SECURE MAGAZINE

INTELIGENCIA ARTIFICIAL

Ocho claves sobre su regulación en la UE

ENTREVISTA

IRATXE IJALBA, CIO DE MUTUALIA

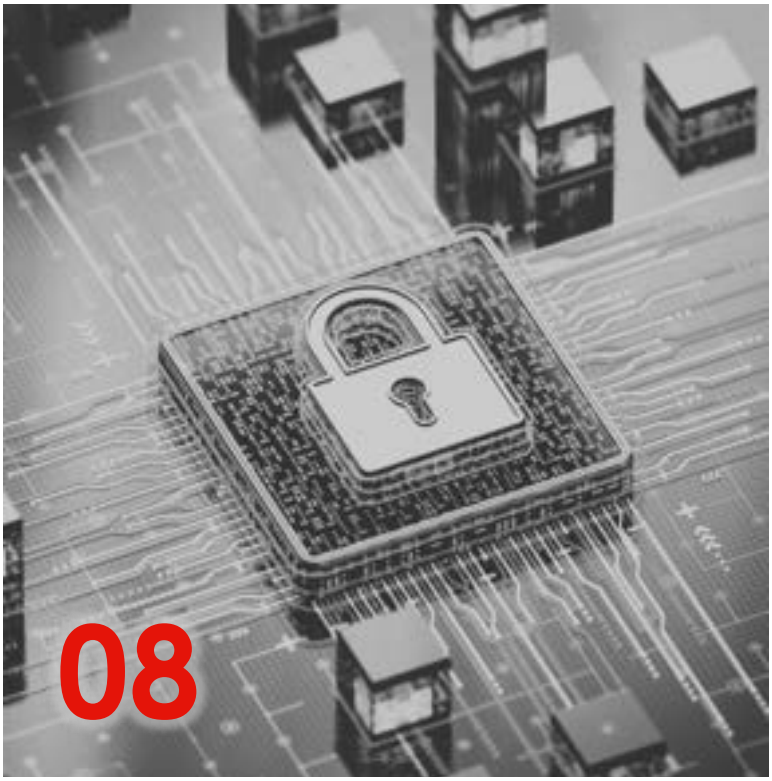
PREVISIONES Y TENDENCIAS

La situación geopolítica y la Inteligencia Artificial generativa serán los mayores desafíos para la ciberseguridad en 2024

ESTUDIO: ESTADO DE LA CIBERSEGURIDAD EN ESPAÑA 2023

SECUREIT by LKS

SUMARIO



INTELIGENCIA ARTIFICIAL

Ocho claves sobre su regulación en la UE

DEEPFAKES

El uso de deepfakes se convierte en una herramienta clave en los conflictos bélicos

Estimados lectores,

En general, la preocupación por la ciberseguridad ha aumentado, especialmente en los últimos años, debido al crecimiento de los ciberataques a nivel global. La inquietud de las organizaciones a este respecto es lógica. El año 2023 ha sido duro desde el punto de vista de los ciberataques, tanto por su incremento en el número como por su sofisticación. En 2024 esta tendencia se mantiene y la situación geopolítica actual y el uso de la Inteligencia Artificial generativa van a jugar un papel clave.

Es innegable que el interés por la IA y sus avances crece de manera exponencial. Europa se encuentra en las etapas finales de la aprobación de un Reglamento sobre IA, un nuevo marco jurídico diseñado para abordar no solo los aspectos técnicos, sino también cuestiones éticas y desafíos de aplicación en diversos sectores. Este Reglamento presta especial atención a la calidad de los datos, la seguridad, la transparencia, la privacidad, la no discriminación y la supervisión humana. El objetivo es garantizar que la IA utilizada en Europa cumpla con los más altos estándares. Nuestra compañera Andrea Fernández, Consultora de Derecho TIC y Protección de Datos, profundiza sobre este tema en su artículo y nos ofrece ocho claves sobre la regulación de la Inteligencia Artificial en la UE.

El uso de herramientas como ChatGPT de OpenAI o Bard de Google son claros ejemplos de la irrupción de la IA generativa en el mercado. En el caso de Chat GPT, las cifras hablan por sí solas: en menos de un año, ha alcanzado los 100 millones de usuarios semanales activos. Escribir correos electrónicos con el tono y el enfoque que pida el usuario; interpretar un texto con diferentes formatos (informe, noticia, etc.); generar textos sobre cualquier tema propuesto en distintos formatos literarios; realizar traducciones a cualquier idioma; comparar productos y realizar recomendaciones; escribir fórmulas de Excel; listar páginas web sobre un tema; elaborar tutoriales… son solo algunas de las múltiples tareas que ChatGPT puede hacer. Pero ¿qué pasa con los datos que introducimos en esta herramienta? Nuestra compañera Natalia Patiño, consultora legal TIC asegura: "*Introducir datos personales en ChatGPT implica perder el control sobre ellos*".

También nuestra entrevistada de esta edición, Iratxe Ijalba, CIO de Mutualia, ha querido destacar la importancia que está teniendo para ellos la irrupción de la Inteligencia Artificial, especialmente desde hace dos años. Nos cuenta que han llevado a cabo proyectos piloto en distintas modalidades de Inteligencia Artificial: "*En IA de análisis de datos masivos hemos puesto en marcha un proyecto con el que ayudamos a los médicos a analizar todas las bajas de contingencia común*". Utilizando la IA en el análisis de imágenes, han desarrollado un proyecto dirigido a analizar imágenes radiológicas y detectar fracturas. Además, utilizan esta tecnología en análisis de voz, con el objetivo de implantar dictados de voz en todas sus aplicaciones y, también, en el análisis de textos, con para llevar a cabo traducciones.

En definitiva, es un hecho que la Inteligencia Artificial generativa ha llegado para quedarse y va a ser uno de los temas más tratados en lo que a ciberseguridad se refiere (tanto por los beneficios en su uso, como por los riesgos que plantea).

No podemos dejar de lado que, de nuevo, una de las principales preocupaciones del sector vuelve a ser el ransomware. Según datos de nuestro Estudio de la Ciberseguridad en España 2023, este malware es el ataque que más inquieta al 93,9% de los profesionales encuestados. No es de extrañar porque, en los últimos años, estos incidentes han aumentado un 200% y más de la mitad de las organizaciones han experimentado, en algún momento, un ataque de ransomware.

Como siempre, contamos con la participación de varios colaboradores a los que agradecemos su dedicación. En este caso, queremos dar las gracias a las compañías Bitdefender, Fortinet, Delinea y Dotlake. Sin sus aportaciones, esta publicación no sería lo mismo.

El equipo de Secure&IT

IRATXE IJALBA

Iratxe Ijalba Izaguirre cuenta con una sólida experiencia y una trayectoria de más de 28 años en el sector tecnológico. Es ingeniera informática y ha consolidado gran parte de su experiencia en la empresa Mutualia, lo que le ha permitido liderar proyectos y adquirir conocimiento en diversos ámbitos como el sanitario, jurídico y de prestaciones económicas, entre otros.

En los últimos 8 años, ha asumido la dirección de Sistemas de Información liderando la transformación digital de la organización y modernizando los servicios. Además, su posterior nombramiento como responsable de Seguridad la ha llevado a fortalecer las medidas de seguridad y a obtener las acreditaciones en seguridad de la información ISO 27001 y Esquema Nacional de Seguridad (ENS).

“A la seguridad de la información hay que dedicarle tiempo y recursos”

Si hablamos de previsiones y tendencias, sectores como la salud, la industria, y los gobiernos son los objetivos principales de los ciberdelincuentes. Además, se espera que aquellos asociados a la situación geopolítica, en los que también está la sanidad, sean blanco de estos ataques debido a su capacidad para poner en riesgo a un país. ¿Cómo se gestiona la seguridad de la información de una organización, sabiendo que es uno de los blancos “favoritos” de los ciberdelincuentes?

Se gestiona con mucha preocupación y a veces durmiendo poco... Pero sí, efectivamente, las empresas que nos dedicamos al área sanitaria somos el blanco de los atacantes, lo llevamos siendo desde hace años y no parece que esto vaya a decaer, sino todo lo contrario. Cada vez vemos más ataques de este tipo, por ejemplo, al Clínic de Barcelona. ¿Y cómo lo afrontas? Estableciendo la seguridad como un pilar básico en la empresa.

Se tiene que entender que la seguridad no es sólo responsabilidad “de informática”, sino que se trata de un riesgo corporativo, que afecta a todos y que debe ser un pilar fundamental en la estrategia empresarial.

La seguridad hay que tenerla en cuenta en todos los proyectos, desde el principio. Hay que ser muy rigurosos en todas las políticas y sistemáticas de seguridad. Y para eso, por lo menos a nosotros, nos han ayudado mucho las certificaciones ISO 27001 y el Esquema Nacional de Seguridad. Estas acreditaciones nos han permitido poner orden y tener muy bien organizados los controles y planes de contingencia. Nos ha llevado tiempo, pero hay que tener en cuenta que a la seguridad hay que dedicarle tiempo y recursos y, desgraciadamente, en las empresas no siempre se hace.

Otro elemento fundamental son los proveedores especializados. Para gestionar la seguridad de la información hay que aliarse con proveedores de garantía, que tengan mucha experiencia y cuenten con gente muy capacitada, e ir de la mano con ellos. Y, por último, y no menos importante, está el usuario. Hay que capacitar y concienciar mucho al usuario del riesgo que conlleva y lo importante que es la seguridad de la información.

Precisamente, has mencionado el ataque al Hospital Clínic de Barcelona, uno de los más destacados de 2023 en nuestro país, al menos por la repercusión mediática que ha tenido. RansomHouse fue el ransomware que le afectó. Este malware ataca al entorno sanitario de todo el mundo. ¿Es el ransomware una de las mayores preocupaciones para ti en lo que a ciberseguridad se refiere?

Pues sí, porque el ransomware es una amenaza muy seria y en constante evolución. Y todos los que nos dedicamos a la seguridad de la información tenemos que ser conscientes de esa gravedad y, sobre todo, de la creciente sofisticación de los ataques que se están lanzando.

En este aspecto, lo que tratamos de hacer es implantar medidas que consigan evitar el ataque o, por lo menos, mitiguen las consecuencias. Entre ellas, contamos con planes de actuación ante ataques de este tipo y con acciones de concienciación.

¿Por qué? Porque la puerta de entrada es el usuario y da igual tecnológicamente todo lo que implantes si luego no conciencias bien al personal y no llevas a cabo acciones para que esté preparado.

Otro de los aspectos que me preocupa mucho, porque estoy notando un incremento, es la suplantación de identidad. De hecho, la semana pasada tuvimos un caso y ya hemos sufrido varios intentos de este tipo. Y, precisamente, los hemos detectado gracias a la concienciación del usuario; han sido ellos mismos los que han reportado esos intentos de suplantación.

En uno de ellos intentaron hacerse pasar, mediante una llamada telefónica, por una empresa proveedora. Su intención era hacer un cambio de la cuenta corriente en la que les pagábamos las facturas. Y en el caso de la semana pasada fue un mail que recibió el área de Recursos Humanos suplantando la identidad de una trabajadora. El correo, por cierto, estaba muy bien elaborado y muy cuidado. Aquí pedían que la nómina se abonase en otra cuenta bancaria.

Has hecho mucho hincapié en el usuario y en su formación y capacitación. Lo cierto es que la mayoría de los ciberataques que sufren las organizaciones se producen desde dentro. Suelen ser errores humanos que no ocurren de forma intencionada, sino por desconocimiento. En este sentido, ¿qué importancia le dais a la concienciación y qué acciones lleváis a cabo?

Le damos muchísima importancia a la concienciación del usuario. Nosotros tenemos personal de muy distinta índole: sanitario, administrativo, de asesoría jurídica, de gestión de prestaciones… Somos más de 600 personas las que trabajamos en Mutualia y contamos con todo tipo de perfiles.

Concienciarlos a todos es difícil, pero, para ello tratamos de llevar a cabo todo tipo de acciones: píldoras informativas, simulaciones de phishing, webinars… Aun así, nos dimos cuenta de que este tipo de actividades se nos quedaban cortas. Por eso, desde hace unos años también hacemos periódicamente hackings éticos internos y externos.

La idea es "engañar" a los usuarios de distintas formas, para ver quién cae en la trampa. Después, divulgamos los resultados y contactamos de forma individual con aquellos que no han superado la prueba para explicárselo personalmente. Es una tarea que nos lleva mucho tiempo, pero, nos está dando muy buenos resultados. En definitiva, además de concienciarles, tratamos de plantearles muchos retos que les ayudan a poner en práctica los conocimientos que adquieren. Siempre intentamos buscar nuevas dinámicas.

En esta línea de acciones, también montamos un escape room de ciberseguridad en nuestras propias instalaciones. Literalmente, metemos a nuestros trabajadores en unas salas y tienen que ir pasando de unas a otras resolviendo unos puzles y retos. El planteamiento es el siguiente: un ciberdelincuente les ha robado la contraseña y ellos deben impedir que borre todos sus datos. Introducimos distintas

"Quiero destacar la importancia que está teniendo para nosotros la irrupción de la Inteligencia Artificial, especialmente desde hace dos años"

dinámicas para que comprendan la importancia de crear contraseñas robustas, contar con múltiple factor de autenticación, etc. Cuando planteamos esta actividad era voluntaria y empezamos con tres grupos de cuatro personas. Pero, gustó tanto, que se corrió la voz y acabaron participando 180 personas de distintas sedes. De hecho, este proyecto lo presentamos a los Quality Innovation Awards en Euskadi y quedamos finalistas.

También estamos trabajando, justo ahora, en el desarrollo de un plan de contingencia ante un ciberataque en el área sanitaria. Nos planteamos escenarios como quedarnos sin sistemas informáticos y analizamos cuáles serían las consecuencias y cómo debemos actuar: qué deben hacer los sanitarios, cuánto podemos esperar antes de tener que trasladar pacientes, si es posible mantener abiertas las urgencias, si se mantienen abiertos los quirófanos… Estamos definiendo un plan de actuación ante ciberataques detallado.

Llevas 28 años en Mutualia, 8 de ellos asumiendo la dirección de Sistemas de Información y liderando la transformación digital y la modernización de los servicios. ¿Cuáles han sido los cambios más importantes en la compañía en este sentido? ¿Qué proyectos destacarías?

Llevamos ya años trabajando con diferentes planes de transformación digital y, siempre, nuestro objetivo en todos ha sido mejorar la experiencia del cliente. En esa línea, hemos montado la oficina virtual para que puedan acceder a los trámites de manera digital.

Pero al margen de la transformación digital, quiero destacar la importancia que está teniendo para nosotros la irrupción de la Inteligencia Artificial, especialmente desde hace dos años. Tanto es así que, en el Comité de Innovación estamos definiendo una estrategia sobre la IA.

Ya hemos llevado a cabo proyectos piloto en distintas modalidades de Inteligencia Artificial. Por ejemplo, en IA de análisis de datos masivos hemos puesto en marcha un proyecto con el que ayudamos a los médicos a analizar todas las bajas de contingencia común. Esta tecnología les orienta en el seguimiento que hay que hacer a los pacientes dependiendo, por ejemplo, de la patología.

mutualia

Mutualia, Mutua colaboradora con la Seguridad Social Nº2, tiene como objeto la gestión de servicios sanitarios, prestaciones económicas y actividades de prevención dirigidas a las empresas asociadas y personas protegidas. Cuenta con una plantilla de más de 600 personas y realiza principalmente su actividad en el País Vasco, donde dispone de 3 hospitales y 15 centros asistenciales que ofrecen cobertura a más de 430.000 personas.

También, utilizamos la IA en el análisis de imágenes. Hemos implantado un proyecto dirigido a analizar imágenes radiológicas y detectar fracturas. Así el médico cuenta, además, con la propuesta de la inteligencia artificial. Y, según nos dicen nuestros radiólogos, lo hace con un alto grado de acierto, aunque siempre es el médico el que hace el diagnóstico.

Por otro lado, estamos utilizando la IA en análisis de voz, con el objetivo de implantar dictados de voz en todas nuestras aplicaciones y, también, en el análisis de textos. Esto último nos sirve para, por ejemplo, poder traducir el informe médico en el momento, de castellano al euskera.

En vuestro ámbito de trabajo, la información tiene un valor incalculable (datos especialmente protegidos, posibles extorsiones, etc.). ¿Crees que, en general, se es consciente de los riesgos de no protegerse y de las consecuencias que puede tener?

En este aspecto, el gran reto que tenemos los que nos dedicamos a la seguridad es conseguir que se comprenda que la responsabilidad, en lo que se refiere a seguridad de la información, es de toda la organización, empezando por la dirección y acabando en el último usuario.

"El gran reto que tenemos los que nos dedicamos a la seguridad es conseguir que se comprenda que la responsabilidad, en lo que se refiere a seguridad de la información, es de toda la organización"

Nosotros, desde nuestra área, podemos implantar todas las medidas técnicas y todos los controles para protegernos, pero las personas también son un riesgo, y concienciar y capacitar al empleado o empleada es fundamental. Afortunadamente, en Mutualia la dirección está totalmente alineada con nosotros.

También hay que gestionar el nivel de seguridad de los proveedores con los que trabajas, porque muchos ciberataques pueden llegar por esta vía, y este riesgo es difícil de controlar porque no depende de nosotros.

Como estamos viendo, sector sanitario se enfrenta a grandes retos en el ámbito de la seguridad de la información y el elevado nivel de riesgo es un factor determinante. ¿Cómo estáis afrontando esos desafíos?

El departamento de TI no crece al mismo ritmo que la seguridad va exigiendo porque los retos a afrontar son cada vez mayores, cada día hay que implantar más medidas de seguridad, más controles. Según pasa el tiempo, la seguridad requiere una mayor supervisión. En nuestro caso, destinamos la mayor parte del presupuesto del departamento a seguridad y a contratar servicios a proveedores.

Nuestro equipo no puede estar formado en todas las tecnologías que continuamente surgen y es fundamental aliarte con proveedores que te den garantías y que tengan mucha experiencia. Y no solo eso… que sean proactivos, que nos mantengan informados, que nos asesoren y que nos ayuden a encontrar lo que mejor se adapte a nuestras necesidades, etc. Son "proveedores estratégicos" y creo que, sin ellos, no podríamos avanzar en mantener la seguridad de la información, sería imposible hacerlo sólo con nuestros recursos.

¿Cuál es la visión de futuro de Mutualia con respecto a la ciberseguridad? ¿En qué proyectos estáis trabajando?

Como bien has dicho, somos empresas que estamos en el punto de mira de los ciberdelincuentes, sobre todo, porque disponemos información sanitaria.

Disponemos de un servicio al que llamo "boinas verdes" que se activa cuando ya te han atacado. Hemos contratado a expertos que actúen cuando ya se han superado las medidas de seguridad y los ciberdelincuentes están dentro. Es un equipo de expertos que "desembarcan" en nuestra empresa en ese momento tan complicado y que nos ayudan a gestionar la situación. Y no hablo solo de la parte técnica, también de la comunicación con los clientes, de la gestión del impacto reputacional, del ámbito legal, de la recogida de pruebas periciales, etc. Este proveedor es Secure&IT. Me da mucha tranquilidad tener contratado su servicio de CSIRT porque sé que tengo a un equipo élite, en el que puedo confiar, con solo llamar por teléfono.

Estamos a primeros de año y es un buen momento para comentar cuáles son tus inquietudes y previsiones. Ya hemos hablado de ransomware, de suplantación de identidad… ¿Qué otros aspectos son los que más te preocupan?

La velocidad a la que va todo. Cada día hay más vulnerabilidades y los ataques son cada vez más sofisticados… estar al día e informado es muy complicado y destinar recursos a conocer las novedades es muy complicado. Por eso, recalco otra vez la importancia de trabajar con empresas especializadas, dejarles te ayuden en esta tarea, que te mantengan informado y te asesoren.

ESTUDIO: ESTADO DE LA CIBERSEGURIDAD EN ESPAÑA 2023

La ciberseguridad es un tema de creciente importancia para las empresas, gobiernos y organizaciones de todo el mundo. El aumento de la digitalización y la conectividad, junto con la sofisticación de las técnicas de ciberataque, han hecho que la seguridad de la información sea una prioridad para todos los actores.

La ciberseguridad tiene un impacto directo en las empresas, ya que puede afectar a su funcionamiento, reputación y rentabilidad. Los ciberataques pueden provocar la pérdida de datos, el robo de información confidencial, el chantaje o el bloqueo de sistemas.
La sofisticación de las técnicas de ciberataque, la escasez de talento cualificado o la falta de concienciación son algunos de los retos a los que se enfrentan los responsables de ciberseguridad. Para hacerles frente, las empresas están invirtiendo en una serie de tecnologías de protección, entre las que se incluyen: seguridad de la nube, de los endpoints, de la red o de los datos.

Con el objetivo de conocer la realidad de la empresa Secure&IT ha realizado una encuesta entre profesionales españoles para conocer qué tipo de amenaza preocupa más a las empresas, qué tipo de tecnologías tiene implantadas en su empresa, cómo impacta la situación geopolítica o cuales son los proyectos que tienen previsto abordar en el corto plazo.

¿Qué tipo de ataque le preocupa más?

Las empresas deben estar preparadas para hacer frente a una amplia gama de ciberamenazas. Pero unas preocupan más que otras. Desde el malware en general al ransomware en particular pasando por el tradicional phishing o la suplantación de identidad, preguntamos qué es lo que más preocupa a los responsables de ciberseguridad.

El ransomware sigue siendo una de las ciberamenazas más graves que enfrentan las empresas. De hecho, es la que más preocupa al 93,9 % de los encuestados, seguido de la exfiltración de datos (52,1 %), el phishing (50,8%) y la suplantación de identidad (42,4 %).

¿Qué tipo de tecnologías tiene implantadas?

En este estudio se plantearon una serie de tecnologías de seguridad básicas que toda empresa debería, en mayor o menor medida, tener implementadas. Los datos recogidos no sorprenden. Firewalls, antivirus, o seguridad en la nube son las tecnologías más implementadas por las compañías españolas. Claro que también son las más tradicionales.

La seguridad del endpoint (79,8 %) es la más adoptada, seguida de medidas específicas de seguridad en la nube (65,8 %).

Por otra parte, años después de contar las bondades de SASE (Secure Access Service Edge) esta tecnología ha sido adoptado por el 12,4% de las empresas, lo que significa que aún le queda mucho recorrido.

Centro de operaciones de seguridad o SOC

Los beneficios de tener un SOC son numerosos, tanto para las empresas como para sus clientes. Son capaces de monitorizar, vigilar, registrar, gestionar y actuar de manera inmediata ante cualquier evento que afecte a la seguridad de la información de las organizaciones.

Entre sus tareas: vigilancia y monitorización 24x7x365; operación, gestión y soporte de sistemas de seguridad TI; gestión de políticas de seguridad y cumplimiento normativo; respuesta rápida ante incidentes de seguridad.

La mayoría de las empresas cuentan con un centro de seguridad, aunque son más (36,5 %) las que tienen acceso a un SOC que no es 24x7, ni cubre todas las tecnologías. Las organizaciones que no tienen un SOC pueden optar por externalizar sus servicios de ciberseguridad a un proveedor de servicios de seguridad (MSSP). Los MSSP ofrecen una amplia gama de servicios de ciberseguridad, como monitoreo de la red, detección de amenazas y respuesta a incidentes.

Gobierno de la ciberseguridad

El Gobierno de la ciberseguridad es el conjunto de principios, políticas, procesos y procedimientos que regulan la gestión de la ciberseguridad en una organización. Su objetivo es garantizar que la organización proteja sus activos de información de las ciberamenazas y es parte esencial de la gestión de la ciberseguridad en cualquier organización.

Preguntados por las acciones que tienen implantadas en las empresas, destaca la amplia adopción de herramientas de concienciación, tanto para la alta dirección (51 %) como de manera más genérica (81,3 %). Asimismo, destaca la gestión de la privacidad y el Derecho TIC (81,3%) y la adopción de políticas formales de seguridad (60,7 %).

Situación geopolítica

La situación geopolítica tiene un impacto significativo en la ciberseguridad de las empresas porque pueden aumentar el riesgo de ciberataques, su sofisticación alcance. De hecho, los ciberataques dirigidos a Ucrania han tenido un impacto en las empresas de otros países, ya que han afectado a la infraestructura crítica y a las cadenas de suministro.

Para el 43,5 por ciento de los encuestados, el conflicto Rusia/Ucrania supone una amenaza general. Y un 36,8 % considera que la actividad de su empresa les pone en el foco de los ciberdelincuentes.

Uso de IA generativa

Es evidente que el uso de IA generativa, como ChatGPT o Bart, ha explotado este año. La IA generativa es una rama de la Inteligencia Artificial que se centra en la creación de contenido, y que tiene el potencial de automatizar tareas, crear nuevos productos y servicios y mejorar la experiencia del cliente.

Más del 10 % de los encuestados no han respondido a esta pregunta. Del total, un 18,7% aseguran controlar el uso y la seguridad de estas herramientas, mientras que un 30,2 % dicen utilizarlas sin tener implantadas medidas específicas, un hecho que está generando enormes riesgos dentro de las empresas.

Inversiones a futuro

Las empresas deben estar preparadas para hacer frente a las ciberamenazas adoptando las tecnologías de seguridad adecuadas. A punto de acabar este 2023, preguntamos a los directivos españoles cuáles son sus planes, qué proyectos tienen pensado afrontar en un futuro cercano.

La seguridad en la nube se ha convertido en el foco de inversión para el próximo año para el 44,2 por ciento de los encuestados, seguida de los servicios de consultoría de cumplimiento y procesos de seguridad (43,5 %). Además, el 35,7 por ciento de las empresas invertirán en segmentación y protección de la red.

OCHO CLAVES SOBRE LA REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL EN LA UE

El interés por los últimos avances en Inteligencia Artificial (IA) crece de manera exponencial. El uso de sistemas como ChatGPT o la automatización de procesos son claros ejemplos. Europa se encuentra en las etapas finales de la aprobación de un Reglamento sobre IA, un nuevo marco jurídico diseñado para abordar no solo los aspectos técnicos, sino también cuestiones éticas y desafíos de aplicación en diversos sectores.

Este Reglamento presta especial atención a la calidad de los datos, la seguridad, la transparencia, la privacidad, la no discriminación y la supervisión humana. El objetivo es garantizar que la IA utilizada en Europa cumpla con los más altos estándares, en consonancia con los valores y derechos fundamentales de la Unión Europea.

Tras el acuerdo al que se llegó el 9 de diciembre de 2023, se ha hecho pública una versión no oficial del texto consolidado sobre la propuesta de Reglamento de Inteligencia Artificial de la UE. No obstante, todavía está pendiente la aprobación del Reglamento por parte del Consejo de la Unión Europea y el Parlamento Europeo, así como su posterior publicación en el Diario Oficial de la Unión Europea.

¿Qué aspectos hay que tener en cuenta sobre el Reglamento de IA?

1. Aplica a **proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA en la Unión**, con independencia de si están establecidos en la UE o en un tercer país. También a los **usuarios de sistemas de IA que se encuentren en la Unión y a los proveedores y usuarios de sistemas de IA que se encuentren en un tercer país**, cuando la información de salida generada por el sistema se utilice en la UE. No se aplicará a los sistemas de IA utilizados exclusivamente con fines militares; ni cuando las autoridades públicas utilicen estos sistemas en el marco de acuerdos internacionales, con fines de cumplimento legal y cooperación judicial con la Unión o con los Estados miembros.

2. El texto incorpora nuevas definiciones de términos relevantes como: "modelo fundacional" (a los que pertenecen ChatGPT, Bard o LLaMA), "sistema de inteligencia artificial", "riesgo significativo", "identificación biométrica", ultrafalsificación" (deep fake) o "espacio controlado de pruebas" (sandbox), entre otros.

3. Entre las novedades introducidas en la última versión, cabe destacar la **regulación específica y completa sobre los modelos fundacionales** (eficiencia energética y medioambiental, gestión de calidad y riesgos, inscripción en un registro europeo…) y los requisitos específicos que se prevén para los sistemas de IA generativa, como la obligación de revelar que los contenidos han sido generados por IA, diseñar sistemas que impidan la generación de contenidos ilegales, etc.

4. La nueva normativa **establece una serie de obligaciones en función del nivel riesgo de la IA**, que se evaluará en función del riesgo que el uso de la tecnología puede suponer para la seguridad, salud y derechos fundamentales de una persona. En concreto, los sistemas de IA se clasifican en cuatro niveles de riesgo: inaceptable, alto, limitado y mínimo.

5. **Los sistemas con un riesgo inaceptable son aquellos que se consideran una amenaza para las personas y serán prohibidos**. Algunos ejemplos serían: la manipulación cognitiva, la puntuación social o los sistemas de identificación biométrica en tiempo real y a distancia. Pero, existen algunas excepciones a esta calificación como, por ejemplo, los sistemas de identificación biométrica a distancia "a posteriori", en los que la identificación se produce tras un retraso significativo. Se permitirán para perseguir delitos graves y sólo cuando haya previa aprobación judicial.

6. En cuanto a los **sistemas de IA de riesgo alto**, en la última versión, se propone la ampliación de la clasificación para incluir los daños a la salud, la seguridad, los derechos fundamentales o el medio ambiente. Estos sistemas deberán cumplir con una serie de obligaciones para **garantizar que aquellos que se utilicen en la Unión Europea sean seguros y respeten tanto los derechos fundamentales de las personas como los valores y garantías de la Unión.** Algunas de las obligaciones previstas son: realizar evaluaciones de riesgo durante todo el ciclo de vida, ser aprobados mediante procedimientos adecuados antes de su uso, ser supervisados por personas físicas, etc.

7. **Los sistemas de IA de riesgo limitado deben ser transparentes y permitir a los usuarios tomar decisiones informadas.** Eso significa que los usuarios deben estar informados de que están interactuando con una IA, salvo en aquellas situaciones en las que resulte evidente. Esto incluye los sistemas de IA que generan o manipulan contenidos de imagen, audio o vídeo (por ejemplo, *deepfakes*).

8. **El régimen sancionador también ha sufrido cambios relevantes en la última versión** (en lugar de tres niveles de sanciones, ahora habrá cuatro). **Las multas más altas podrán ser de hasta 30 millones de euros o, si es una empresa, hasta el 6% del volumen de negocio total anual global del ejercicio financiero anterior.** Además, el texto propone que los proveedores, distribuidores, importadores o cualquier otro tercero, no puedan repartirse la carga de las sanciones y costas procesales, a través de cláusulas contractuales.

Avances en el ámbito nacional

El pasado 10 de noviembre de 2023 entró en vigor el Real Decreto 817/2023, cuyo objetivo es la creación de un entorno de pruebas controlado (*Sandbox*) para determinar cómo implementar los requisitos aplicables a los sistemas de IA de riesgo alto, según lo previsto en la propuesta de Reglamento.

Además, en agosto, el Consejo de Ministros aprobó el estatuto de la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA). Esto refleja el compromiso de España con la transformación digital, en línea con la Agenda Digital 2026 y la Estrategia Nacional de Inteligencia Artificial (ENIA), que busca un desarrollo inclusivo, sostenible y centrado en la ciudadanía. La AESIA, adscrita al Ministerio de Asuntos Económicos y Transformación Digital, **convierte a España en el primer país europeo con una entidad de supervisión de IA, anticipándose a la entrada en vigor del Reglamento Europeo de Inteligencia Artificial**, que requerirá a los Estados miembros designar una autoridad de supervisión de IA.

Andrea Fernández, Consultora de Derecho TIC y Protección de Datos en Secure&IT

CHAT GPT VS. DATOS PERSONALES

"Introducir datos personales en ChatGPT implica perder el control sobre ellos"

- **La información que los usuarios introducen en ChatGPT queda registrada y puede ser reutilizada para seguir "entrenando" a la aplicación.**
- **Así, al introducir datos personales, se pierde el control sobre esa información.**
- **Los expertos advierten que esta herramienta facilita o complementa la labor humana, pero no la sustituye.**

La inteligencia artificial generativa ha ganado importancia, especialmente, en el último año. Herramientas como ChatGPT de OpenAI o Bard de Google han irrumpido en el mercado y lo han hecho para quedarse. En el caso de Chat GPT, las cifras hablan por sí solas: **en menos de un año, ha alcanzado los 100 millones de usuarios semanales activos.**

Escribir correos electrónicos con el tono y el enfoque que pida el usuario; interpretar un texto con diferentes formatos (informe, noticia, etc.); generar textos sobre cualquier tema propuesto en distintos formatos literarios; realizar traducciones a cualquier idioma; comparar productos y realizar recomendaciones; escribir fórmulas de Excel, listar páginas web sobre un tema, elaborar tutoriales… son solo algunas de las múltiples tareas que esta potente herramienta, lanzada al público en 2022 por OpenAI de forma gratuita, puede hacer.

Para utilizar correctamente ChatGPT, se debe partir de la base de que se trata de una

herramienta que facilita o complementa la labor humana, pero no la sustituye. No es una herramienta infalible, por lo que su uso debería verificarse siempre y, además, no razona, sino que sus respuestas están vinculadas a los datos con los que ha sido previamente entrenada. En este sentido, Natalia Patiño, consultora legal TIC de **Secure&IT,** apunta: "*Hay habilidades humanas y emociones que no están al alcance de la IA, al menos de momento. Por eso, es importante mantener el equilibrio entre la automatización del Chat GPT y el trabajo humano*".

El modelo ChatGPT funciona utilizando una técnica de aprendizaje automático conocida como **"aprendizaje por transferencia"**, un entrenamiento en base a un conjunto de datos a gran escala cuyo resultado sirve, a su vez, para continuar entrenando al modelo de aprendizaje. Esto implica el uso de una cantidad ingente de datos, que es lo que hace posible que las respuestas ofrecidas por la herramienta sean completas.

Cuando el usuario introduce una petición e interactúa con ChatGPT, el modelo ajusta su respuesta en función de la retroalimentación del usuario y los datos contextuales que aporta. En consecuencia, la herramienta genera respuestas cada vez más precisas y similares a la forma humana de expresión.

Pero, para el "entrenamiento" de esta herramienta se utilizan **todos los datos** que los usuarios introducen en ella. Por eso, es importante tener presente que esa información queda registrada y puede ser reutilizada; también los datos personales.

Natalia Patiño: "***La introducción de datos personales y, en general, de información confidencial, implica perder el control sobre esos datos e informaciones***. *Y, en el caso de los datos personales, esta situación podría suponer un incumplimiento grave de la normativa vigente. En este sentido, es importante puntualizar que un dato personal es cualquier información referida a una persona física, identificada o identificable. Por tanto, no solo habrá que evitar introducir en el ChatGPT datos directamente identificables, sino aquellos que, de forma indirecta, puedan llevar a la identificación*.

Por este motivo, es muy importante no incluir este tipo de información en las consultas, sobre todo, teniendo en cuenta que actualmente los chats basados en IA son, en general, muy opacos".

La calidad de la respuesta del ChatGPT viene determinada por la calidad del "prompt" o entrada, es decir, el contexto aportado por el propio usuario al realizar la petición. El uso de entradas adecuadas y bien formuladas es fundamental para obtener resultados satisfactorios de ChatGPT, de modo que una buena entrada debe ser clara y, preferiblemente, incluir palabras clave que ayuden a construir la respuesta. Pero, hay que tener presente que se pueden generar respuestas incorrectas, respuestas incompletas o inexactas e incluso "alucinaciones" (es decir, respuestas perfectamente convincentes, pero falsas o inventadas).

Además, las respuestas generadas puedan estar condicionadas por diferentes tipos de sesgos: "*Un ejemplo es el sesgo de retroalimentación que se produce cuando los sistemas de inteligencia artificial aprenden a través de la retroalimentación de los usuarios, lo que puede perpetuar los prejuicios y los estereotipos existentes. Por ejemplo, el edadismo y la discriminación por género pueden continuar lastrando la contratación de personas mayores de cuarenta y cinco años o señalar sólo perfiles de hombres para ocupar puestos directivos si el modelo de IA para la selección de candidatos aprende de información previa ya sesgada*", explica Patiño.

El incremento en el uso de estas tecnologías planteó la necesidad de regular el uso de la Inteligencia Artificial en la Unión Europea. De hecho, **Europa se encuentra en las etapas finales de la aprobación de un Reglamento sobre IA**, un nuevo marco jurídico diseñado para abordar no solo los aspectos técnicos, sino también las **cuestiones éticas** y los múltiples desafíos de aplicación que plantea en diversos sectores.

SECURE&IT

OBTIENE LAS CERTIFICACIONES

ISO 14001 E ISO20000-1

Elevamos nuestro compromiso con la sostenibilidad y la gestión de servicios de TI.

En **Secure&IT** estamos muy contentos de anunciar que hemos obtenido la certificación ISO 14001 e ISO 20000-1, lo que implica nuestro compromiso con la sostenibilidad ambiental y la excelencia en la gestión de servicios de Tecnologías de la Información. Estas certificaciones, otorgadas por la Organización Internacional de Normalización (ISO), reconocen el cumplimiento de estándares internacionales rigurosos.

Certificación ISO 14001: Sistemas de Gestión Ambiental

La certificación ISO 14001 refleja el compromiso de **Secure&IT** con la protección y el respeto del medio ambiente, así como con la gestión sostenible de los recursos. El certificado de Sistema de Gestión Medioambiental ISO reconoce las buenas prácticas medioambientales de nuestra organización, así como nuestra intención de seguir mejorando la prevención del cambio climático, garantizando los más altos estándares de calidad.

Reafirmamos así nuestro objetivo de trabajar por nuestro entorno y por el planeta.

Certificación ISO 20000-1: Gestión de Servicios de TI

También hemos certificado la arquitectura, sistemas y procesos de nuestro servicio de seguridad gestionada, **Secure&View©**, llevados a cabo en nuestros centros de operaciones de seguridad SOC-CERT (en Madrid y Vitoria), conforme a la norma ISO/IEC 20000-1:2018.

La Norma ISO 20000-1 certifica que la metodología y prácticas que implementamos en la gestión de la información están correctamente definidas, lo que nos permite una integración de los procesos con mejora continua en la calidad de los servicios, tanto de forma interna como para los clientes. Reforzando, una vez más, nuestro compromiso con la excelencia y la calidad.

Estas certificaciones se suman a las que ya teníamos: ISO 27001, ISO 9001 y Esquema Nacional de Seguridad (nivel alto), evidenciando nuestra cultura de empresa en la mejora continua del Sistema de Gestión Integrado de Seguridad.

CIBERSEGURIDAD INDUSTRIAL

SECUREIT
by LKS Next

LA SITUACIÓ GEOPOLÍTICA Y LA IA GENERTIVA SERÁN LOS MAYORES DESAF

PARA LA CIBERSEGURIDAD EN 2024

- **La situación geopolítica y el uso de la IA generativa serán clave en el incremento de los ciberataques.**
- **Sectores como banca, aseguradoras, administraciones públicas, sanidad, fabricantes de armamento, infraestructuras críticas o líneas aéreas serán el blanco de los ciberataques.**

La preocupación por la ciberseguridad ha aumentado, especialmente, en los últimos años, debido al crecimiento de los ciberataques a nivel global.

De hecho, en el año 2023 los ciberataques se incrementaron hasta alcanzar un valor global cercano al 1,5% del PIB mundial, superando la suma de los otros tres grandes "motores" económicos en el mundo del crimen: el tráfico ilegal de armas, la trata de seres humanos y el mercado ilegal de drogas. Precisamente, en 2024 se espera de nuevo un aumento en el número y la sofisticación de los ataques y, en este sentido, **la situación geopolítica actual y el uso de la inteligencia artificial generativa van a jugar un papel clave**.

Más allá del incremento numérico, **lo más preocupante es la evolución de estos ciberataques**. Según Francisco Valencia, director general de **Secure&IT**, "*ya no estamos hablando de ataques que vienen del extranjero y se lanzan de una manera arbitraria y sin criterio, sino que están altamente localizados, con un conocimiento profundo de las políticas empresariales y de las operaciones internas de las organizaciones a las que se ataca*".

Evolución de los ataques: la influencia de la situación geopolítica y la IA generativa

Conflictos como las guerras entre Ucrania y Rusia o Israel y Palestina, así como la tensión geopolítica global, están influyendo notablemente en la generación y dirección de los ciberataques.

Con el conflicto armado entre Rusia y Ucrania, empezó también una "batalla" en el ciberespacio. Esto hizo que las armas asociadas al mundo de la ciberguerra fueran muy accesibles en la Dark y Deep Web, lo que ha generado una preocupante acumulación de "armamento" que puede usarse para atacar a cualquier empresa y administración del mundo. Además, la evolución de la tecnología, unida al instinto de supervivencia, ha provocado que muchas personas opten por el cibercrimen como vía para obtener solvencia económica, lo que, lógicamente, está influyendo en el incremento de ciberataques.

Además, los grandes operadores de ciberdelincuencia hacen que "el trabajo" sea más fácil para sus "afiliados", lo que ha llevado a un aumento tanto en la cantidad como en la diversidad de atacantes en todos los niveles: desde el crimen organizado, hasta individuos autónomos que utilizan las nuevas tecnologías para lanzar ataques y, en algunos casos, obtener ingresos. Una situación que está generando una amenaza sin precedentes.

La utilización de la inteligencia artificial para perpetrar ataques también va a ser significati-

FÍOS

va. Los ciberdelincuentes emplearán la IA generativa (una rama de inteligencia artificial que puede crear contenido original a partir de datos existentes) para suplantación de identidad y, también, para elaboración de malware, altamente sofisticado, capaz de eludir las defensas de los sistemas de seguridad existentes. Se prevé que la IA generativa sea empleada para engañar en diversas situaciones, desde la creación de interacciones en vídeo hasta la redacción de correos electrónicos perfectamente adaptados al idioma y estilo de escritura de los usuarios. Serán, por tanto, ataques más sofisticados y difíciles de detectar que, incluso, pueden superar a los métodos tradicionales como el phishing o el fraude al CEO.

Para luchar contra esta amenaza emergente, Francisco Valencia propone la integración de la inteligencia artificial no generativa: "*Esta modalidad de IA se enfocaría en detectar diferencias y marcadores que distingan entre contenido auténtico y generado artificialmente*".

En el caso del ransomware, que ya había evolucionado hacia una triple extorsión (al robo de datos y la exigencia de una recompensa económica a la empresa afectada, se sumó el chantaje a sus clientes), se podría alcanzar el cuádruple chantaje con la reciente incorporación del VIP, una figura autorizada para tomar decisiones, como el pago de rescates dentro de organizaciones, y a la que se van a dirigir muchos de los ataques.

Además, se prevé un aumento en los ataques de robo de credenciales en entornos Cloud, que va a impactar, especialmente, en sectores como la banca, las aseguradoras o los proveedores de servicios. En este sentido, Valencia apunta: "*La falta de medidas como la autenticación de doble factor puede facilitar mucho estos ataques*".

Sectores más vulnerables

Ninguna organización, independientemente de su tamaño o del sector al que pertenezca, está libre de ser atacada. Pero, sectores como la sanidad, la industria y la administración pública son de claro interés para los delincuentes, debido a su mayor disposición a pagar rescates. Además, se espera que los sectores relacionados con la situación geopolítica (banca, aseguradoras, administraciones públicas, sanidad, fabricantes de armamento, infraestructuras críticas o líneas aéreas) sean blanco de los ataques, debido a su capacidad para poner en riesgo a un país.

PREDICC
PARA 20
PANOR

En este articulo exploramos nuestras predicciones sobre IA y ransomware: la reducción de la barrera de acceso inicial para los atacantes. Esto dará como resultado un aumento en los endpoints comprometidos y hablaremos sobre las implicaciones desde la perspectiva de la superficie de ataque.

La continua evolución de las amenazas a los endpoints

Los endpoints siguen siendo uno de los objetivos más destacados para los ciberdelincuentes en un ciberataque y son el vector de entrada inicial más común. Como resultado, los ataques dirigidos al endpoint se intensificarán y hay varias áreas clave donde esto se pondrá de manifiesto:

- **Living Off The Land**. Los ciberdelincuentes quieren evitar ser detectados una vez que han comprometido un sistema. Una de las formas en que perpetúan sus ataques sin generar demasiadas alarmas es empleando técnicas de tipo LOLBin (Living Off the Land). Este tipo de ataque utiliza binarios ya existentes en el sistema (programas y software que ya están instalados en un sistema) para llevar a cabo un ataque, en lugar de depender de la ejecución de software malicioso por separado, que puede ser fácilmente identificado incluso por software de seguridad heredado. Hemos visto principalmente este tipo de explotación de recursos en dispositivos Windows, donde el atacante utiliza PowerShell, WMI, Programador de tareas y otros servicios integrados en el sistema operativo para ejecutar o activar scripts maliciosos en el endpoint, pero cada vez más, los ciberdelincuentes comprometen los archivos binarios. También comprometen binarios en dispositivos Linux y macOS. Estas tácticas de ataque han demostrado ser efectivas y exitosas, y seguiremos viendo un aumento de ataques que utilizan estas tácticas en 2024. Esto subraya la importancia de emplear tecnología EDR/XDR (endpoint detection and response and extended detection and response) y servicios MDR (managed detection and response) que pueda correlacionar eventos en toda la red y ayude a identificar el comportamiento asociado con un incidente de seguridad que puede involucrar técnicas tipo LOLbin.
- **Traiga su propio driver vulnerable (BYOVD).** Los ciberdelincuentes están explotando cada vez más los drivers vulnerables para obtener acceso privilegiado a los sistemas, y luego lo usan para eludir las soluciones de seguridad en los endpoints, implantar y activar ransomware, moverse lateralmente a través de la red de una organización y filtrar datos valiosos. Al igual que LOLBins, explotar los drivers existentes en un sistema ayuda al atacante a pasar desapercibido por las soluciones de seguridad tradicionales y, a menudo, a eludir la protección de firma digital de Microsoft. Vimos, por ejemplo, al grupo de hackers Lazarus, con sede en Corea del Norte , explotar drivers pertenecientes a software de autenticación para comprometer la seguridad de una organización a la que apuntaban. En 2024 es muy probable que veamos un aumento de los ataques que utilizan las vulnerabilidades de los drivers para comprometer los endpoints.
- **Heterogeneidad en Windows.** Microsoft presentó el subsistema de Windows para Android a los expertos en octubre de 2021 y permitió las secuencias de comandos Python en Microsoft Office en 2023. Estas nuevas características permiten que Windows ejecute aplicaciones no nativas en Windows. Por sí solas, estas adiciones introducen un conjunto completamente nuevo de código y vulnerabilidades potenciales en Windows. Cada nuevo software aumenta la superficie de ataque, que es el número total de puntos o "vectores de ataque" que atacante puede intentar explotar. Al tener como objetivo los sistemas Windows y Android, los atacantes tienen más oportunidades de encontrar debilidades. Para agravar el problema, la utilización del subsistema Android en Windows a menudo implica la descarga de aplicaciones. Además, a los ciberdelincuentes les encanta infectar APK de terceros (ejecutables de Android) con malware. El soporte incluido de secuencias de comandos Python abre las puertas a ataques adicionales dirigidos a usuarios que

CIONES EN CIBERSEGURIDAD 024: CAMBIOS EN EL RAMA DE ATAQUES

ejecutan Microsoft Office. Ya hemos comenzado a ver algunos paquetes de software malicioso que explotan el índice de paquetes de Python (PyPI). Para protegerse contra estas amenazas, los usuarios deben abstenerse de descargar aplicaciones en sistemas Android y cumplir con la instalación de software que esté disponible solo a través de Google Play Store o Company Portal.

- **Bypass de EDR.** Los ciberdelincuentes han desarrollado una serie de técnicas para evitar la detección de EDR. Logran esto modificando el código en la memoria, incapacitando los enlaces del modo de usuario, deshabilitando por completo el servicio Antimalware Scan Interface (AMSI). AMSI permite que las soluciones de seguridad escaneen el código que se ejecuta en los sistemas Windows en busca de amenazas, utilizando Kernel Exploits y manipulando los registros de auditoría utilizados por soluciones EDR. A medida que la adopción de EDR crezca en popularidad, también lo hará la adopción de técnicas de elusión de EDR por parte de los ciberdelincuentes. Las organizaciones deben implementar tecnología de defensa en profundidad que utilice múltiples capas de seguridad que se complementen y se superpongan entre sí. Esto incluye capacidades de protección de procesos que fortalecen el endpoint contra la manipulación de DLL y combina seguridad en modo usuario y modo kernel junto con heurística para identificar e impedir técnicas de omisión de EDR.

Amenazas crecientes en la nube.

Las cargas de trabajo y la infraestructura de la nube se han vuelto fundamentales para la operativa de las organizaciones en todo el mundo. Esta dependencia crítica de los entornos de nube conlleva un mayor riesgo. En 2023 se produjo un aumento de los ciberataques dirigidos a arquitecturas nativas de la nube, como las plataformas de orquestación de contenedores. Los ciberdelincuentes continuaron explotando vulnerabilidades en servicios ampliamente utilizados y abusaron de las configuraciones erróneas en cargas de trabajo en la nube. Comprender estas amenazas emergentes es crucial para que las organizaciones fortalezcan sus defensas y garanticen que su transición a la nube en 2024 siga siendo segura y resiliente.

- **Azure y Azure AD bajo asedio.** el año pasado se produjo un aumento en la disponibilidad de herramientas de código abierto disponibles, que son particularmente útiles para administrar, monitorizar y proteger cargas de trabajo en la nube pública, particularmente para Microsoft Azure®. Anticipamos que los ciberdelincuentes buscarán secuestrar muchas de estas herramientas para obtener acceso no autorizado a cargas de trabajo en la nube. Al "conectarse" a las interfaces de programación de aplicaciones (API) utilizadas por estas herramientas, o explotar controladores vulnerables, los ciberdelincuentes podrán exponer la seguridad de los entornos de nube con los que interactúan estas herramientas. Con esa exposición, los ciberdelincuentes podrán acceder a Azure AD y crear cuentas con acceso elevado que les permitirá debilitar las defensas en las organizaciones (por ejemplo, deshabilitar la autenticación multifactor) o manipular infraestructuras de administración existentes como Intune™ para ejecutar malware en los hosts. Las soluciones de detección y respuesta extendidas (XDR) que ofrecen protección para cargas de trabajo en la nube y plataformas de identidad pueden ayudar a descubrir comportamientos asociados con el uso indebido de estas herramientas.

- **El auge de los gusanos nativos de la nube.** La mayor adopción de DevOps en la nube y la creciente popularidad de plataformas de contenedores como Kubernetes, OpenShift o Docker han ampliado la superficie de ataque potencial para los ciberdelincuentes, que van a seguir aprovechando las configuraciones erróneas en estos entornos de nube para obtener acceso a las organizaciones. Se espera un aumento en los gusanos nativos de la nube que hacen proliferar el malware. Al explotar la naturaleza misma de estas plataformas entrelazadas, estos gusanos tienen el potencial de causar mucho daño en muy poco tiempo. Las organizaciones con presencia en la nube deben contratar servicios profesionales de gestión de seguridad para identificar y resolver estas configuraciones.

Superficies de ataque emergentes: las nuevas fronteras.

Los endpoints y las cargas de trabajo en la nube seguirán siendo los principales objetivos de los ciberataques en 2024. Pero, además, los ciberdelincuentes van a ampliar la forma en que atacan estos activos.

- **Apuntando a aplicaciones de comunicación.** En 2024 veremos un aumento de ataques que utilizan aplicaciones de comunicación como Slack® y Teams™, convirtiendo estas plataformas en campos de batalla muy parecidos a territorios disputando nuevas tierras. Por su naturaleza, estas herramientas seguirán siendo un vector de ataque muy importante. Las organizaciones deben emplear seguridad de múltiples capas en sus endpoints que incluya una protección de red efectiva, que pueda interceptar la transferencia de archivos maliciosos a través de estas plataformas.
- **Interacciones cambiantes de los usuarios y dispositivos no administrados.** El 70% de los incidentes que el equipo de Bitdefender MDR investigó en 2023 se originaron en dispositivos no administrados, lo que deja clara la efectividad de apuntar a estos equipos. Las empresas deben permanecer alerta contra los ataques de phishing que emplean códigos QR, o aquellos que involucran al actor de la amenaza utilizando números de teléfono o cuentas secuestradas para iniciar chats que conducen a la exposición de datos confidenciales del usuario. Las organizaciones deben emplear políticas rígidas, en este sentido, para prevenir las amenazas que se originan por el uso de dispositivos no administrados, y se debe alentar a los empleados a instalar seguridad móvil sólida en sus dispositivos con capacidad para detectar mensajes maliciosos.
- **Mayor uso de marcos y lenguajes de programación independientes de la plataforma por parte de los ciberdelincuentes.** El año pasado se intensificaron los ataques escritos en lenguajes de programación independientes como Rust, Go y Swift. Además de utilizar estos lenguajes independientes de la plataforma, también hemos visto un mayor uso de marcos de código abierto como Havok y Sliver, empleados en conexiones de comando y control por parte de grupos cibercriminales. Los beneficios para los atacantes consisten en poder comprometer todos y cada uno de los sistemas operativos.
- **Explotación de vulnerabilidades en las CPU.** En 2023 se descubrieron varias vulnerabilidades importantes en las CPU, como el problema de prefijo redundante de Intel y el muestreo de datos de recopilación, el inicio de AMD y ZenBleed. Estos fallos pueden permitir a los ciberdelincuentes filtrar información confidencial a través de límites de privilegios o, incluso, llevar a cabo ataques DoS en sistemas comprometidos. Debido a su naturaleza, estos errores son difíciles de resolver y, a menudo, requieren una actualización del sistema operativo o del microcódigo.
- **Conflictos globales que conducen a un aumento del hacktivismo.** La ciberguerra sigue siendo una herramienta eficaz para lograr objetivos políticos, sociales o nacionales. Estos objetivos pueden consistir, por ejemplo, en alterar una infraestructura crítica, robar datos confidenciales o influir en la opinión pública. En los últimos dos años se ha visto un aumento significativo de los ataques contra las infraestructuras críticas, perpetuados por grupos sospechosos de estar patrocinados por algunos Estados. Se espera que, en 2024, aumenten estos ataques en frecuencia y alcance.

Conclusión

Este año el panorama de la ciberguerra está experimentando un cambio sísmico, impulsado por la integración acelerada de herramientas de Inteligencia Artificial (IA), un mayor enfoque en los entornos de nube y una superficie de ataque en expansión, provocada por plataformas y prácticas laborales heterogéneas. Está claro que, si bien los desafíos son muchos, también hay motivos sustanciales para el optimismo. Los mismos avances tecnológicos que han envalentonado a los ciberatacantes también están dotando a los defensores de herramientas más sólidas y sofisticadas. Los gobiernos, las organizaciones y los expertos en ciberseguridad colaboran cada vez más, compartiendo conocimientos y recursos para adelantarse a las amenazas. Este esfuerzo colectivo es un testimonio de la resiliencia y adaptabilidad de la comunidad de ciberseguridad.

Las organizaciones que se centran en la prevención son las que tienen más probabilidades de afrontar con éxito estos tiempos turbulentos. De cara a 2024, las organizaciones deberían adoptar un plan que incluya capacidades efectivas de prevención, protección, detección y respuesta para formar no solo componentes de una estrategia de ciberseguridad saludable, sino los mismos pilares sobre los que se construye su resiliencia.

Richard De La Torre, Technical Marketing Manager, de Bitdefender

Bitdefender®

BUILT FOR RESILIENCE

TU CENTRO AVANZADO DE FORMACIÓN EN CIBERSEGURIDAD

SECURE ACADEMY

www.secureacademy.es

SECUREIT by LKS

CIBERATAQUES A NUESTRO SISTE
¿ESTAMOS PREPARADOS?

Cada vez que un centro sanitario, hospital, ambulatorio o clínica es ciberatacado todos corremos un grave peligro. No sólo por lo evidente que resulta que un recurso fundamental para la sociedad como es la sanidad se vea atacado, con las consecuencias para la vida y la salud de las personas que eso conlleva, sino también para algo que, en ocasiones, se olvida: la compraventa de nuestros datos personales, identidades e historiales clínicos y el uso fraudulento que hacen de ellos.

Barcelona acaba de vivir una de estas situaciones. El Hospital Clínic sufrió recientemente un ciberataque de gran magnitud que paralizó sus sistemas, obligándolo a anular más de 3.000 visitas médicas debido a un ataque de ransomware, que afectó no sólo a las tres sedes del hospital, sino también a tres centros de atención primaria de Barcelona. Los ciberdelincuentes pidieron un rescate para recuperar los datos robados, por un valor de más de 4 millones de dólares, pero el Govern se negó a negociar con ellos. Desafortunadamente, no es un caso aislado en España. Según un estudio realizado por Proofpoint y el Instituto Ponemon, el 89% de las organizaciones sanitarias ha sufrido una media de 43 ataques en los últimos 12 meses, casi uno por semana. Ante estos alarmantes datos, debemos preguntarnos ¿estamos preparados para proteger nuestro sistema sanitario?

Hay un elemento clave en este incremento de ataques al sistema de salud: **el acelerado proceso de digitalización que está experimentando la sanidad**. Esto ha provocado que, por un lado, exista un perímetro de seguridad que cubrir cada vez más amplio, unos dispositivos conectados, en muchos casos obsoletos, y una falta de concienciación en ciberseguridad de los profesionales sanitarios, que dan lugar a errores que pueden comprometer la seguridad del sistema. Ante esta situación, los departamentos de IT de los centros sanitarios están sometidos a una enorme presión y necesitan prepararse frente a una serie de amenazas muy peligrosas que aún están por venir.

Principales amenazas del sistema sanitario

La mayoría de los ciberdelincuentes consiguen entrar comprometiendo credenciales para tener acceso a cuentas con privilegios del personal sanitario, para acceder a datos críticos, como historiales médicos de pacientes, o bien para tomar el control de dispositivos médicos conectados, para de esta forma extorsionar y pedir rescates económicos o conseguir información que luego poder vender. Pero ¿qué tipo de amenazas son las más frecuentes?

Pensar que los ciberdelincuentes sólo atacan a los empleados con acceso a datos críticos sería un gran error. La mayoría de los trabajadores utilizan cuentas con privilegios de administrador en sus propios ordenadores, todo lo que necesitan los atacantes es comprometer este tipo de cuentas y obtener acceso al sistema. Los ciberdelincuentes suelen utilizar ataques de phishing o contraseñas comprometidas con el objetivo de infiltrarse en la red de un centro y moverse lateralmente de un sistema a otro, hasta obtener acceso a los recursos críticos. Una vez conseguido el acceso, los recursos se cifran y se exige el pago de un rescate para liberarlos. Otra de las principales amenazas para los sistemas sanitarios es contar con aplicaciones en la nube poco seguras. Y es que, debido a la necesidad de dar acceso en remoto a los trabajadores, la migración de datos sanitarios de pacientes a entornos híbridos y multicloud los convierte en un objetivo muy atractivo. En este mismo sentido, con el aumento del número de trabajadores sanitarios a distancia, también se han incrementado los ataques a través de conexiones remotas poco seguras. Y en este contexto, la mayoría de los ataques se producen por cuentas de usuarios y sesiones remotas que no están suficientemente protegidas.

Otro problema que se ha agravado en los últimos años es el uso de los llamados bots maliciosos, esto

es, de redes de bots que se utilizan expresamente para escanear sitios web de la sanidad en busca de vulnerabilidades e iniciar patrones de ataque. Las rutinas de daño más habituales incluyen la recopilación de datos de sitios web, el envío de spam a través de los equipos infectados o la instalación de puertas traseras en los sistemas para obtener después acceso a la red. De hecho, según estimaciones de los expertos, el tráfico de bots maliciosos se ha cuadriplicado de 2020 a 2021.

Medidas que pueden evitar un ciberataque

Debido a que los ciberataques se centran en las identidades humanas y de máquinas con privilegios, una de las prioridades de los departamentos de seguridad de las organizaciones sanitarias debe ser la integración de soluciones de gestión de acceso privilegiado para poder gestionar eficazmente las contraseñas de una organización, para mejorar la seguridad y la facilidad de uso. De este modo, se pueden detener muchos ataques de ransomware antes de que causen daños. Y para poder aplicar una solución adecuada que garantice la seguridad y proteja a los centros sanitarios, conviene tener en cuenta varios aspectos:

- **Revisar las cuentas con privilegios** en la organización: desde las cuentas de DevOps hasta los usuarios de negocio con privilegios y las cuentas de máquina con amplios permisos.
- **Otorgar permisos según el principio de mínimo privilegio.** Esto significa que los usuarios autenticados solo deben obtener los permisos mínimos que necesitan para realizar sus tareas. De esta forma, se limitan los posibles daños en caso de que un atacante se haga con el control de una cuenta.
- **Implementar una autenticación multifactor sólida.** Esto es especialmente importante para proteger recursos de nivel 0 ó 1, ya que no solo requieren una MFA fuerte, sino que también conviene ejecutarlos en un entorno aislado.
- **Guardar siempre en repositorio seguro** las credenciales de acceso de las cuentas con privilegios y los pares de claves SSH para evitar que caigan en manos equivocadas.
- **Nunca conceder derechos privilegiados de forma indefinida.** Se debe otorgar acceso solo cuando es necesario a los usuarios con privilegios durante un periodo de tiempo predefinido.
- **Aplicar un modelo de confianza cero para todos los usuarios, no sólo para los teletrabajadores y proveedores de servicio externos**. La práctica recomendada es bloquear primero todos los tipos de acceso para todos los usuarios (Zero Trust) y luego definir los permisos para cada usuario autorizado. Esto proporciona una protección óptima de los datos sensibles.
- **Fomentar una conciencia de seguridad**. Se ha demostrado la eficacia de ofrecer regularmente a los empleados de todos los niveles jerárquicos formación en ciberseguridad y enseñarles las prácticas más adecuadas.
- Aplicando estas medidas de seguridad preventivas con las soluciones de ciberseguridad adecuadas se consigue, por un lado, prevenir ataques e incluso frenarlos antes de que sucedan y, por otro lado, una vez que ya ha sucedido, tener una rápida capacidad de respuesta ante el incidente, de forma que la situación pueda ser controlada lo antes posible. Pero para conseguirlo es indispensable equiparar las inversiones en nuevas tecnologías, en aplicaciones o migraciones con la inversión en ciberseguridad. Porque la ciberseguridad, al igual que la salud, no es un privilegio sino una necesidad.

Roger Gallego, Territory Sales Manager de Delinea

Delinea

LA CIBERINTELIGENCIA EN UN MUNDO EN CONSTANTE CAMBIO

En el cambiante entorno digital, donde las amenazas cibernéticas evolucionan constantemente, la ciberinteligencia se erige como un pilar fundamental para la seguridad organizacional.

Identificar y contrarrestar las tácticas, técnicas y procedimientos (TTPs) empleados por ciberdelincuentes es crucial.

Este artículo explora la evolución de la ciberinteligencia, destacando el papel esencial del threat hunting en la detección proactiva de amenazas. Desde la evolución de las TTPs hasta los desafíos persistentes, examinaremos cómo Dotlake CTI proporciona inteligencia valiosa al sumergirse en la Darknet.

También analizaremos la importancia de un Centro de Operaciones de Seguridad (SOC) en la defensa proactiva y exploraremos desafíos y perspectivas futuras en el fascinante mundo de la ciberinteligencia.

Explorando la Evolución de las Tácticas, Técnicas y Procedimientos y el Threat Hunting

La ciberinteligencia se consolida como un ámbito en continua evolución que desempeña un papel fundamental en la salvaguardia de las organizaciones frente a las amenazas cibernéticas cada vez más sofisticadas. Ante el incremento de los ataques cibernéticos, es imperativo que las empresas se preparen para identificar y contrarrestar las tácticas, técnicas y procedimientos (TTPs) empleados por los ciberdelincuentes. En este contexto, el threat hunting emerge como una técnica esencial para detectar y neutralizar amenazas antes de que puedan causar estragos.

- **Threat Hunting: Un Enfoque Proactivo en la Detección de Amenazas**

El threat hunting se define como una estrategia proactiva para identificar amenazas dentro de una red. A diferencia de los enfoques tradicionales de seguridad, que se centran en la detección y respuesta a incidentes, el threat hunting busca identificar y eliminar amenazas antes de que se materialicen. Para llevar a cabo esta tarea, los analistas de ciberinteligencia deben emplear una combinación de herramientas y técnicas avanzadas para rastrear y analizar el tráfico de red, los registros de eventos y otros indicadores de compromiso.

- **Tácticas, Técnicas y Procedimientos y su evolución (TTPs)**

Los actores cibernéticos, dinámicos por naturaleza, buscan constantemente nuevas formas de realizar sus actividades delictivas, aprovechando todas las tecnologías disponibles y futuras para maximizar su impunidad. La comprensión de sus acciones y ubicación es esencial para anticipar, prevenir o detener sus ataques. Las TTPs constituyen el núcleo de las operaciones cibernéticas empleadas para infiltrarse en una red y comprometer la seguridad de una organización. Un ejemplo destacado de esta evolución es el phishing, que ha pasado de correos electrónicos genéricos a campañas altamente personalizadas. La inteligencia artificial se incorpora para personalizar mensajes, aumentando la efectividad de estos ataques, mientras que la ingeniería social se vuelve más astuta al aprovechar la información disponible en redes sociales y otros canales.

Desafíos Permanentes en Ciberinteligencia y Respuesta Proactiva de Dotlake CTI

La ciberinteligencia se enfrenta a un desafío constante: mantenerse al día con las cambiantes TTPs. El análisis de patrones, la correlación de datos y el uso de tecnologías emergentes, como el aprendizaje automático, se han convertido en aliados esenciales para anticipar y contrarrestar estas amenazas en constante evolución.

En respuesta a estos desafíos, Dotlake CTI ha surgido como un defensor proactivo. Diseñada para abordar los retos persistentes, proporciona a sus clientes valiosa inteligencia que les capacita para prever y anticiparse a posibles ataques. En las profundidades de la Darknet, Dotlake se desplaza sin ser identificada, extrayendo información de los rincones más oscuros y de difícil acceso. Además, monitorea fuentes como Telegram, donde los criminales exponen ataques, víctimas o venden datos. De esta manera, los clientes acceden al ecosistema del cibercrimen, monitorizando a los actores cómoda, rápida y eficientemente.

El Rol Fundamental de un SOC en la Detección de TTPs y Threat Hunting

La efectiva operación de un Centro de Operaciones de Seguridad (SOC) se vuelve esencial en la defensa proactiva contra las amenazas cibernéticas en constante evolución. Actuando como el epicentro para la coordinación de operaciones de seguridad, el SOC permite una respuesta rápida y eficiente ante posibles incidentes. La utilización de herramientas avanzadas de análisis de datos, junto con vigilancia constante y búsquedas activas de indicadores de compromiso, capacita a los analistas del SOC para identificar anomalías y actividades maliciosas, evitando la materialización de incidentes críticos de seguridad.

Desafíos y Perspectivas Futuras en Ciberinteligencia

A pesar de los avances, persisten desafíos en ciberinteligencia. La falta de estandarización en la recopilación e intercambio de inteligencia dificulta la colaboración entre organizaciones. La creciente complejidad de las amenazas requiere un constante desarrollo de habilidades y tecnologías por parte de los profesionales de la seguridad. En el horizonte futuro de la ciberinteligencia, se prevé una mayor integración de inteligencia artificial y aprendizaje automático, mejorando la detección de amenazas y aumentando la automatización en la respuesta a incidentes.

Conclusión

El mundo de la ciberinteligencia es dinámico y desafiante. La evolución constante de las TTPs y la adopción del threat hunting son ejemplos claros de cómo los defensores buscan adelantarse a los ciberdelincuentes. La colaboración global y la continua innovación tecnológica, junto con el aumento del nivel de madurez de la ciberinteligencia, son cruciales para enfrentar las amenazas digitales en constante cambio y salvaguardar la integridad de nuestras redes y datos.

Sandra Musulen, Product Manager en Dotlake

CIBERSEGURIDAD, EL CON MENOR TASA DE DES DE ESPAÑA

- **En España, unos 125.000 empleados trabajan en ciberseguridad.**
- **Para 2024 se calcula que se necesitarán 80.000 nuevos profesionales de ciberseguridad.**
- **El número de mujeres que trabaja en ciberseguridad ha aumentado en torno al 30%.**

El número de puestos de trabajo relacionados las Tecnologías de la Información y la Comunicación (TIC) no deja de crecer. La ciberseguridad es un sector en auge que tiene una gran demanda de profesionales y, por tanto, ofrece importantes oportunidades laborales. Según ObservaCiber, en España, **unos 125.000 empleados trabajan en ciberseguridad**. Pero, el imparable crecimiento del sector hace que también exista una escasez de expertos.

Actualmente hay una brecha de 30.000 vacantes sin cubrir, lo que está llevando a casi la mitad de las organizaciones a utilizar la formación y cualificación de personal interno para cubrir los puestos existentes, tal y como señala INCIBE. **Para 2024 se calcula que se necesitarán 80.000 nuevos profesionales de ciberseguridad,** una cifra que se incrementa cada año.

Este escenario pone de manifiesto la necesidad de adaptación del mercado laboral. Entre las principales razones está el desconocimiento generalizado del sector y la necesidad de una mejor definición de los perfiles. Además, es necesario fomentar la formación, tanto por parte de las empresas como por los centros educativos, para revertir así, la falta de concienciación que se sigue dando en el sector.

Los perfiles más buscados son aquellos relacionados con Cloud Computing, análisis de riesgos, Inteligencia Artificial o gobernanza. Pero no son los únicos, el sector brinda muchas oportunidades, no solo en el ámbito técnico. Elena Timón, responsable de Personas de **Secure&IT** explica: "*Sí es cierto que el sector técnico abarca la mayoría de los puestos, pero también hay que cubrir otros campos como la comunicación, el marketing o el derecho TIC, entre otros. El abanico es amplio y las opciones muy diversas*".

Las mujeres en ciberseguridad

Otra de las preocupaciones del sector sigue

SECTOR SEMPLEO

siendo la brecha de género, aunque es cierto que, según INCIBE, **el número de mujeres que trabaja en el mundo de la ciberseguridad ha aumentado considerablemente, en torno al 30%.** En este sentido, el Foro Económico Mundial vaticina que hasta, aproximadamente, el año 2150, no se igualará el número de hombres y mujeres dedicados al mundo de la tecnología.

La falta de mujeres se debe, prácticamente, a las mismas razones que la escasez de profesionales, pero va un poco más allá, pues los estereotipos o falta de visibilidad de las mujeres del sector están afectando en este sentido. Por este motivo, han surgido diferentes organizaciones que tratan de promover los estudios STEM, así como las habilidades digitales, entre las niñas y adolescentes. El objetivo es optimizar las oportunidades para mujeres empresarias, y reducir los estereotipos de género en este sector.

Ante esta situación, Timón expone que "*es necesario fomentar el aumento de profesionales y, en concreto, de mujeres en el sector TIC. Lo podemos conseguir trabajando aspectos como la formación o la concienciación, la creación de planes de carrera, el aumento de la visibilidad de las mujeres del sector o la eliminación de los estereotipos*".

Desde **Secure&IT** queremos reiterar la necesidad de incorporar nuevos talentos al sector TIC y las grandes oportunidades profesionales que la ciberseguridad ofrece.

EL USO DE DEEPFAKE UN 900%

SE CONVIERTE EN UNA HERRAMIENTA CLAVE EN LOS CO

- **El uso de este tipo de manipulaciones, especialmente en el contexto de los conflict consecuencias catastróficas.**
- **Esta amenaza requiere de tecnologías de detección avanzadas, colaboración interna ciencia sobre los riesgos.**

Los deepfakes (combinación de "deep learning" y "fake") plantean, en la actualidad, una seria amenaza. Estas creaciones, que implican la manipulación realista de imágenes y vídeos, están teniendo un impacto significativo en diversos ámbitos, incluyéndose como armamento de guerra y para distorsionar la percepción pública de los conflictos. De hecho, según datos recopilados por el Foro Económico Mundial, los ataques de *deepfake* se disparan anualmente un 900%.

La Oficina Federal de Investigación de Estados Unidos (FBI) ya advirtió este verano de su creciente uso con fines delictivos, especialmente, para llevar a cabo estafas y extorsiones. En muchos de los casos, los delincuentes crean grabaciones manipuladas, que difunden en foros y webs pornográficas, con el objetivo de exigir a las víctimas un dinero por eliminarlas.

En el conflicto entre Rusia y Ucrania, existen muchos ejemplos de cómo los *deepfakes* pueden distorsionar la realidad. De hecho, unos ciberdelincuentes rusos publicaron un video falso del presidente de Ucrania, Volodymyr Zelensky, ordenando la rendición de los soldados ucranianos ante las fuerzas rusas, que se convirtió en el primer uso de desinformación con *deepfake* como arma en un conflicto militar.

Según Francisco Valencia, director general de **Secure&IT** "*los deepfakes se han convertido en una herramienta muy peligrosa en el contexto de las guerras, donde la desinformación puede tener consecuencias catastróficas, debido a las reacciones que puede provocar*". También insiste en que este tipo de manipulación tiene el potencial de socavar la confianza pública y perjudicar mucho el discurso público de los afectados.

De manera similar, en el conflicto entre Israel y Hamás, la inteligencia artificial se está utilizando como "arma" en la guerra de la desinformación, para generar de forma masiva noticias falsas. Desde que se produjo el asalto de milicianos de Hamás en el sur de Israel, y a pesar de la extensa cobertura mediática que ha recibido el conflicto, las redes sociales están siendo inundadas de rumores y noticias falsas.

Con la tecnología que se utiliza en la actualidad, es cada vez más difícil diferenciar entre *fake news* y hechos reales. De hecho, algunas televisiones y periódicos se han hecho eco de ellas dándolas por válidas e, incluso, llegado a difundirlas.

ES SE DISPARA

ONFLICTOS BÉLICOS

tos bélicos, puede tener

cional y una mayor con-

Es el caso de un vídeo que, supuestamente, mostraba un helicóptero del ejército israelí siendo derribado por un soldado de Hamás. Sin embargo, estas imágenes pertenecen al videojuego Arma 3 desarrollado por los estudios Bohemia Interactive.

En este sentido, Francisco Valencia, recalca que la respuesta a esta amenaza requiere tecnologías de detección avanzadas, colaboración internacional y una mayor conciencia sobre los riesgos asociados.

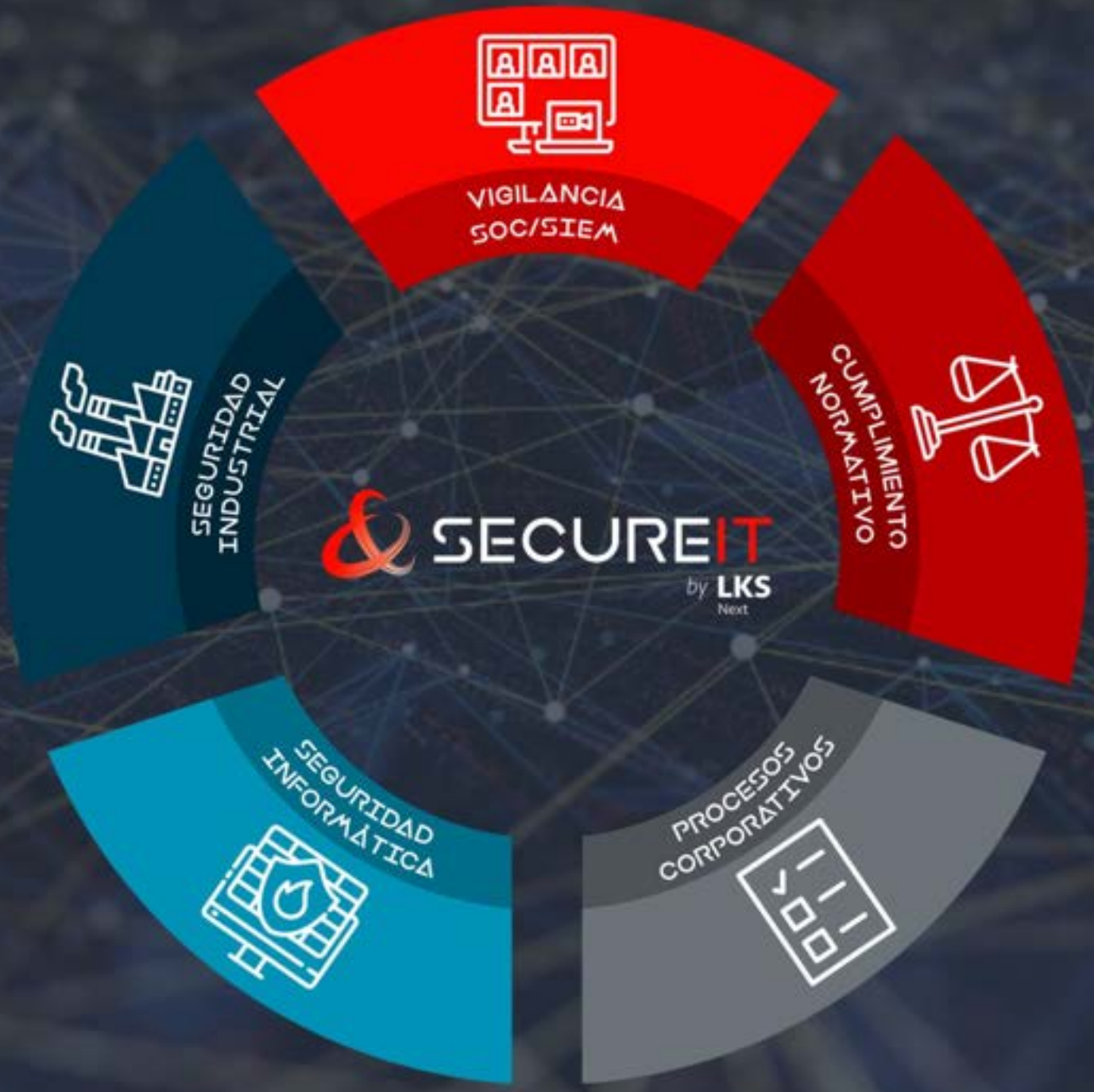
Consejos para detectar un deepfake

Detectar un *deepfake* puede ser difícil, ya que las tecnologías detrás de ellos están mejorando constantemente. Sin embargo, hay algunos aspectos que pueden ayudar a identificarlos:

- **Observación de los ojos**: En los *deepfakes*, los ojos a menudo presentan problemas, como movimientos poco naturales, parpadeos irregulares o la falta completa de parpadeo.
- **Análisis de movimientos labiales y sincronización del audio**: Los *deepfakes* pueden tener dificultades con la sincronización labial. Es importante observar si los movimientos de los labios coinciden con las palabras pronunciadas en el audio.
- **Evaluación de la calidad de la piel**: Los *deepfakes* pueden mostrar inconsistencias en la piel, especialmente alrededor de los bordes del rostro, el cabello y los hombros.
- **Iluminación y sombras:** Las diferencias en la iluminación y las sombras en el rostro pueden ser indicadores de que se trata de un *deepfake*.
- **Verificación de la fuente:** Los *deepfakes* suelen circular con mayor frecuencia por plataformas menos reguladas, por lo que es importante verificar si el contenido proviene de una fuente confiable.

NO ES SOLO SEGURIDAD, ES CONFIANZA

EXPERIENCIA, CALIDAD E INNOVACIÓN



WWW.SECUREIT.ES