SECURE
MAGAZINE

LA DIRECTIVA WHISTLEBLOWING
¿Qué es y cómo te afecta?

ENTREVISTA
JORGE BERMÚDEZ, FISCAL ADSCRITO A LA SECCIÓN DE CRIMINALIDAD INFORMÁTICA

CIBERVIOLENCIA DE GÉNERO
El 25% de las mujeres de 16 a 25 años ha recibido insinuaciones inapropiadas a través de redes sociales

ESPECIAL: JORNADA DE CIBERSEGURIDAD 2023

& SECUREIT by LKS

SUMARIO

04 ENTREVISTA

Jorge Bermúdez, Fiscal adscrito a la Sección de Criminalidad Informática - Fiscal Provincial de Gipuzkoa

10 JORNADA DE CIBERSEGURIDAD

El cibercrimen alcanza un valor global cercano al 1,5% del PIB mundial

14 CIBERINTELIGENCIA DE AMENAZAS

La ciberinteligencia de amenazas logra reducir el tiempo de respuesta ante posibles ciberataques

18 ISO 27001 E ISO 27002

Novedades en la ISO 27001 e ISO 27002

CIBERVIOLENCIA

El 25% de las mujeres de 16 a 25 años ha recibido insinuaciones inapropiadas a través de redes sociales

DIRECTIVA WHISTLEBLOWING

La Directiva Whistleblowing: qué es y cómo te afecta

20 RECONOCIMIENTOS

- **Secure&IT** vuelve a certificarse como Great place to Work
- **Secure&IT** primera empresa en España en certificarse en categoría alta en el nuevo ENS

22 ARTÍCULOS PARTNERS

- Fortinet: *Converger las redes y la seguridad, en enfoque SASE*
- Bitdefender: *Un 23% de los profesionales de TI admite haber encubierto violaciones de datos en sus organizaciones*
- Armis: *¿Está realmente completo tu inventario de activos?*
- AuthUSB: *Ciberataques a través de dispositivos USB*

Estimados lectores,

El cibercrimen ha alcanzado un valor global cercano al 1,5% del PIB mundial. Ha llegado al billón de dólares, 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. En cuanto a sus objetivos, se dirige a todos los mercados, pero, principalmente, a empresas, gobiernos y administraciones. Lo cierto es que las organizaciones del cibercrimen funcionan como cualquier otra empresa. De hecho, sus objetivos son los mismos: reducir costes, incrementar ingresos y mejorar la eficacia y la continuidad de negocio. Tanto es así que, incluso, algunas de ellas, como es el caso del grupo de ciberdelincuentes DarkSide, cuentan con un código de conducta.

Estas son algunas de las cuestiones que se trataron en nuestra jornada de ciberseguridad "La responsabilidad de la empresa ante las nuevas ciberamenazas". En ella, se puso de manifiesto que el principal objetivo de los ciberdelincuentes es obtener información y dinero, generar inestabilidad política y desestabilizar el modelo occidental, es decir, a Europa y EE.UU.

También participó en la jornada, como ponente, nuestro entrevistado Jorge Bermúdez, Fiscal adscrito a la Sección de Criminalidad Informática de la Fiscalía Provincial de Gipuzkoa, que manifestó su preocupación con respecto a algunos ciberdelitos: "*Si hablamos de lo que más me preocupa, en el plano de las estafas te diría que son los delitos que cada vez tenemos más dificultades para perseguir. Y, en lo referente a la pornografía de menores, el hecho de que hemos pasado de la distribución, es decir, de usuarios que utilizaban redes de intercambio de archivos para obtener este material y que contribuían a su difusión, a la creación de contenido. Estamos dejando el perfil de usuario consumidor y para pasar al perfil de usuario productor de pornografía*".

No podemos olvidar que están en auge las nuevas modalidades de ransomware y los ataques de tipo Wiper –aquellos vinculados al ciberterrorismo y la ciberguerra–. Además, el mercadeo delictivo en la Deep Web de credenciales y ataques de tipo *command and control* es cada vez más conocido. Esto provoca que la ciberdelincuencia sea muy accesible, tanto, que es posible hacerlo, incluso, desde el teléfono móvil. Con este panorama, la ciberinteligencia de amenazas se está convirtiendo en una técnica de prevención fundamental.

En esta edición de **Secure&Magazine** también hablamos de normativa. La Directiva (UE) 2019/1937 (más conocida como "Directiva Whistleblowing"), regula la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. Te contamos qué es y cómo te afecta.

Además, hablamos sobre las novedades en ISO 27001 e ISO 27002. Con el paso de los años, ha habido un cambio significativo en nuestra forma de trabajar y de entender las aplicaciones y la operatividad entre ellas. Las nuevas formas de trabajo o los nuevos entornos hacen que nos encontremos ante un panorama diferente en lo que se refiere a gestión diaria de la seguridad de la información. Y ese, precisamente, es el objetivo de los cambios introducidos estas normas: adecuarse al nuevo entorno, tanto en la parte de gestión diaria como en la aplicación de controles de seguridad.

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 Fortinet, Bitdefender, Armis y AuthUSB. Sin sus aportaciones, esta publicación no sería lo mismo.

Aprovechamos también la ocasión para reiterar nuestro agradecimiento a los asistentes, patrocinadores y ponentes su participación en nuestra jornada de ciberseguridad.

El equipo de Secure&IT

JORGE BERMÚDEZ

Fiscal de la 46ª promoción (2006), licenciado en Derecho por la Universidad de Deusto. Desde julio de 2022, ocupa el cargo de Fiscal adscrito a la Sección de Criminalidad Informática de la Fiscalía Provincial de Gipuzkoa.

Durante casi 13 años, hasta marzo de 2020, desempeño el cargo de Delegado de Criminalidad Informática en la Fiscalía Provincial de Gipuzkoa.

Además de su trabajo en la fiscalía, ha realizado importantes contribuciones académicas en el ámbito del derecho y la tecnología. Es coautor de libros como *Investigación Tecnológica y Derechos Fundamentales* y *Memento de ciberseguridad*.

También ha sido invitado como ponente en reconocidas conferencias y eventos relacionados con la seguridad de la información y la criminalidad informática, como RootedCON y Sec/Admin.

Ha asumido roles docentes en diversas instituciones educativas, impartiendo clases en el curso de Experto Tecnológico e Informática Forense de la Universidad de Extremadura, el Máster en Ciberdelincuencia de la Universidad de Nebrija y el curso de Experto en Derecho Digital de la Universidad de Deusto.

Por otro lado, ha representado a la Fiscalía General del Estado en diversas actividades de colaboración internacional. Ha contribuido en iniciativas conjuntas con la Escuela Judicial de Emiratos Árabes Unidos en Abu Dhabi, la Academia de Derecho Europea, la Agencia Española para la Cooperación Internacional y el Desarrollo en Santa Cruz de la Sierra (Bolivia) y el Programa de Asistencia contra el Crimen Trasnacional Organizado (El PAcCTO) en Quito (Ecuador).

“Necesitamos una “tinderización” de la ciberseguridad, que haga transparente su funcionamiento para el usuario”

¿Cuáles son los ciberdelitos más comunes con los que os soléis encontrar? Y, en este sentido, ¿cuáles son los que más os preocupan?

En cuanto a delitos informáticos, las estadísticas de la Fiscalía General del Estado son claras: por goleada, los más numerosos son las estafas, seguidas por los delitos relacionados con la pornografía de menores.

Pero, aquí la cuestión es cuáles son los delitos que ni siquiera llegamos a ver, no porque no estén reflejados en las estadísticas, sino, porque no tenemos capacidad para verlos. Con esto me refiero a grandes exfiltraciones de datos, *ransomware* masivo… Este tipo de delitos se ven rara vez y suelen ir ligados a un arduo trabajo policial, dentro de alguna macrooperación y, frecuentemente, en colaboración con otros países. De repente, “cazan” a una persona que puede ser el administrador de alguna organización que se lucra mediante ataques de *ransomware*, o realizando chantajes a empresas, a las que se amenaza con la publicación de datos obtenidos en una exfiltración anterior. No son unicornios rosas, porque existen, pero son raros de ver, e infinitamente más complejos de investigar.

Si hablamos de lo que más me preocupa, en el plano de las estafas te diría que son los delitos que cada vez tenemos más dificultades para perseguir. Y, en lo referente a la pornografía de menores, el hecho de que hemos pasado de la distribución, es decir, de usuarios que utilizaban redes de intercambio de archivos para obtener este material y que contribuían a su difusión, a la creación de contenido. Estamos dejando el perfil de usuario consumidor y para pasar al perfil de usuario productor de pornografía.

En líneas generales, ¿es fácil sentar a un ciberdelincuente en el banquillo?

No, no es nada fácil. Estamos en una situación que se podría comparar a la que teníamos en la persecución del tráfico de drogas a principios de los 80. Aquella época en la que se cogía a los pequeños “camellos” en la calle, no estaba regulada la existencia de una fiscalía especial como la Fiscalía Antidroga, no había operaciones con la Audiencia Nacional, etc. Ese periodo anterior a las operaciones contra los grandes capos, que se produjeron cuando se empezó a tener medios.

Ahora, en cuanto a ciberdelitos, estamos en esa situación, capturando a “pequeños camellos”. Aunque es cierto que, ocasionalmente, caen en las redes de la policía y, por tanto, llegan a los banquillos personas con un mayor rango dentro de alguna organización criminal.

¿Tiene la justicia las herramientas necesarias para hacerlo? ¿Qué echas en falta en este sentido?

Siempre digo con bastante ironía que me encantó la reforma de 2015 de la Ley de Enjuiciamiento Criminal porque, como está muy enfocada a dar cumplimiento tanto al Convenio de Budapest sobre ciberdelincuencia, como a la distinta normativa coetánea de la Unión Europea, nos solucionó los problemas que teníamos en 2001. Con un poco de suerte, en 2040 nos habrá solucionado los problemas que tenemos ahora.

El inconveniente es que se utilizan herramientas tan ambiciosas, desde el punto de vista el legislador, que son prácticamente imposibles de aplicar. No sirven, salvo en operaciones muy específicas (como puede ser la inspección remota de equipos informáticos, prevista en el artículo 588 septies de la Ley de Enjuiciamiento Criminal). Digamos que esto solo es válido en operaciones de gran formato y, para el delincuente que está detrás de un proxi o de una red de anonimización, nos bastaría con algo mucho más sencillo, que no está contemplado en la Ley de Enjuicia-

miento Criminal. Por hacer una comparativa, diseñaron una especie de nave espacial y se olvidaron de proveernos de una simple fragata para nuestros mares.

Y no estoy hablando en hipótesis. Pongo un ejemplo: hay una herramienta tecnológica disponible para el FBI que es NIT (Network Investigative Technique), que explota una vulnerabilidad de Tor para obtener la localización e identificación real de un sujeto que esté operando detrás de esta red. Esto sería infinitamente más útil, por ejemplo, para poder localizar a un sujeto; llevar a cabo una entrada y registro en su domicilio; incautar sus equipos, poder examinarlos y obtener datos para, en definitiva, poder presentar un caso sólido en los tribunales. Esa posibilidad no la tenemos.

De hecho, no es tanto una cuestión de herramientas de la justicia, sino de que la ley autorice que la justicia permita a la policía la utilización de herramientas que existen y que están en el mercado.

“Se está produciendo una alta profesionalización de bandas que dan soporte a pequeños delincuentes, que obtienen lucro con unos conocimientos muy escasos”

¿Cuáles son los mayores desafíos a los que os enfrentáis con respecto a los ciberdelitos, en comparación con otro tipo de delitos?

La base del problema es el avance de la criptografía: cifrados más potentes y difíciles de romper, el hecho de que los propios *malware* disponen de técnicas internas de enmascaramiento o de que las comunicaciones entre los delincuentes se cifran… En definitiva, el cifrado es una herramienta que los criminales están utilizando en su propio beneficio, con el objetivo de securizar sus transmisiones y ocultar sus datos y sus botines. En este sentido, la justicia no le puede poner puertas al campo. No se puede prohibir la criptografía.

Y, a partir de ahí, también influye el progresivo grado de sofisticación de las herramientas que tienen los delincuentes a su alcance por un proceso, además, de banalización en su uso. Las herramientas son cada vez más de “botón gordo”. Te facilitan tu herramienta lista para delinquir y, además, ponen a tu disposición un sistema de asistencia al usuario por si tu troyano no roba bien. Se está produciendo una alta profesionalización de bandas que dan soporte a pequeños delincuentes, que obtienen lucro con unos conocimientos muy escasos, simplemente, acudiendo a un mercado que les está ofreciendo lo que conocemos como *crime as a service*.

Después de lo que hemos hablado… ¿Podemos decir que tienen mayor impunidad los delitos si se llevan a cabo en el mundo digital?

Sí, por supuesto. En el mundo analógico siempre hay un culpable. No puedes matar a una persona desde la otra punta del globo o robarle desde otro continente. Tienes que estar presente. Y la presencia del delincuente implica la posibilidad de su aprehensión y que sea llevado ante la justicia.

Cuando hablamos del mundo de las tecnologías, tenemos que recordar que Internet nace, precisamente, para hacer irrelevantes las fronteras. Con lo cual, nos encontramos ante ese problema territorial.

Dicho esto, claro que también se atrapa a los ciberdelincuentes, pero, lo cierto es que, para coger a un atracador que se haya llevado un botín de un millón de euros de un banco, hacen falta coches patrulla y buenos agentes, adecuadamente entrenados. El mismo robo, de un millón de euros, cometido desde la habitación de un “niñato” en la otra punta del planeta, implica montar un dispositivo enorme.

En cuanto a la regulación en ciberseguridad, como en otros ámbitos, se va adaptando a la realidad. Un ejemplo es la puesta en marcha del Reglamento de Inteligencia Artificial de la UE, un proyecto legislativo pionero, que se votó a mediados de junio. Pero ¿va a la velocidad correcta o, con respecto al mundo digital, la legislación va por detrás?

Nunca va a la velocidad correcta. Recordemos que el primero correo electrónico se mandó en 1971 y, en pleno año 2005, se hablaba de las nuevas tecnologías y se hacía referencia al

email. No era precisamente nuevo. También es cierto que la tecnología avanza a un ritmo frenético. De hecho, las generaciones más jóvenes consideran que Facebook es una red social para viejos (y eso los que han oído hablar de él).

¿Qué podemos hacer para mejorar esta situación? Y, en concreto, ¿qué puede hacer el regulador?

El problema que tenemos con esta legislación es que trabajamos en modo científico loco. Parece que todo lo que podemos hacer, tenemos que probarlo o hacerlo. Y esto no pasa solo en el plano de las ciencias computacionales, pasa también con la genética y otros campos de conocimiento. A veces suena un poco a capítulo de Los Simpson, pero, lo cierto es que estamos jugando con fuerzas cuya comprensión no alcanzamos del todo. Y esa es la cuestión, que igual es un botón que no habría que pulsar y nos estamos pasando de listos.

Y, en cuanto a la Inteligencia Artificial, ¿qué opinas sobre cómo se está abordando la legislación en este sentido?

En lo que a la inteligencia artificial se refiere, para empezar, tengo que decir que soy bastante escéptico del término. Para mí, la inteligencia artificial es lo que se conoce ahora como inteligencia artificial general. Es decir, una inteligencia con consciencia de sí misma y capacidad para tomar iniciativas. En cuanto a la toma de decisiones, lo que ahora tenemos son máquinas muy listas que, en base a una alimentación masiva de datos y a algoritmos que les permiten aprender de esa información con la que han sido alimentadas, ofrecen respuestas muy rápidas a problemas muy complejos. Pero, todavía no tienen iniciativa propia. Esa barrera la establece un fenómeno que en ciencia computacional se conoce como la singularidad. La barrera de singularidad no la hemos cruzado, ni creo que estemos cerca de cruzarla, o, por lo menos, eso espero.

En cualquier caso, lo que sí empieza a haber es un fenómeno muy preocupante: el funcionamiento de estos algoritmos de *machine learning* en modo *black box*. Se empezó a ver el problema con los vehículos de conducción autónoma, que se diseñan de una cierta forma para que

"Estamos jugando con fuerzas cuya comprensión no alcanzamos del todo. Y esa es la cuestión, que igual es un botón que no habría que pulsar y nos estamos pasando de listos"

tengan un conocimiento básico de las reglas de circulación. Pero, a medida que se entrena a estas máquinas, van aprendiendo y van generando nuevos algoritmos para la resolución de nuevos problemas. Al principio conducen por un circuito de pruebas, en el que no se producen los eventos que pueden suceder en una carretera real (un niño que sale corriendo detrás de una pelota, una señora que cruza la calle, un conductor agresivo…). Pero, las máquinas van aprendiendo a reaccionar y generan un nuevo código. El problema es que llega un momento en el que los propios ingenieros, que están detrás del proyecto, reconocen que son incapaces de saber qué hace la máquina, porque ha aprendido por sí misma. Además, existe otro factor: el aprendizaje se hace una manera que no es accesible al programador, por tanto, ya no sabemos cómo piensa esa máquina.

En mi caso, me fascina pensar cómo van a legislar eso. Es decir, establecer la responsabilidad sobre decisiones tomadas a través de un sistema informático más o menos avanzado, tiene una dificultad relativa. Se puede determinar si es responsabilidad del diseñador del software, del diseñador del hardware, del cliente que lo utiliza de forma adecuada o no… Hasta ahí lo podemos acotar. Pero, desde el momento en el que la máquina se autoprograma, a través de datos que percibe directamente, y aprende a resolver problemas que nunca le habían sido planteados y que no estaban en el código original… ¿A quién le podemos achacar la responsabilidad?

En una de tus ponencias hablas sobre el caso Alcasec y analizas el ciberataque que sufrió el Punto Neutro Judicial (PNJ), la red de telecomunicaciones que conecta los órganos judiciales con otras instituciones del Estado y que gestiona el Consejo General del Poder Judicial (CGPJ).

¿Consideras que es un caso aislado o la administración pública está demasiado expuesta a este tipo de ataques?

Hay que diferenciar entre superficie de exposición y riesgo. En nuestro caso, la administración pública tiene una superficie de exposición inmensa porque vivimos en un estado del bienestar en el que la administración presta muchos servicios y, por tanto, tiene muchos frentes que cubrir. Pero, superficie de exposición no siempre significa riesgo. El riesgo supone que esa superficie de exposición es, además, vulnerable al ataque.

Es evidente que las administraciones públicas están implementando mecanismos de ciberseguridad. El Centro Nacional de Inteligencia (CNI), a través del Centro Criptológico Nacional (CCN), es el garante último de la seguridad de las administraciones públicas. El problema es que vivimos en un estado descentralizado, en el que los centros de poder y toma de decisiones están cada vez más atomizados, sobre todo, en lo que a decisiones tecnológicas se refiere. Con lo cual, las comunidades autónomas tienen sus propias fuentes regulatorias y sus propias agencias de desarrollo tecnológico e, incluso, los municipios empiezan a tener también sus propios centros tecnológicos. En este sentido, es mucho más fácil actuar en una administración estatal, con un centro decisor que establece qué políticas y esquemas de seguridad se implementan o qué medios se utilizan, y todo el mundo procede de manera uniforme, que en un sistema descentralizado, con múltiples centros de decisión.

"¿Por qué Alcasec atacó a través de la administración de justicia del País Vasco? Porque, en ese momento, le resultó el punto más vulnerable. Nada más"

¿Por qué Alcasec atacó a través de la administración de justicia del País Vasco? Porque, en ese momento, le resultó el punto más vulnerable. Nada más.

¿Cuánta "culpa" de estos ataques tiene la falta concienciación y de formación de los usuarios?

Muchísima. Aquí nunca pasa nada, hasta que pasa. Somos un país mediterráneo, con esa filosofía de vida. Tenemos usuarios que son, incluso, reticentes a instalarse aplicaciones de doble factor de autenticación en sus dispositivos. La gente percibe los dispositivos informáticos que pone a su disposición el empleador como algo que les tiene atados y, en muchos casos, no los cuidan bien.

¿Cuál es tu visión sobre el futuro de la ciberseguridad y los ciberdelitos? ¿Hacia dónde debemos ir?

Siempre hemos dicho que tiene que haber un evento colosal que ponga en el ojo de la atención pública esta cuestión. Pero, quizá sea más fácil una reinvención de la tecnología, algo que haga obsoletos los esquemas actuales (no sé si será la computación cuántica o algún otro uso tecnológico). A lo que me refiero es a que Internet no se inventó para ser segura, sino para que funcionara; para que la información viajara de un punto a otro, por cualquier línea viable. Y, además, la seguridad siempre se ha sido pensada por y para expertos.

Por eso, yo propongo "tinderizar" la ciberseguridad, un concepto que ya comenté en una ocasión en INCIBE. Me explico: antes teníamos páginas de contactos en las que hacía falta introducir un formulario larguísimo, con tus gustos, aficiones, características físicas, etc., y un algoritmo calculaba la compatibilidad con otros usuarios. Y, de repente, aparece una aplicación en la que lo único que tienes que hacer es deslizar el dedo para un lado o para otro, y ya está. Y lo que ocurre es que esa app se come todo el pastel del mercado. Por eso, creo que lo que necesitamos en este sentido, es una "tinderización" de la ciberseguridad, que haga transparente su funcionamiento para el usuario. Que no haya que preocuparse de saberse cinco contraseñas o de cuándo toca cambiarlas. Hay que huir de complicarle la vida al usuario y, por el contrario, complicársela más a los ciberdelincuentes.


TU CENTRO
AVANZADO
DE FORMACIÓN
EN CIBERSEGURIDAD
SECURE
ACADEMY
www.secureacademy.es
SECUREIT
by LKS

JORNADA DE CIBERSEGURIDAD

El cibercrimen alcanza un valor global cercano al 1,5% del PIB mundial

- **El cibercrimen supera las cifras del tráfico de armas, drogas y personas juntos.**
- **Los objetivos de los ciberdelincuentes son los mismos que los de las empresas: reducir costes, incrementar ingresos y mejorar la eficacia y la continuidad de negocio.**
- **Lockbit 3.0 es uno de los malware que más víctimas suma a nivel mundial y el que más preocupa a las organizaciones.**

El cibercrimen ha alcanzado un valor global cercano al 1,5% del PIB mundial. Ha llegado al billón de dólares, 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. En cuanto a sus objetivos, se dirige a todos los mercados, pero, principalmente, a empresas, gobiernos y administraciones.

Lo cierto es que las organizaciones del cibercrimen funcionan como cualquier otra empresa. De hecho, sus objetivos son los mismos: reducir costes, incrementar ingresos y mejorar la eficacia y la continuidad de negocio. Tanto es así que, incluso, algunas de ellas, como es el caso del grupo de ciberdelincuentes DarkSide, cuentan con un código de conducta.

En este sentido, Francisco Valencia, director general de **Secure&IT** advierte: "*Nos encontramos en un momento de gran polarización política, conflictos bélicos, crisis energética y alimentaria, inflación económica… Todo esto ha provocado que el cibercrimen se haya convertido en una opción muy viable para muchas personas, y las cifras lo demuestran: el cibercrimen mueve casi el doble de dinero que el tráfico de drogas, armas y trata de personas juntos*".

Sin embargo, según apunta el subdirector del Centro de Coordinación Nacional (NCC) de INCIBE, Ignacio González, la percepción general de los usuarios en nuestro país es que son menos atacados: "*En general, año tras año, los usuarios piensan que son menos atacados. Pero, sin embargo, la tendencia real es creciente. De hecho, el porcentaje de usuarios que declaran tener malware en sus equipos es muy bajo, sobre todo, si lo comparamos con la realidad*".

Estas son algunas de las cuestiones en materia de ciberseguridad que se han tratado en la jornada "La responsabilidad de la empresa ante las nuevas ciberamenazas", organizada por **Secure&IT**. En ella se puso de manifiesto que el principal objetivo de los ciberdelincuentes es obtener información y dinero, generar inestabilidad política y desestabilizar el modelo occidental, es decir, a Europa y EE.UU.

Cibercrimen en la actualidad

En el panorama del cibercrimen, existen diferentes perfiles, pero, los principales actores son: los atacantes solitarios, mercenarios que se venden al mejor postor; el crimen organizado, en el que se encuentran organizaciones como DarkSide, Revil, Anonymous, etc.; países, como Irán, Rusia, China o Corea del Norte, que buscan una ventaja militar, económica o política y, para ello, contratan a muchos de esos grupos del crimen organizado; y, por último, los "insiders", es decir, empleados, clientes o proveedores cuyos ataques pueden ser intencionados o no.

En cuanto a la tipología de los ataques, aumentan los de "Command and Control", aquellos dirigidos a OT, dispositivos móviles e IoT, el robo de información con chantaje –el conocido como "Fraude al CEO"–, el robo de credenciales y phishing y, especialmente, el ransomware con exfiltración.

Una de las organizaciones cibercriminales que está sembrando el terror en el RaaS (Ransomware as a Service) es LockBit. Su nueva variante LockBit 3.0 se ha convertido en uno de los malware que más víctimas suma a nivel mundial. Este ransomware busca automáticamente sus objetivos, propaga la infección y cifra todos los dispositivos accesibles en una red. Se utiliza para lanzar ataques selectivos contra las organizaciones, con el objetivo de interrumpir su actividad, extorsionarlas y robar los datos para su posible publicación. De hecho, Lockbit 3.0 es el malware que más preocupa a los expertos reunidos en la jornada de **Secure&IT**.

Durante la jornada, además, Jorge Bermúdez, Fiscal adscrito a la Sección de Criminalidad Informática de la fiscalía provincial de Gipuzkoa, analizó el caso del ciberataque el Punto Neutro Judicial (PNJ). El ataque fue perpetrado por el hacker José Luis Huertas, alias Alcasec, que recientemente ha sido puesto en libertad, tras permanecer en prisión provisional imputado por robar y poner a la venta un millón y medio de datos tributarios de casi 600.000 contribuyentes.

También participaron en el evento Manuel Carreras, Ingeniero Preventa de **Secure&IT**, Jesús Varela, Regional Sales Director de la empresa Fortinet; Luis Fisas, South EuropeDirector de Bitdefender; Axel Pérez, Solution Architect de Armis; María Cobas, CMO de AuthUSB y la psicóloga clínica, consejera delegada de Grupo Luria, Nieves Jerez.

Igual que en la edición anterior, la jornada se dividió en dos partes. La tarde se destinó a la realización de varios talleres, en los que los participantes pudieron comprobar, de forma práctica, cómo las tecnologías pueden ayudar a las empresas en la gestión de su seguridad de la información.

CIBERSEGURIDAD INDUSTRIAL

SECUREIT by LKS Next

LA CIBERINTELIGENCIA DE AMENAZAS

LOGRA REDUCIR EL TIEMPO DE RESPUESTA ANTE POSIBLES CIBERATAQUES

Francisco Valencia: "Los ciberdelincuentes están a tan solo un clic de sus "armas" en la Dark y la Deep Web, donde pueden descargarse programas para atacar empresas y administraciones de cualquier parte del mundo".

Todas las empresas, independientemente de su tamaño, están en el punto de mira de los ciberdelincuentes. Hoy en día la información vale mucho y los datos de cualquier organización están muy cotizados en el mercado negro.

Sin embargo, la ciberseguridad es una de las asignaturas pendientes para muchos organismos y empresas de España. De hecho, nuestro país es uno de los más ciberatacados del mundo, pero no se encuentra entre los primeros puestos en lo que a inversión en soluciones para evitar estos asaltos se refiere.

Actualmente, están en auge las nuevas modalidades de ransomware y los ataques de tipo Wiper –aquellos vinculados al ciberterrorismo y la ciberguerra–. Además, el mercadeo delictivo en la Deep Web de credenciales y ataques de tipo command and control es cada vez más conocido. Esto provoca que la ciberdelincuencia sea muy accesible, tanto, que es posible hacerlo, incluso, desde el teléfono móvil.

En este sentido, Francisco Valencia, director general de **Secure&IT** explica: "*Con el conflicto armado en Ucrania empezó también la "batalla" en el ciberespacio. Las "armas" asociadas al mundo de la ciberguerra se han hecho muy accesibles y los ciberdelincuentes están a tan solo un clic de ellas en la Dark y la Deep Web, donde pueden descargarse programas para atacar empresas y administraciones, de cualquier parte del mundo*".

Ciberinteligencia de amenazas

Con este panorama, la ciberinteligencia de amenazas se está convirtiendo en una técnica de prevención fundamental.

Su aplicación se basa en la anticipación. De hecho, gracias a la ciberinteligencia de amenazas es posible reducir el tiempo de respuesta ante incidentes y, por lo tanto, la oportunidad de los ciberdelincuentes para perpetrar el ataque.

Cuando se lanza un ataque a una organización siempre hay alguna pista previa que delata la acción de los ciberdelincuentes. La clave de esta herramienta es adelantarse a sus movimientos; ponerse en su lugar y tratar de actuar como ellos.

Así, hay que conocer a los ciberdelincuentes y saber qué buscan, qué herramientas utilizan, desde dónde operan o cuáles son sus capacidades. Para ello, es necesario analizar de forma continua internet, foros, la Deep Web, la Dark Web y otros lugares donde puede haber información sensible que se pueda utilizar en un ciberataque dirigido, o ser la causa de una brecha de seguridad no detectada.

Francisco Valencia: "*A través de fuentes internas y externas de información, y tras un proceso de filtrado y evaluación, se obtiene una información precisa que permite a las organizaciones utilizar la inteligencia generada para anticiparse a los ciberataques. A través de estas fuentes, podemos saber si sus tarjetas de crédito están comprometidas; si se están llevando a cabo actividades maliciosas dirigidas a su organización; si tiene equipos o cuentas de empleados comprometidos; si se ha producido una fuga de datos y qué información de la empresa circula en Internet e, incluso, se pueden prevenir los ataques de phishing*".

La clave de la ciberinteligencia de amenazas es adelantarse a los movimientos de los ciberdelincuentes.

LA DIRECTIVA WHISTLEBLOWING
QUÉ ES Y CÓMO TE AFECTA

La Ley 2/2023, que transpone la Directiva (UE) 2019/1937 (más conocida como "Directiva Whistleblowing"), regula la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

Esta normativa establece la obligación, de determinadas empresas privadas y organismos públicos, de implantar un Sistema Interno de Información dirigido a personas que tengan, o hayan tenido, alguna relación con la organización en el contexto laboral (candidatos de empleo, empleados, exempleados, contratistas, etc.). Además, hay que tener en cuenta que los Sistemas Internos de Información deben cumplir una serie de requisitos: nombramiento de un responsable del sistema, creación de un canal de denuncias, creación de una serie de políticas, formación, etc.

Debido a los riesgos a los que se exponen las personas que informan sobre posibles irregularidades a través de los canales de información corporativos, la Ley 2/2023 tiene como objetivo, además de prevenir y detectar irregularidades, **proteger a los denunciantes de buena fe, evitando que puedan sufrir cualquier tipo de represalia en el contexto laboral.**

¿Qué personas están protegidas por la Ley?

La ley protege a los informantes que trabajen en el sector público y privado, y que hayan obtenido información sobre infracciones del derecho de la Unión Europea, en un contexto laboral o profesional.

También están incluidos los informantes que hayan obtenido la información en el marco de una relación laboral ya finalizada, voluntarios, becarios, trabajadores en periodo de formación, así como a aquellos cuya relación laboral todavía no haya comenzado (en los casos en los que la información sobre infracciones haya sido obtenida durante el proceso de selección o negociación precontractual).

¿A quién aplica? ¿Tu empresa está obligada a cumplir con esta normativa?

En el **sector privado**, la normativa aplica a las personas físicas o jurídicas que tengan contratadas a 50 o más trabajadores. Las personas jurídicas con entre 50 y 249 trabajadores pueden compartir el sistema con otras entidades que cumplan con los requisitos establecidos por la ley.

También están obligados por la normativa los partidos políticos, sindicatos, organizaciones empresariales y fundaciones financiadas con fondos públicos, así como las personas jurídicas que ya estuvieran obligadas por la "Directiva Whistleblowing".

En el **sector público**, todas las entidades están obligadas a tener un Sistema Interno de Información (independientemente del número de integrantes). Sin embargo, en casos específicos, como los municipios con menos de 10.000 habitantes o las entidades vinculadas o dependientes de órganos de las administraciones territoriales, pueden compartir el sistema con otros organismos, siempre y cuando se garantice la independencia y no se genere confusión para los ciudadanos.Principio del formularioFinal del formulario

¿Cuáles serán sus obligaciones?

Principalmente, los sujetos obligados por la normativa tendrán que **implantar un Sistema Interno de Información**. A través de este sistema, debe ser posible la comunicación por diferentes vías sobre las infracciones previstas en el ámbito de aplicación de la Ley 2/2023, garantizando la confidencialidad de todos los datos e informaciones que consten en la comunicación.

El sistema de información deberá contar con un responsable y con un procedimiento de gestión de comunicaciones. Además, los sujetos obligados **deberán informar y formar a los empleados sobre sus derechos y obligaciones al respecto**. Aquí se incluyen las medidas de protección del denunciante establecidas en la organización, así como de los canales internos y externos de comunicación que tienen a su disposición.

¿Es obligatorio nombrar un DPO?

Aunque el anteproyecto de la Ley establecía esta obligación, en el texto actual de la Ley 2/2023, solo se obliga a la Autoridad Independiente de Protección del Informante (AAI) y a las autoridades independientes que se constituyan a nombrar un Delegado de Protección de Datos (DPO). En consecuencia, se ha eliminado la obligación de designar un DPO para aquellas entidades que deben contar con un Sistema Interno de Información, por el mero hecho de ser un sujeto obligado. Las organizaciones deberán analizar si tienen la obligación de designar un DPO teniendo en cuenta los criterios establecidos en RGPD y la LOPDgdd.

¿Quién debe gestionar el canal de comunicaciones?

La norma permite que la gestión de los Sistemas Internos de Información de forma interna o externa. Se puede externalizar la gestión del sistema de recepción de informaciones, siempre que la entidad en la que se externaliza garantice ser independiente, tratar la información de manera confidencial, y garantice el secreto de las comunicaciones y de los datos de carácter personal.

¿Existe la posibilidad de recibir una sanción por no cumplir con la Ley?

Se establecen diferentes categorías de infracciones: leves, graves y muy graves. El importe de la sanción varía, dependiendo de si la infracción ha sido cometida por una persona física o jurídica. En el caso de las personas físicas, las sanciones podrán llegar hasta los 300.000 euros, cuando se trata de infracciones muy graves. Si hablamos de personas jurídicas, pueden recibir multas de hasta 1.000.000 de euros, en el caso de infracciones muy graves. Para las infracciones más graves se prevén sanciones administrativas adicionales, que podrán consistir en la prohibición de obtener subvenciones o beneficios fiscales, o la prohibición de contratar con el sector público, entre otras.

¿Cuál es el plazo establecido para implementar o adaptar el Sistema interno de información?

Desde que entró en vigor, la Ley ha establecido un plazo máximo de 3 meses para que las entidades obligadas implementen el Sistema interno de información, lo que significa que deben hacerlo **antes del 13 de junio de 2023**. Sin embargo, se ha establecido una excepción que permite una ampliación del plazo para las entidades del sector privado con menos de 249 trabajadores y para los municipios con menos de 10.000 habitantes, que tienen hasta el 1 de diciembre de 2023 para cumplir con esta obligación.

¿Necesitas asesoramiento personalizado sobre este tema? ¿Quieres crear un sistema interno de información y no sabes cómo? En **Secure&IT** podemos ayudarte. ¡Contacta con nosotros!

Juan Manuel Valiente

Responsable del Área Jurídica de Secure&IT

NOVEDADES EN ISO 27001 E ISO 27002

Con el paso de los años, ha habido un cambio significativo en nuestra forma de trabajar y de entender las aplicaciones y la operatividad entre ellas. La COVID, las nuevas formas de trabajo o los nuevos entornos hacen que nos encontremos ante un panorama diferente en lo que se refiere a gestión diaria de la seguridad de la información.

Y ese, precisamente, es el objetivo de los cambios introducidos en la ISO 27001:2022 e ISO 27002:2022: adecuarse a este entorno nuevo, tanto en la parte de gestión diaria como en la aplicación de controles de seguridad.

ISO 27001:2022

La ISO 27001 es la norma internacional que, por excelencia, define los requisitos de gestión de la seguridad de la información. Antes de entrar en materia, hay que aclarar que los cambios en la nueva versión de este estándar no son muy sustanciales, pero, destacan algunos aspectos:

- Se deben **determinar cuáles de los requisitos de las partes interesadas serán abordados a través del Sistema de Gestión de Seguridad de la Información**.
- La organización debe **establecer, implementar, mantener y mejorar** de manera continua **un Sistema de Gestión de Seguridad de la Información**, incluyendo los procesos necesarios y sus interacciones, de acuerdo con los requisitos de esta norma.
- Los **objetivos en el SGSI deben estar monitorizados** y tiene que estar disponible como información documentada.
- Cuando la organización determine la necesidad de realizar **cambios en el SGSI, se deberán llevar a cabo de manera planificada**.
- **La comunicación con las partes interesadas se ha simplificado**. Se han agrupado dos requisitos en uno más genérico y, de esta forma, hay un mayor margen de actuación a la hora de aplicar la norma.
- En el control operacional, **se establecen criterios para los procesos** y se implementarán los controles en base a ellos.
- La organización debe **evaluar el desempeño de la seguridad de la información y la efectividad del Sistema de Gestión de Seguridad de la Información**.
- Se debe **garantizar que los procesos, productos o servicios proporcionados externamente, y que son relevantes para el SGSI, están controlados**. El requisito incluye también productos y servicios contratados a proveedores externos.
- Se debe **evaluar** el desempeño de la seguridad de la información y la efectividad del **Sistema de Gestión de Seguridad de la Información**.
- En la revisión por dirección, se deberá **prestar atención a los cambios en las necesidades y expectativas** que son relevantes para el SGSI.

En este sentido, Pablo Zarco, el responsable del área de Procesos de **Secure&IT** apunta: "*Como se puede observar, la ISO 27001:2022 no ha sufrido cambios muy sustanciales. No obstante, estas modificaciones nos harán revisar todos los procedimientos asociados con el objetivo de garantizar que, si algún punto queda pendiente, lo podamos incorporar en la medida y la forma en la que nos pide la nueva normativa.*"

ISO 27001:2022

La ISO 27002 está ligada a la 27001; es un estándar de apoyo y respaldo. De hecho, incluye controles de seguridad técnicos y organizativos para implementar la 27001, que es la norma certificable. Es decir, la ISO 27001 proporciona el marco de requisitos para poder implementar un Sistema de Gestión de Seguridad de la Información y la 27002 los con-

troles de seguridad que, a modo de recomendaciones, sustentarían este sistema.

¿Qué cambios son los más significativos?

- **Cambio de nombre.** Se ha cambiado el término "Código de prácticas" por el de "Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información".
- **Cambios en controles de seguridad.** La versión 2013 contenía 114 controles divididos en 14 dominios. La versión actual contiene 93 controles divididos en cuatro grandes bloques: organizacionales (37 controles), de personal (8 controles), físicos (14 controles) y tecnológicos (34 controles). También se han añadido 11 controles nuevos y otros, de los existentes, se han agrupado o renombrado.
- **Incorporación de nuevos elementos a nivel de control.** En esta nueva versión se han añadido una serie de atributos a cada uno de los controles de la ISO 27002, con el objetivo de filtrar u ordenar los controles según su ámbito de aplicación o propósito: Tipo de control (preventivo, detectivo y correctivo); dimensiones de información involucrada (confidencialidad, integridad y disponibilidad); conceptos de ciberseguridad (identificar, proteger, detectar, responder y recuperar); capacidades operativas (seguridad física, seguridad de sistemas y redes, seguridad de aplicaciones, configuración segura, gestión de identidad y acceso, gestión de amenazas y vulnerabilidades, continuidad, seguridad de relaciones con proveedores, cumplimiento y legal, gestión de eventos de seguridad de la información y garantía de seguridad de la información); dominios de seguridad (gobernanza y ecosistema, protección, defensa y resiliencia).

Las empresas que estén certificadas en ISO 27001 deberán asegurar el cumplimiento de los nuevos controles y la reorganización los existentes, para adaptarse a la nueva 27002. En este sentido, será necesario que **las organizaciones revisen el tratamiento de riesgos, alineen la lista de controles en la declaración de aplicabilidad (SOA) y actualicen las políticas y procedimientos.**

En cuanto a objetivos y plazos, estas son las fechas más significativas:

- **Primeras fechas para evaluaciones en el nuevo estándar**: se inició en **noviembre de 2022.** Actualmente continuamos con esta definición y se estima las primeras certificaciones para el mes de abril de 2023 .
- **Disponibilidad general de certificación: comprende el periodo de febrero a abril de 2023.** En este periodo se está llevando a cabo el despliegue general de la norma.
- **La última fecha para auditorías iniciales o recertificaciones de la versión de 2013 será abril de 2024.** A partir de esta fecha no se podrá realizar ninguna auditoría más relacionada con la ISO 27002:2013. Tendrán que realizarse las de la nueva versión.
- **La invalidación de todos los certificados de la versión 2013 se llevará a cabo en octubre de 2025.**

Pablo Zarco: "*Para la realización de todos estos cambios, las organizaciones cuentan con un periodo de transición, que suele ser de dos años. Pero, hay que tener en cuenta que, aunque las certificadoras no exigirán las modificaciones en ese tiempo, deberán confirmar que la organización está en proceso de adaptación a la nueva norma*".

SECURE&IT

VUELVE A CERTIFICARSE COMO

GREAT PLACE TO WORK

Secure&IT, empresa líder en el sector de la seguridad de la información, se ha vuelto a certificar como un Gran Lugar para Trabajar con un altísimo *Trust Index*©.

Este reconocimiento es otorgado por la consultora *Great Place to Work*®, líder en la identificación y certificación de *Excelentes Lugares para Trabajar*.

Se trata de la certificación internacional más prestigiosa, en gestión de personas y estrategia de negocio, basándose en la percepción de los empleados sobre la confianza, la camaradería, el liderazgo y las oportunidades de crecimiento. que se otorga anualmente a los mejores empleadores del mundo.

El 96% de los trabajadores opinan que Secure&IT es un gran lugar para trabajar.

Por segundo año consecutivo, tras un diagnóstico del ambiente organizacional, la compañía ha vuelto a obtener la certificación "Great Place to Work" que acredita que tiene una cultura de alta confianza, capaz de atraer y retener talento. El índice de confianza (Trust Index©) obtenido por **Secure&IT** en la certificación ha sido de 96%, lo que se traduce en que 9,6 de cada 10 personas opinan que es un excelente lugar para trabajar; una cifra por encima de la media de compañías incluidas en las *Best Work Places 2022*, que es de 87. Este logro representa un aumento significativo en comparación con el 92% obtenido el año pasado, lo que demuestra el compromiso continuo de la compañía en crear un entorno laboral excepcional para los trabajadores.

En concreto, los resultados de la encuesta desvelan la especial valoración que sus profesionales hacen de la camaradería, la credibilidad y el orgullo; entre otras cuestiones. Destaca la cercanía con los trabajadores, el trato recibido y la forma en la que la compañía contribuye a la sociedad.

Entre las principales estrategias en materia de RR.HH. puestas en marcha por **Secure&IT** destaca su labor para fomentar el compañerismo, el buen ambiente laboral y el crecimiento profesional de sus trabajadores.

Francisco Valencia, director general de **Secure&IT**: *"Estamos muy emocionados de recibir una calificación del 96% en la certificación "Great Place to Work". En Secure&IT valoramos a nuestros empleados y creemos que un excelente ambiente laboral es fundamental para el éxito de nuestra empresa. Juntos, hemos construido una comunidad en la que todos se sienten valorados, respetados y motivados para dar lo mejor de sí mismos. Por eso, seguiremos trabajando para buscar continuamente formas de fortalecer nuestra cultura empresarial, y para seguir siendo un lugar donde todos puedan desarrollar su carrera profesional".*

Great Place to Work® es la firma consultora que durante más de 30 años lleva trabajando con empresas de todo el mundo para identificar, crear y mantener culturas de alta confianza y alto rendimiento ayudando a las organizaciones a convertirse en *Mejores Lugares para Trabajar*.

SECURE&IT PRIMERA EMPRESA EN ESPAÑA EN CERTIFICARSE EN CATEGORÍA ALTA EN EL NUEVO ENS

En **Secure&IT** estamos muy contentos de anunciar que, además de certificar nuestros sistemas de información (aquellos que dan soporte a los servicios de arquitectura, sistemas y procesos que se emplean en nuestro servicio de seguridad gestionada, **Secure&View©**) en el nuevo Real Decreto del Esquema Nacional de Seguridad, hemos sido los primeros en España en certificarnos en categoría alta.

¿Qué significa esto para nuestros clientes? Con el Esquema Nacional de Seguridad se establecen controles de seguridad, que son exhaustivamente analizados y que garantizan las medidas de seguridad más exigentes, en los sistemas con los que prestamos servicio.

La subida de nivel, de medio a alto, supone la implementación de nuevos controles y requisitos, así como nuevos roles y responsabilidades, más exigentes.

¿En qué consiste el Esquema Nacional de Seguridad?

Como decíamos, el Esquema Nacional de Seguridad establece controles que se analizan de manera muy exhaustiva y que garantizan las medidas de seguridad más exigentes.

Para implantar el ENS es necesario **elaborar una Política de Seguridad**; realizar un análisis previo (se analiza la criticidad de los servicios y la tipología de la información afectada) para poder determinar la **categoría del sistema**; llevar a cabo un **análisis de riesgos**, en base a una metodología reconocida internacionalmente y en función de la categoría del sistema; elaborar una **declaración de aplicabilidad** que determine qué medidas son las más eficaces para reducir el riesgo del sistema, y –una vez hecho esto- hay que implantar las medidas adoptadas.

Además, como el Esquema Nacional de Seguridad es un sistema de gestión de la seguridad de la información, basado en el ciclo de mejora continua de Deming, requiere **llevar a cabo verificaciones periódicas**. El objetivo es asegurar que el sistema funciona adecuadamente, identificar no conformidades o puntos de mejora y aplicar las medidas necesarias.

Renovamos certificación y subimos de categoría

La certificación en categoría alta en el nuevo Real Decreto del Esquema Nacional de Seguridad (ENS) se suma a nuestros certificados **ISO 9001 e ISO 27001**. A esto se añade que somos **miembros Gold de la Red Nacional de SOC del CCN-CERT**; del **TF-CSIRT**, el principal foro europeo de Respuesta a Incidentes y Equipos de Seguridad Informática; del foro **FIRST**, organización referente en la respuesta ante incidentes a nivel mundial y tenemos el sello **Cybersecurity Made in Europe**, que otorga ECSO y que pone en valor la calidad de las empresas europeas de ciberseguridad.

CONVE
SEGURI
EN EN

El teletrabajo y el modelo de trabajo híbrido siguen siendo una prioridad para muchas empresas. Así lo corrobora el Estudio global de Fortinet `Trabajo desde cualquier Lugar´, que desvela que el 60% de los encuestados continúa teniendo empleados que trabajan desde casa y el 55% tiene una estrategia de trabajo híbrida. Por tanto, la mayoría de las organizaciones seguirán operando con una red híbrida que combine una infraestructura tradicional con un sistema basado en la nube. Pero este crecimiento del trabajo desde cualquier lugar también ha introducido nuevos riesgos. Según ese mismo estudio, en los últimos 2 a 3 años, el 62% de las empresas han sufrido una brecha atribuible, al menos en parte, a vulnerabilidades relacionadas con el trabajo desde cualquier lugar.

El problema radica en que cuando las soluciones de seguridad no están integradas tanto on-premise como en cloud, es casi imposible garantizar una seguridad coherente para todos los usuarios. Cada una de ellas puede funcionar por sí sola y responder a las capacidades que promete, pero no están diseñadas para trabajar con el resto de soluciones que las rodean. Además, la proliferación de proveedores en estos entornos reduce la visibilidad y el control y ahí es donde nace la vulnerabilidad de la red y se generan las brechas de seguridad entre las soluciones aisladas. Y cuanto mayor y más distribuida sea la red, más generalizados pueden ser estos problemas.

Para resolver estos problemas surgió el enfoque SASE de un único proveedor, un servicio que permite el acceso de confianza cero basado en la identidad del usuario, dispositivo o entidad, combinado con el contexto en tiempo real (como la postura de seguridad del dispositivo, por ejemplo) para ejecutar y establecer el gobierno de las políticas de seguridad y cumplimiento.

Las ventajas de consolidar productos y reducir el número de proveedores, como propone SASE de un único proveedor, van desde la reducción de la huella total de los proveedores dentro de la red hasta la reducción de los gastos generales asociados a la implantación, gestión, optimización y mantenimiento de una amplia variedad de soluciones. Evidentemente, no resulta sorprendente que la reducción de productos y proveedores ahorre dinero, pero la convergencia también puede hacerlo.

Convergencia de redes y seguridad

Y es que la convergencia de infraestructura y seguridad permite a una organización establecer la seguridad en cualquier lugar y en cualquier perímetro, de forma que funciona como un elemento totalmente integrado de la red, y la integración del despliegue, la gestión, la configuración y la orquestación garantiza que todos los elementos funcionen juntos a la perfección, a lo largo de toda la red, como un único marco.

Por qué es importante un enfoque SASE de un único proveedor

Las soluciones SASE de varios proveedores suelen acarrear problemas de implementación y gestión. Los controles manuales, las secuencias de comandos y la limitada información sobre amenazas que utilizan la mayoría de los proveedores de SASE no pueden seguir el ritmo de la rápida evolución del panorama actual de las amenazas, lo que convierte a las organizaciones en vulnerables.

Frente a esa propuesta, la solución SASE de un único proveedor hace converger las redes y la seguridad y puede transferir sin problemas las conexiones entre la nube y los dispositivos locales. Con un enfoque de proveedor único, las políticas de acceso y seguridad van allá donde vaya el usuario, en lugar de terminar en el extremo de la red. Sólo mediante la convergencia de las redes y la seguridad de extremo a extremo las organizaciones pueden implantar una arquitectura integral de confianza cero.

Está claro, por tanto, que para reducir la complejidad y proporcionar una seguridad coherente a una plantilla híbrida global, que trabaja tanto en las instalaciones de la empresa como fuera de ellas, las organizaciones

ERGER LAS REDES Y LA IDAD, NFOQUE SASE

necesitan un enfoque SASE de proveedor único.

Así lo pone de manifiesto Gartner, en *Market Guide for Single-Vendor SASE,* que destaca que para 2025:

- Un tercio de los nuevos despliegues SASE se basarán en una oferta SASE de un único proveedor, frente al 10% en 2022.
- El 80% de las empresas habrán adoptado una estrategia para unificar la web, los servicios en la nube y el acceso a aplicaciones privadas utilizando una arquitectura SASE/SSE, frente al 20% en 2021.
- El 65% de las empresas habrá consolidado componentes SASE individuales en uno o dos proveedores SASE asociados explícitamente, frente al 15% en 2021.
- El 50% de las nuevas compras de SD-WAN formarán parte de una oferta SASE de un único proveedor, frente al 10% en 2022.

La propuesta de Fortinet: Universal SASE

La propuesta de Fortinet va más allá del enfoque SASE de proveedor único y marca la tendencia hacia Universal SASE, seguridad integral basada en la nube, alojada y gestionada por Fortinet, para proteger a los usuarios remotos con una sencilla interfaz de usuario también basada en la nube, una licencia de usuario y un agente unificado.

Esta propuesta se materializa en FortiSASE, que ofrece una solución SASE integral que amplía la convergencia de redes y seguridad desde el perímetro hasta los usuarios remotos. Hace converger a la perfección la red (SD-WAN) y la seguridad en la nube (SSE compuesto por una pasarela web segura, acceso universal a la red de confianza cero, broker de seguridad de acceso a la nube y Firewall-as-a-Service). Además, un único sistema operativo (FortiOS) y un único agente (FortiClient), con IA y ML en capas, impulsan la eficiencia operativa.

FortiSASE respalda tres casos de uso principales:

- Acceso seguro a Internet: protección de todo el tráfico de usuarios hacia y desde Internet.
- Acceso Privado Seguro - Acceso seguro y fiable a aplicaciones alojadas de forma privada
- Acceso SaaS seguro: visibilidad y control completos para aplicaciones SaaS

Organizaciones de todos los tamaños y de todos los sectores, desde fabricantes de aluminio hasta cadenas de comida rápida, confían en FortiSASE para habilitar un Acceso Seguro a Internet que sea rápido y garantice una seguridad consistente para todo el tráfico de usuarios hacia y desde Internet. Esta es una ventaja de importancia crítica a medida que más usuarios se unen a una fuerza de trabajo remota, las aplicaciones SaaS experimentan una rápida adopción, y los datos se mueven rápidamente entre los centros de datos, filiales y entornos híbridos y multi-cloud.

La seguridad y las redes deben continuar convergiendo para permitir a las organizaciones adaptarse a las continuas necesidades y prioridades que surgen en el panorama empresarial actual. Y teniendo en cuenta que la opción del trabajo desde cualquier lugar es la nueva normalidad, las compañías que no hayan empezado a adoptar soluciones de redes y seguridad convergentes pronto tendrán que hacerlo.

Por último, teniendo en cuenta que cada organización tiene un viaje de aceleración digital único, con su propuesta, Fortinet se ha marcado el objetivo de ayudar a unificar las soluciones de seguridad y redes para reducir la complejidad, aumentar la eficacia de la seguridad y garantizar una experiencia de usuario fiable en las redes, que se encuentran en plena expansión de hoy en día.

UN 23% DE LOS PROFESIONALES DE TI A
HABER ENCUBIERTO VIOLACIONES DE D
EN SUS ORGANIZACIONES

Bitdefender publica un informe que revela los principales retos e inquietudes de las empresas en materia de

Bitdefender, líder mundial en ciberseguridad, ha presentado el Informe de Evaluación de la Ciberseguridad en 2023, basado en el análisis de una encuesta independiente realizada entre directores de seguridad y TI, que pone de manifiesto las principales inquietudes, prácticas y problemas relacionados con la seguridad, así como los mayores retos que afrontan las empresas en sus entornos.

"Las organizaciones de todo el mundo se encuentran sometidas a la enorme presión de lidiar con unas amenazas en permanente evolución, como el ransomware, las vulnerabilidades de día cero y el espionaje, a la vez que luchan con la complejidad de extender la cobertura de seguridad a todos los entornos y con una continua escasez de capacitación", ha señalado Andrei Florescu, director general adjunto y vicepresidente sénior de productos de Bitdefender Business Solutions Group. *"Los resultados de esta encuesta demuestran, más que nunca, la importancia de la seguridad por capas, que ofrece prevención, detección y respuesta ante las amenazas avanzadas en toda la empresa, además de aumentar la eficiencia, que permite a los equipos de seguridad hacer más con menos"*.

Este informe se basa en el análisis de una encuesta independiente realizada a más de 400 profesionales de seguridad y TI, desde gerentes hasta directores de seguridad de la información (CISO), de empresas de más de mil empleados en España, Francia, Alemania, Italia, Reino Unido y Estados Unidos.

Entre los principales hallazgos del Informe de Evaluación de la Ciberseguridad en 2023 destacan los siguientes:

- **Los profesionales de ciberseguridad reciben a menudo instrucciones para no divulgar las vulneraciones.** Un tercio (34,8%) de los profesionales de seguridad y TI encuestados en España manifiesta haber recibido instrucciones de no divulgar alguna violación de seguridad que debería haberse denunciado, secreto que admiten haber guardado el 22,73% de los profesionales españoles. Estos casos de solicitudes para que los profesionales de seguridad y TI no divulgaran las vulneraciones se dan con mayor frecuencia en Estados Unidos (71 %), seguidas por Reino Unido (44 %), Italia (36,7 %) y Alemania (35,3 %). A nivel mundial, un 30% de los encuestados admite haber mantenido una violación confidencial cuando sabía que debería ser reportada.
- **Casi tres de cada cuatro encuestados aumentará su presupuesto de seguridad.** El 70% de los profesionales encuestados en España (74% en el resto del mundo) planea aumentar su presupuesto en seguridad en 2023, mientras que el 20% (25% global) planea reducir las nuevas compras de tecnología de ciberseguridad y otro 20% (23% global) tiene previsto disminuir las nuevas contrataciones de ciberseguridad. España lidera con un 13,64% el porcentaje de encuestados que afirman que la incertidumbre económica no ha afectado a su presupuesto de seguridad para 2023.
- **Más de la mitad de las empresas encuestadas han sufrido alguna violación de la seguridad durante los últimos 12 meses.** Además de que un gran porcentaje de los profesionales reciben instrucciones para mantener las vulneraciones en secreto, el 52% de los encuestados a nivel global reconoce haber sufrido una vulneración o filtración de datos durante los últimos 12 meses. Estos casos se dan sobre todo en Estados Unidos, con un 75% (un 23 % más que la media), seguido por Reino Unido (51,4 %), Alemania (48,5 %) y España (43,94%). Dada la frecuencia de las filtraciones de datos y la presión para mantenerlas en secreto, los profesionales de seguridad y TI afrontan una situación delicada. A más de la mitad de los encuestados (el 55%) les preocupa que su empresa se enfrente a problemas legales debido a la gestión inadecuada de una violación de la seguridad.

- **El ransomware es la amenaza más preocupante para los españoles.** Ante la pregunta de qué amenaza para la seguridad les causa mayor inquietud, los profesionales españoles citan el ransomware (60,61%) como su principal preocupación, seguido de cerca por el phishing / ingeniería social (59%), las vulnerabilidades de software y las amenazas de día cero (50%), los ataques contra su canal de suministro (43,94%), las amenazas internas (37,88%), el espionaje (21,21%) y la escalada de privilegios (16,67%). A nivel global, los encuestados manifiestan hallarse más preocupados por las vulnerabilidades de software o las amenazas de día cero (53,38%), seguidas de cerca por las amenazas de phishing o ingeniería social (52%) y, en tercer lugar, los ataques dirigidos contra la cadena de suministro (49%). El hecho de que las vulnerabilidades de software sean su principal preocupación viene a corroborar la investigación de Bitdefender Labs que puso de manifiesto un notable aumento en 2023 de los ciberdelincuentes que explotan vulnerabilidades de software conocidas mediante ataques de prueba de concepto (PoC).

- **El principal reto para los profesionales españoles es la complejidad de las soluciones de seguridad.** Más de la mitad de los profesionales de seguridad y TI encuestados en España (56%) afirman que el mayor desafío que afrontan es la complejidad de las soluciones de seguridad (43% a nivel global), seguido de la ampliación de las capacidades de seguridad informática en múltiples entornos (50%), la incompatibilidad con otras soluciones de seguridad (33,33%), la falta del conjunto de habilidades en materia de seguridad (27%), demasiadas alertas (24%) y las capacidades de informes (18%). En el resto del mundo, con un 43%, el principal desafío para los profesionales reside en ampliar la capacidad de seguridad informática en todos los entornos.

- **La cobertura continua de ciberseguridad es crucial para las empresas.** Casi todos los encuestados (el 99%) manifiestan que contar con un proveedor de seguridad gestionada, como un servicio de detección y respuesta gestionadas (MDR), constituye un elemento clave de sus programas de seguridad. De hecho, casi todos los encuestados (el 99%) afirman que actualmente utilizan o están planteándose utilizar un proveedor de servicios gestionados de seguridad. El principal motivo se encuentra en disponer de una cobertura de seguridad disponible todos los días y a todas horas (45% a nivel global y 42% en España), seguido por la capacidad de liberar recursos internos de informática o ciberseguridad (35% a nivel global y 36% en España). Además, el 95% de los encuestados en España (93% en el resto del mundo) destacan la importancia de la búsqueda proactiva de amenazas.

Fuentes de datos

Bitdefender encargó a Censuswide, consultora internacional líder en estudios de mercado, que encuestara y analizara las respuestas de más de 400 profesionales de TI y seguridad de empresas a partir de mil empleados de diversos sectores. Dicha encuesta y análisis se desarrollaron desde diciembre de 2022 hasta enero de 2023. Los encuestados se repartieron geográficamente por igual entre Francia, Alemania, Italia, España, Reino Unido y Estados Unidos.

Para descargar gratuitamente una copia del Informe sobre el panorama de amenazas del consumidor de 2023, puedes acceder aquí.

Bitdefender
BUILT FOR RESILIENCE

¿ESTÁ REALMENTE COMPLETO INVENTARIO DE ACTIVOS?

Los retos de visibilidad de red tienen sus culpables habituales en los activos no gestionados, el Internet de las Cosas (IoT) y la tecnología operativa (OT). Aunque en los entornos empresariales la mayoría de activos sean conocidos y están gestionados, debido al mayor uso de dispositivos informáticos tradicionales como ordenadores portátiles y servidores, seguimos encontrando puntos ciegos.

Es posible que tu empresa tenga un problema de visibilidad, no necesariamente porque los dispositivos y sistemas sean invisibles, sino por la falta de un inventario fiable que ofrezca una imagen completa y precisa del entorno.

Este artículo analiza los retos de la fragmentación de IT y ofrece orientación sobre cómo las empresas pueden superar los silos y lograr una visibilidad holística de los activos conectados a la red de la empresa.

Los obstáculos de una visibilidad de IT fragmentada y un contexto limitado

Es probable que tu pila tecnológica disponga de varias herramientas para recopilar y analizar distintos tipos de información sobre activos. Véanse algunos ejemplos de herramientas de gestión de activos:

- El software de gestión de activos informáticos (ITAM) proporciona un inventario de sus activos, incluidas las fechas de compra y los números de serie.
- La base de datos de gestión de la configuración (CMDB) almacena datos más específicos sobre los elementos configurables (CI) de sus activos.
- Endpoint Protection Platform (EPP) examina archivos y sistemas para detectar y bloquear malware u otras actividades maliciosas.

Cuando se utilizan soluciones dispares, el resultado es una visibilidad de IT fragmentada, que no ofrece una visión completa del entorno de activos de extremo a extremo. Y muy a menudo, estas herramientas proporcionan información contradictoria o duplicada, es difícil saber en qué fuente de datos confiar y cómo remediar los datos.

Tener un inventario de activos fragmentado y en silos es una de las principales señales de falta de visibilidad de los dispositivos informáticos. Para los profesionales de la seguridad encuestados por Armis, la visibilidad de los activos es el mayor reto de ciberseguridad al que se enfrentan sus organizaciones. Nuestra investigación también señala que sólo la mitad de las empresas conocen el número de activos conectados a su red corporativa.

Consecuencias de una visibilidad de activos limitada

Se habla de visibilidad de IT en silos cuando los activos de hardware y software de una organización se gestionan de forma independiente dentro de divisiones o departamentos separados. La falta de visibilidad holística de los activos empresariales puede provocar ineficiencias y puntos ciegos en materia de seguridad. Y crear retos como:

- Errores manuales e incapacidad de escalar la implementación debido a procesos manuales poco fiables y lentos para la recopilación de datos de activos.
- Infrautilización de los activos empresariales. Al conocer datos de utilización de los activos, se pueden eliminar licencias de software y reducir costes.
- Informes imprecisos. Si su inventario de activos no se actualiza en tiempo real, la información con la que se trabaja es obsoleta y poco fiable.
- Redundancias. Al no saber qué activos forman parte del ecosistema empresarial, se puede incurrir en gastos en activos nuevos e innecesarios.
- Costes elevados asociados al tiempo de inactividad o al mantenimiento de los dispositivos y sistemas heredados.

Mayor exposición a riesgos por no tener un conocimiento completo de la superficie de ciberataque.

¿Qué se necesita para una visibilidad completa de los activos de IT?

Para obtener una visibilidad completa de los activos informáticos, es necesaria una plataforma que se integre a la perfección con herramientas preexistentes y reúna información de múltiples fuentes en un único lugar. En otras palabras, es necesario el descubrimiento continuo de nuevos activos, un inventario fiable y evaluaciones en tiempo real basadas en la inteligencia de activos y el panorama de amenazas.

Tener una lista de los dispositivos conectados a la red de la empresa no es suficiente. También es necesaria información contextual. Por ejemplo:

- ¿Dónde están los dispositivos y cuándo se vieron por última vez?

O TU

- ¿Son vulnerables? ¿Siguen recibiendo asistencia de sus fabricantes? ¿Hay algún parche disponible?
- ¿Con qué frecuencia se utilizan? ¿Por quién? ¿Con qué fin?

Tener respuestas a estas preguntas permite a las organizaciones gestionar mejor sus activos digitales.

Casos de uso para una visibilidad completa de los dispositivos

Eficacia operativa y ahorro de costes

Con un inventario exhaustivo de todos los activos, las partes interesadas pueden acceder y ver fácilmente el estado y la ubicación de los activos en tiempo real. La información sobre la utilización de los dispositivos permite una gestión más eficiente de los activos, incluido el seguimiento del inventario y la asignación de recursos. He aquí algunos escenarios:

- Se puede evaluar el uso de los dispositivos y tomar decisiones de adquisición basadas en datos para evitar la escasez de equipos.
- Se puede comprender mejor cuándo retirar del servicio dispositivos lentos y obsoletos que están obstaculizando la productividad de los empleados.
- Se puede preguntar por qué no se utiliza un dispositivo e investigar si se debe a una falta de demanda o a un mal funcionamiento.

Examinar estas cuestiones puede ayudar a racionalizar las operaciones y reducir la deuda técnica.

Mejoras en la seguridad

La visibilidad de los activos informáticos también permite a las organizaciones tomar medidas proactivas para mejorar su ciber resiliencia. Algunos ejemplos de lo que se puede hacer:

Asegurarse de que los dispositivos están actualizados y que los endpoints están correctamente desplegados.

Evaluar los riesgos y priorizar las acciones necesarias como parte de un programa de gestión de vulnerabilidades.

Los activos informáticos gestionados también plantean riesgos

La visibilidad completa de los activos de IT es fundamental porque los dispositivos gestionados plantean riesgos de ciberseguridad propios. Por ejemplo, es posible que se tenga un inventario de todos los ordenadores en el entorno, pero estas máquinas pueden no tener las últimas actualizaciones de seguridad, pueden estar infectadas con malware o pueden verse fácilmente comprometidas debido a los débiles hábitos de contraseña de los empleados. De hecho, el 56% de los encuestados en un estudio de Keeper admiten utilizar la misma contraseña para varios sitios/aplicaciones. Si una contraseña se ve comprometida, un atacante puede utilizar esa misma contraseña para acceder a otras cuentas y violar su red.

La visibilidad de la seguridad de la red ayuda a minimizar los incidentes cibernéticos causados por el elemento humano (por ejemplo, ataques sociales, usos indebidos y errores). Uno de los casos de uso sería identificar los activos gestionados configurados incorrectamente, un tema cada vez más preocupante dado que el 13% de las brechas se deben a errores humanos, según el informe de Verizon. Por ejemplo, un tipo común de error que suele dar lugar a filtraciones es el almacenamiento en la nube mal configurado y sin los controles de acceso adecuados. Una mayor visibilidad de los activos facilita descubrir problemas de seguridad como éste y priorizar las correcciones antes de que sea demasiado tarde.

Matt Hubbard, Director de marketing de productos y soluciones empresariales

ARMIS

CIBERATAQUES A TRAVÉS DE DISPOSTIV USB

INCIDENCIA Y DESAFÍOS PARA LAS ORGANIZACIONES INDUSTRIALES

En la era digital, la interconexión de sistemas y la dependencia de la tecnología han llevado a un aumento significativo de los ciberataques. Las organizaciones industriales no son una excepción y se han convertido en un objetivo atractivo para los ciberdelincuentes.

En particular, los ataques dirigidos a través de dispositivos USB han demostrado ser una amenaza persistente. Este artículo explora la incidencia y los desafíos que suponen los ciberataques dirigidos a organizaciones industriales a través de dispositivos USB, centrándose en la ingeniería social como una táctica comúnmente utilizada.

OS

Incidencia

Los ciberataques a través de dispositivos USB han ganado popularidad debido a su efectividad y simplicidad.

En el año 2022 y según un estudio llevado a cabo por Honeywell, el 52% de las amenazas se desarrollaron para su utilización a través de medios removibles, el 79% de estas tienen el potencial de hacer disrupciones críticas y el incremento que se ha producido durante este año en este tipo de ataques es de un 35%.

Las organizaciones industriales son especialmente vulnerables a este tipo de ataques ya que el uso de este tipo de dispositivos es frecuente para labores de parcheado, actualización de maquinaria, cambios en las lineas de producción etc…Debido a la presencia de sistemas críticos de control y supervisión a traves de estos ciberataques se podrían paralizar operaciones vitales si son comprometidos.

Desafíos

Ingeniería social:

La ingeniería social desempeña un papel crucial en el éxito de los ataques a través de dispositivos USB. Los atacantes utilizan tácticas de manipulación psicológica para engañar a los empleados y lograr que inserten los dispositivos USB infectados en los sistemas corporativos. Esto puede implicar el envío de correos electrónicos de phishing convincentes, la colocación estratégica de dispositivos USB en lugares donde los empleados puedan encontrarlos o incluso el uso de pretextos para persuadir a los empleados desprevenidos.

Detección y mitigación:

La detección de dispositivos USB maliciosos es un desafío constante para las organizaciones industriales. Los dispositivos infectados pueden estar ocultos en apariencia, lo que dificulta su identificación. Además, la falta de conciencia y capacitación adecuada sobre los riesgos asociados con los dispositivos USB puede llevar a una adopción descuidada por parte de los empleados. La implementación de medidas de seguridad, como la utilización de soluciones de detección y políticas estrictas de uso de dispositivos USB, se vuelve esencial para mitigar esta amenaza.

Consecuencias operativas y financieras:

La disrupción en las redes operativas, además de la interrupción de las operaciones, pueden resultar en pérdida de datos, robo de propiedad intelectual y daño a la reputación empresarial. Los costos asociados con la recuperación y reparación de los sistemas afectados son muy significativos, sin mencionar las posibles multas regulatorias y demandas legales de los afectados.

Medidas de mitigación

Concienciación y capacitación:

La ciber educación de los empleados, a todos los niveles desde el CEO a la última persona que ha entrado, es fundamental para prevenir los estos. Las organizaciones industriales deben implementar programas de concienciación y capacitación regulares para informar a los empleados sobre las tácticas utilizadas por los ciberdelincuentes y fomentar prácticas de seguridad sólidas, como evitar la inserción de dispositivos USB desconocidos en sistemas corporativos, teniendo en cuenta que los dispositivos móviles que pertenecen a la empresa se incluyen también en este rango.

Políticas y procedimientos de seguridad:

Es importante establecer políticas y procedimientos claros en relación con el uso de dispositivos USB en las organizaciones industriales. Esto incluye restricciones sobre la conexión de dispositivos efectuar un cierre (físico o a través de Bios) de todos los puertos USB de la organización no permitiendo las excepciones bajo ningún concepto, la implementación de controles de acceso físico y la utilización de soluciones de seguridad que en primer lugar monitoreen , detecten y detengan actividades sospechosas en tiempo real a los tres niveles de ataque que se pueden producir (Ataque eléctrico destructivo, Ataque a nivel Hw (Rubber ducky y similares) y ataque a nivel Sw (Malware específico)

Además, estas soluciones deben estar de forma constante analizando del dispositivo presentado ya que, en cualquier momento puede cambiar su comportamiento, de tal manera que NUNCA se puede permitir la entrada en la organización de dispositivos externos.

Por último, deben dar también una capa de información, trazabilidad y auditoria de la capa USB en tiempo real al administrador de la red.

En España se ha desarrollado una tecnología única que realiza todas esas acciones de manera sencilla y rápida. authUSB SafeDoor®

Actualizaciones y parches:

Mantener los sistemas y dispositivos actualizados con los últimos parches de seguridad es crucial para los fabricantes de equipos industriales y proveedores de softwa-re suelen lanzar actualizaciones de seguridad para corregir vulnerabilidades conocidas. Es responsabilidad de las organizaciones industriales implementar estas actualizaciones de manera oportuna y de manera que el efectuarlas no suponga comprometer a la organización.

Conclusión:

Los ciberataques dirigidos a organizaciones industriales a través de dispositivos USB representan una amenaza real y significativa en la era digital actual. La ingeniería social desempeña un papel fundamental en el éxito de estos ataques, lo que destaca la importancia de la concienciación y capacitación de los empleados. Al implementar políticas de seguridad sólidas, medidas de detección avanzadas y programas de educación continuos, las organizaciones industriales pueden fortalecer su postura de seguridad y mitigar los riesgos asociados con los ciberataques a través de dispositivos USB.

CIBERVIOLENCIA,

VIOLENCIA DE GÉNER

- **El 25% de las mujeres de 16 a 25 años ha recibido insinuaciones inapr**
- **En España se han multiplicado por cinco los ciberdelitos sexuales con**

Actuar contra la violencia de género es uno de los retos de la sociedad actual.

El desarrollo de las TIC ha provocado que, en los últimos años, se haya producido un aumento de la **ciberviolencia**, una forma de violencia que va mucho más allá del ámbito del hogar, de la pareja o de la familia: se extiende en toda la Red y de formas muy distintas. Hay algunas violaciones de la privacidad en el mundo online que son bastante habituales: hackeo para obtener información personal de la víctima, suplantación de la identidad digital, vigilancia y seguimiento por geolocalización, spameo o acoso. Pero, la ciberviolencia también incluye aspectos como la "porno-revancha", el grooming (acciones llevadas a cabo por un adulto para ganarse la amistad de un menor de edad, con el objetivo de abusar sexualmente de él) o el sexting (difusión de imágenes o vídeos eróticos sin autorización de la persona que aparece en ellos).

Según el informe "Políticas públicas contra la violencia de género", elaborado por el Observatorio Nacional de Tecnología y Sociedad, en menos de una década se han multiplicado por cinco, en España, los delitos de contacto mediante tecnología con fines sexuales con menores de 16 años.

Este informe también recoge los datos de la *"Macroencuesta de Violencia contra la Mujer"* realizada a 10.000 mujeres. Según su información, **el 7,2% de las encuestadas recibió imágenes sexualmente explícitas,** el 15,2% experimentó acoso reiterado por parte de una misma persona y el 4,3% sufrió la publicación de las imágenes por parte del acosador.

En este sentido, hay que destacar que la edad es un factor determinante. Las mujeres jóvenes sufren en mayor medida el ciberacoso. **Más de un 25% de las mujeres entre 16 y 25 años ha recibido insinuaciones inapropiadas a través de redes sociales**. Y, alrededor del 20% de las jóvenes entre 16 y 20 años ha recibido correos electrónicos, mensajes de texto o fotografías sexualmente explícitas, que les hicieron sentirse ofendidas, humilladas o intimidadas.

Según Francisco Valencia, director general de Secure&IT: "***La educación debe ser la herramienta para combatirlo*** *y, en este sentido, los adultos debemos plantearnos qué mensaje estamos lanzando a nuestros jóvenes. No podemos inculcarles a nuestros hijos que los celos son una expresión de amor y, según estudios realizados por la Delegación del Gobierno para la Violencia de Género, más de un tercio de los adolescentes ha*

UNA
O INVISIBLE

opiadas a través de redes sociales.
n menores de 16 años.

escuchado esto por parte de personas mayores.

Además, ***cada vez es más urgente que introduzcamos en nuestro día a día la defensa de la privacidad y los datos personales, porque los peligros del ciberespacio son muchos y muy graves".***

El principal problema al que nos enfrentamos a la hora de analizar la incidencia de la violencia de género digital en España es la escasez de estadísticas. Según señala el Instituto Europeo de Igualdad de Género, los datos sobre ciberviolencia contra mujeres y niñas son escasos y se sabe muy poco sobre el porcentaje real de víctimas y de la prevalencia de daños causados.

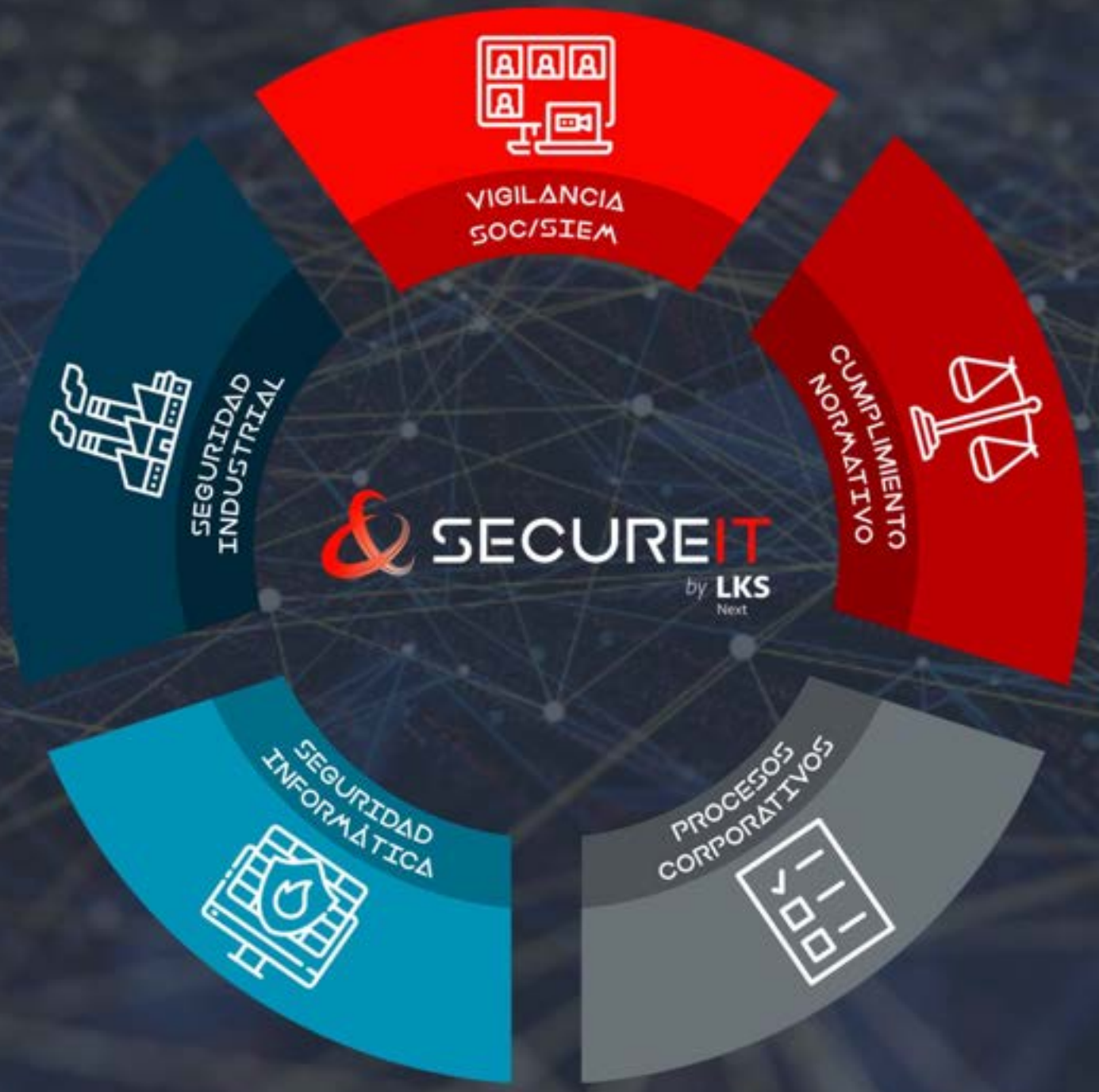
Cómo denunciar la ciberviolencia

La denuncia puede ser interpuesta, desde el anonimato, por la persona agredida o por alguien que haya sido testigo de esa conducta. Se pueden dirigir al Grupo de Delitos Telemáticos de la Guardia Civil, a la Brigada de Investigación Tecnológica de la Policía Nacional, a los Mossos de Escuadra y a la Ertzaintza. También es posible acudir a los juzgados a interponer la demanda, personándose directamente el denunciante o su representante legal.

"Las redes sociales dejan un rastro y todas las acciones de ciberviolencia quedan registradas, aunque los ciberdelincuentes intenten borrar sus pasos. Los expertos pueden, podemos, encontrarles, por este motivo es tan importante que ***denunciemos*** *este tipo de acciones y que el miedo o la vergüenza no sean un motivo de silencio",* declara Valencia.

NO ES SOLO SEGURIDAD, ES CONFIANZA

EXPERIENCIA, CALIDAD E INNOVACIÓN



WWW.SECUREIT.ES