Unido y Estados Unidos de América.

Basándose en el análisis de los equipos de Ernst & Young, se identifican tendencias normativas clave que los responsables políticos y las empresas deben tener en cuenta a la hora de trabajar para mejorar la confianza en el uso de la IA. La regulación y las orientaciones consideradas son coherentes con los principios básicos de la IA definidos por la OCDE y respaldados por el G20. Así mismo, estas jurisdicciones están adaptando sus regulaciones a los riesgos percibidos para valores fundamentales como la privacidad, la no discriminación, la transparencia y la seguridad. Por último, muchas de estas jurisdicciones utilizan los espacios aislados de regulación como herramienta para que el sector privado colabore con los responsables políticos en el desarrollo de normas que cumplan el objetivo central de promover una IA segura y ética.

Deloitte AI Institute 20 páginas



Implicaciones jurídicas de la IA Generativa

En este documento se examinan cuestiones jurídicas comunes que surgen en el espacio de la Inteligencia Artificial (IA) Generativa. Para ello se establecen consideraciones sobre la propiedad intelectual, la protección de datos y los contratos. Así mimo se analizan algunos puntos legales comunes, considerando que los marcos normativos aplicables son emergentes y evolucionan rápidamente.

El entusiasmo actual por la adopción de la Inteligencia Artificial se debe en parte a la llegada de la modalidad generativa. A medida que las empresas exploran cómo utilizar estas nuevas herramientas, surgen temas que pueden generar preocupación a diferentes grupos de interés de la empresa, en particular a los profesionales jurídicos. Aunque la ventaja competitiva de la IA Generativa es tentadora, la adopción de esta tecnología potente y diferenciadora exige prestar atención a los riesgos que podrían poner en peligro la marca de una empresa, su reputación, la confianza de las partes interesadas o, lo que es más importante, su cumplimiento de las obligaciones legales y reglamentarias.

Transformación digital del sector público

Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF) 16 páginas

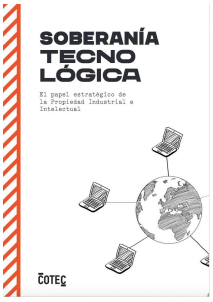
Tecnología en Educación, ¿en qué términos?

El documento se elabora a partir del informe "Global Education Monitoring Report 2023" publicado por la UNESCO sobre la adopción de la tecnología digital en el ámbito educativo y los cambios que ha supuesto dicha inclusión. Expone cómo las regulaciones establecidas para la tecnología no abordan de manera eficaz las necesidades de este ámbito de la sociedad si no se considera el contexto educativo. Se apunta a que lo relevante deben ser los resultados de los procesos de enseñanza y aprendizaje y no simplemente los aspectos tecnológicos.

Respecto a los Objetivos de Desarrollo Sostenible (ODS) se señalan diversos mensajes clave agrupándolos en dos secciones: tecnología en educación y monitorizando la educación. Entre estos puntos se destaca la falta de evidencia clara sobre el posible valor añadido de la tecnología digital en la educación, o las oportunidades que el diseño universal aporta a los aprendices con discapacidad. Así mismo se pone en valor que el derecho a la educación esté englobando cada vez con mayor intensidad el derecho a una conectividad significativa. En cuanto al compromiso con los indicadores de los ODS, 3 de cada 4 países lo han asumido, si bien los porcentajes de posible cumplimiento para 2025 siguen siendo bajos. Se indica que el porcentaje de población infantil sin escolarizar sigue siendo alto, idea en línea con la necesidad de algunos países de mejorar la ratio de matrícula en la 1ª infancia.

Fundación COTEC

48 páginas



Soberanía tecnológica

Este documento destaca el papel de la propiedad industrial como factor catalizador de la soberanía tecnológica y ofrece recomendaciones para su fortalecimiento. Subraya además la importancia de contar con capacidades tecnológicas propias y alianzas con terceros para la comercialización y suministro de tecnologías críticas, evitando dependencias.

Este trabajo es fruto de un Grupo de Trabajo coordinado por PONS IP en el que han participado cerca de 30 miembros de la Fundación COTEC de los ámbitos público y privado.

Destaca la relevancia de la soberanía tecnológica para que un territorio pueda decidir de manera autónoma sobre cuestiones estratégicas. En este sentido se hace una revisión del enfoque adoptado por la Unión Europea que sitúa la soberanía tecnológica dentro del concepto más amplio de autonomía estratégica abierta. Recoge también algunos de los principales retos que enfrenta España para desempeñar un rol relevante en las medidas que se desplieguen en la Unión Europea, entre los que destacan la disponibilidad de perfiles profesionales en ámbitos STEM, o la inversión en las empresas de tecnología profundas (deep tech).

Entre las 13 propuestas en el ámbito de la propiedad industrial que recoge, recomienda la promoción de informes de vigilancia tecnológica y el desarrollo de un modelo de propiedad conjunta de patentes entre el sector público y privado. Además, sugiere la creación de plataformas para promover una oferta unificada de licenciamiento de patentes y proporcionar apoyo en litigios fuera de España.

PwC (PricewaterhouseCoopers)

20 páginas

Perspectivas del Panorama Mundial de las Telecomunicaciones 2023-2027

El informe analiza la situación del sector de las telecomunicaciones y su potencial de crecimiento hasta 2027. Este sector es un facilitador fundamental de la innovación y de la transformación digital. Sin embargo, mientras el volumen de datos que se mueve en el mundo aumenta a gran velocidad, los ingresos que las compañías del sector generan por los servicios más esenciales, como el acceso a Internet, lo hacen de forma moderada. Esto dificulta las grandes inversiones en infraestructuras que deben realizar las empresas de telecomunicaciones, como la expansión del 5G y de las redes de fibra óptica.

Para el estudio se abarcan cinco segmentos de telecomunicaciones en 53 territorios, repartidos entre Norteamérica, Europa Occidental, Europa Central, Oriente Medio y África, Latinoamérica y Asia Pacífico. La agrupación Resto de MENA se trata como un país y comprende Argelia, Bahrein, Jordania, Kuwait, Líbano, Marruecos, Omán y Qatar. Estos territorios representan alrededor del 80% de la población mundial y la suma de todos ellos genera la estimación "Total".

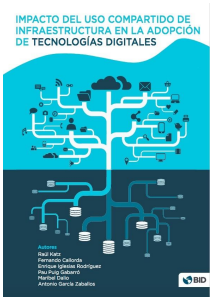
La innovación en el sector de las telecomunicaciones requiere de una inversión significativa de tiempo, dinero, pensamiento estratégico y recursos. Los operadores tendrán que dominar la capacidad de ser una empresa de servicios públicos, construyendo y explotando los activos de red de manera eficiente para poder recuperar el coste del capital y obtener beneficio. Muchas de las áreas que

ofrecen oportunidades estratégicas de crecimiento empujarán a las empresas a interactuar con proveedores, clientes y competidores de nuevas formas. En consecuencia, quienes actúen como facilitadores del ecosistema encontrarán un gran potencial.

Conectividad

Katz, Raúl et al.

120 páginas



Impacto del uso compartido de infraestructura en la adopción de tecnologías digitales

Compartir infraestructura es un mecanismo con un gran potencial para reducir los costos de ampliar el acceso a la banda ancha. La compartición puede ser una herramienta decisiva para permitir el despliegue de redes fijas (fibra óptica hasta el hogar o FTTH) y móviles (5G) de próxima generación. El objetivo de este informe es evaluar el impacto que el uso compartido de infraestructura tiene en el acceso a servicios de banda ancha y proporcionar recomendaciones para la implementación de políticas y regulaciones.

Tomando como punto de partida la lista de países de la región que han implementado políticas y regulaciones de compartición de infraestructura de manera efectiva, se identifican los municipios para los que se han alcanzado y se determina cuándo se implementaron y si se están utilizando para prestar servicios. Paralelamente se llevó a cabo un análisis a nivel regional en el que se evaluó el impacto de las políticas nacionales de compartido de infraestructura y de su regulación frente a una muestra agrupada de datos subnacionales-municipales de penetración, calidad, precio y accesos de nueva generación.

Más allá del beneficio económico que el uso compartido de infraestructura representa para los operadores de telecomunicaciones, este estudio plantea que además se genera un impacto socioeconómico fundamental: el aumento en la adopción de tecnologías digitales. Los gobiernos deben continuar favoreciendo el impulso de la regulación de la compartición de infraestructura, sobre todo en lo referente a tecnologías inalámbricas, dado que estas contribuyen al cierre de la brecha digital rural. Aunque los acuerdos de red compartida son la forma correcta de abordar el reto de la conectividad en zonas rurales, se reconoce que son difíciles de aplicar sin la intervención del gobierno.